PROGRAM GUIDE

8th International Conference on Availability, Reliability and Security (ARES 2013)

IFIP WG 8.4, 8.9, TC5 International Cross-Domain Conference and Workshop (CD-ARES 2013)

02 – 06 September 2013

Universität Regensburg, Germany

Organized by…

Universität Regensburg & secure sba-research.org

Supported by…

TU WIEN Technische Universität Wien Vienna University of Technology; ifip; UR; ITSECURITY Bavarian IT Security & Safety Cluster; Regensburger Universitäts Stiftung; SECBIT; Society for ICT Knowledge Transfer

Table of Contents

The 8th International Conference on Availability, Reliability and Security (ARES 2013) 4
Cross-Domain Conference and Workshop (CD-ARES 2013) 5
Overview 6
Monday, 02 September 2013 7
Tuesday, 03 September 2013 22
Wednesday, 04 September 2013 41
Thursday, 05 September 2013 57
Friday, 06 September 2013 63
Keynotes, Tutorials & Panel 70
Floor plan 74
How to get to the Conference Venue (Universität Regensburg) 75
About Regensburg 76
Regensburger Dult (23.08.2013 – 08.09.2013) 77
Where to eat in your free time (tips from a local) 78
Social Events 79
Conference Office 80

The 8th International Conference on Availability, Reliability and Security (ARES 2013)

The 8th International Conference on Availability, Reliability and Security (ARES 2013) brings together researchers and practitioners in the field of dependability and information assurance. ARES 2013 highlights the various aspects of dependability, following the tradition of previous ARES conferences, again with a special focus on the crucial linkage between availability, reliability, security and privacy.

ARES aims at contributing to an intensive discussion of research issues in the field of dependability as an integrative concept that in its core comprises research contributions from availability, safety, confidentiality, integrity, maintainability, security and privacy and their different areas of application. The conference emphasizes the interplay between foundations and practical issues of research in information security and will also look at upcoming research challenges.

ARES 2013 is dedicated to expanding collaborations between different sub-disciplines and to strengthening the community for further research which, previous ARES conferences have started to build.

This year we are very happy to welcome two well-known keynote speakers: Elena Ferrari, Director DiSTA STRICT SociaLab, University of Insubria, Italy and Carl Gunter, Department of Computer Science, University of Illinois at Urbana-Champaign, USA.

From the many submissions we have selected the **22** best for a presentation as full paper. The quality of submissions has steadily improved over the last years and the conference officers sometimes faced a difficult decision when selecting which papers should be accepted. This year's acceptance rate for full papers is **24**%.

In addition, several workshops and short papers are included in the program and show intermediate results of ongoing research projects and offer interesting starting points for discussions. In addition to the keynotes ARES 2013 also features 4 tutorials, given by Stefan Katzenbeisser (TU Darmstadt & CASED, Germany), Haya Shulman (TU Darmstadt, Germany), Ludwig Fuchs (University of Regensburg, Germany) and Gary McGraw (Cigital, United States). Further a panel discussion will be held reflecting the topic of "Threats & Risk Management – Bridging the Gap between Industry needs and Research", moderated by Martin Gilje Jaatun (SINTEF ICT, Norway) and discussed by Gary McGraw (Cigital, United States), Greg Soukiassian (BC & RS, France) and Chris Wills (CARIS Research, UK).

A different country hosts the conference every year. The 2013 edition takes place in Regensburg, Germany, at the University of Regensburg.

We wish all participants an enjoyable conference and interesting discussions.

The ARES 2013 Program Committee Co-Chairs

Günther Pernul, *University of Regensburg, Germany*
Ravi Sandhu, *University of Texas at San Antonio, United States*

Cross-Domain Conference and Workshop (CD-ARES 2013)

The Cross-Domain Conference and Workshop CD-ARES is focused on the holistic and scientific view of applications in the domain of information systems. The idea of organizing cross-domain scientific events originated from a concept presented by the IFIP President Leon Strous at the IFIP 2010 World Computer Congress in Brisbane, which was seconded by many IFIP delegates in further discussions. Therefore, CD-ARES concentrates on the many aspects of information systems in bridging the gap between the research results in computer science and the many application fields. This effort leads us to the consideration of the various important issues of massive information sharing and data integration, which will (in our opinion) dominate scientific work and discussions in the area of information systems in the second decade of this century.
The organizers of this event who are engaged within IFIP in the area of Enterprise Information Systems (WG 8.9), Business Information Systems (WG 8.4), and Information Technology Applications (TC 5) very much welcome the typical cross-domain aspect of this event.

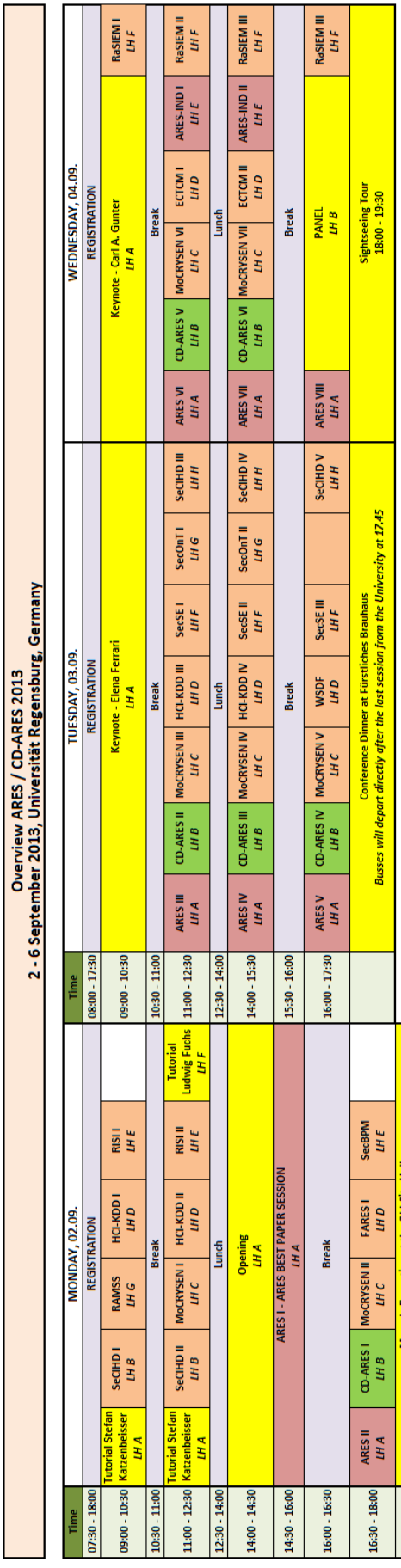
The collocation with the SeCIHD 2013 Workshop was another possibility to discuss the most essential application factors. Special thanks to Professor Ilsun You for all his efforts in this special track, which was this year for the third time.
Also, we are proud to announce the Special Session Human–Computer Interaction & Knowledge Discovery (HCI-KDD), which was organized in the context of CD-ARES 2013. The ultimate goal of the task force HCI-KDD is to combine the best of two worlds: human–computer interaction (HCI), with emphasis on human intelligence, and knowledge discovery from data (KDD), dealing with computational intelligence. The cross-domain integration and appraisal of different fields provide an atmosphere in which to foster different perspectives and opinions. Special thanks to Dr. Andreas Holzinger, who made it possible to bring together researchers from diverse areas in a highly inter-disciplinary manner, to stimulate fresh ideas and encourage multi-disciplinary work.
Today, e-business depends heavily on the major cryptographic breakthroughs of almost 40 years ago. Without asymmetric cryptography, hardly any form of business transaction would be as easy to secure as it is today. We are thus very happy to have an excellent section on applied cryptography in this book.
The special track on modern cryptography and security engineering (MoCrySEn) attracted 30 submissions, of which the Program Committee selected 16 for publication in the workshop proceedings. The accepted papers dealt with symmetric-key cryptography, public-key cryptography, algorithmic cryptanalysis, software and hardware implementation of cryptographic algorithms, database encryption and interaction between cryptographic theory and implementation issues.

The papers presented at this conference were selected after extensive reviews by the Program Committee with the essential help of associated reviewers. We would like to thank all the Program Committee members and the reviewers, who made great effort contributing their time, knowledge, and expertise and foremost the authors for their contributions.

The CD-ARES 2013 Editors

Alfredo Cuzzocrea, *ICAR-CNR and University of Calabria, Italy*
Christian Kittl, *Evolaris Next Level, Austria*
Dimitris E. Simos, *SBA Research, Austria*
Edgar Weippl, *Vienna University of Technology and SBA Research, Austria*
Lida Xu, *Old Dominion University, US*

Overview



Overview ARES / CD-ARES 2013
2 - 6 September 2013, Universität Regensburg, Germany

Time	MONDAY, 02.09.					TUESDAY, 03.09.							WEDNESDAY, 04.09.					
07:30 - 18:00	REGISTRATION					REGISTRATION							REGISTRATION					
09:00 - 10:30	Tutorial Stefan Katzenbeisser *LH A*	SeCHD I *LH B*	RAMSS *LH G*	HCI-KDD I *LH D*	RISI I *LH E*	Keynote - Elena Ferrari *LH A*							Keynote - Carl A. Gunter *LH A*					RaSIEM I *LH F*
10:30 - 11:00	Break					Break							Break					
11:00 - 12:30	Tutorial Stefan Katzenbeisser *LH A*	SeCHD II *LH B*	MoCRYSEN I *LH C*	HCI-KDD II *LH D*	RISI II *LH E*	Tutorial Ludwig Fuchs *LH F*	ARES III *LH A*	CD-ARES II *LH B*	MoCRYSEN III *LH C*	HCI-KDD III *LH D*	SecSE I *LH F*	SecOnT I *LH G*	SeCHD III *LH H*	ARES VI *LH A*	CD-ARES V *LH B*	MoCRYSEN VI *LH C*	ECTCM I *LH D*	ARES-IND I *LH E*	RaSIEM II *LH F*
12:30 - 14:00	Lunch					Lunch							Lunch					
14:00 - 15:30	Opening *LH A*					ARES IV *LH A*	CD-ARES III *LH B*	MoCRYSEN IV *LH C*	HCI-KDD IV *LH D*	SecSE II *LH F*	SecOnT II *LH G*	SeCHD IV *LH H*	ARES VII *LH A*	CD-ARES VI *LH B*	MoCRYSEN VII *LH C*	ECTCM II *LH D*	ARES-IND II *LH E*	RaSIEM III *LH F*
14:30 - 16:00	ARES I - ARES BEST PAPER SESSION *LH A*					Break							Break					
16:00 - 16:30	Break					ARES V *LH A*	CD-ARES IV *LH B*	MoCRYSEN V *LH C*	WSDF *LH D*	SecSE III *LH F*		SeCHD V *LH H*	ARES VIII *LH A*	PANEL *LH B*				RaSIEM III *LH F*
16:30 - 18:00	ARES II *LH A*	CD-ARES I *LH B*	MoCRYSEN II *LH C*	FARES I *LH D*	SecBPM *LH E*	Conference Dinner at Fürstliches Brauhaus *Busses will depart directly after the last session from the University at 17.45*							Sightseeing Tour 18:00 - 19:30					
	Mayor's Reception at the Old City Hall 19:30 - 23:00																	

Time	THURSDAY, 05.09.							FRIDAY, 06.09.		
08:00 - 17:30	REGISTRATION							REGISTRATION		
09:00 - 10:30	Tutorial Haya Shulman *LH A*	ARES IX *LH F*	CD-ARES VII *LH E*	TWISNet I *LH D*	ARES XI *LH F*	FARES II *LH D*	SecATM I *LH E*			
10:30 - 11:00	Break									
11:00 - 12:30	Tutorial Haya Shulman *LH A*	ARES X *LH F*	IWSMA *LH G*	TWISNet II *LH D*	FARES III *LH F*	FARES IV *LH D*	SecATM II *LH E*			
12:30 - 14:00	Lunch									
14:00 - 15:30	Tutorial - Gary McGraw *LH A*									SecATM III *LH E*
15:30 - 16:00	Break									
16:00 - 17:30	Tutorial - Gary McGraw *LH A*									

Monday, 02 September 2013

07:30 – 18:00 Registration for all events

09:00 – 10:30 Parallel Sessions

Tutorial

Location: Lecture Hall A

Challenges in Data Protection - Privacy by Design (Part I)

Stefan Katzenbeisser (TU Darmstadt & CASED, Germany)

Abstract: The increasing use of networked IT systems brings new challenges regarding the protection of privacy sensitive data. While in the past privacy was mainly assured through regulatory approaches, access control and audits, these mechanisms tend to be inappropriate for largely distributed systems. New technical protection mechanisms come to rescue: they allow to make sensitive data available for various applications, while protecting them from misuse. The tutorial will provide an introduction two technically different approaches. First, data usage control allows to implement fine-granular data-centric access control policies which span across systems boundaries. These approaches gained popularity due to the availability of novel operating systems security concepts, such as strong isolation and virtualization, and can be implemented using concepts like Trusted Computing. Second, cryptographic protocols, based on homomorphic encryption and Secure Multiparty Computation, can be designed, which allow to privately process sensitive data and prevent data leakage to insiders.

SeCIHD I – Cyber Security and Dependability I – 3rd International Workshop on Security and Cognitive Informatics for Homeland Defense

Session Chair: Ilsun You (Korean Bible University, South Korea)

Location: Lecture Hall B

1. Keynote – Visual Cryptography: An Overview
   Roberto De Prisco (University of Salerno, Italy)

   Abstract: Secret sharing allows the sharing of a secret among a set of participants in such a way that only some (qualified) subsets of participants can recover the secret while all other (forbidden) subsets have no information about the secret. Visual Cryptography is a special type of secret sharing in which the secret is an image, the shares are images printed on transparencies and the reconstruction process is the superposition of the shares. Visual Cryptography has been introduced by Kafri and Keren (1987) and Naor and Shamir (1984). After the paper by Naor and Shamir a large number of papers have studied several aspects of the problem. Three different models have been used: the random grid model, the deterministic model and the probabilistic model. Lower bounds, constructions of schemes, generalizations and extensions have been studied. In this talk we will give a survey of the field focusing on the relations between the models, providing an account of the most important results and presenting novel insights regarding the relations among the three models.

2. Cyber Threats Monitoring: Experimental Analysis of Malware Behavior in Cyberspace
   Clara Maria Colombini (University of Milan, Itlay), Antonio Colella (Italian Army, Itlay), Marco Mattiucci (High Tech Crime Department (RTI), Itlay), Aniello Castiglione (University of Salerno, Italy)

   Abstract: Cyberspace is a borderless new universe in which all actors, including States, share information and communications technologies, now indispensable to the modern lifestyle. Since the beginning of the 21st century, the ability to leverage cyberspace has become the most important source of power. Due to the proliferation of ICT systems into all aspects of life, the importance of information for political matters has increased awfully. State and

non-State actors can use this power to achieve objectives into cyberspace and physical world. Low cost and high potential impact make cyber-power attractive to all actors. In fact, cyber threats have grown exponentially with the proliferation of the cyberspace infrastructures. Consequently, cyberspace has become a war-fighting domain with the potential to destroy or make useless logical, physical, technical, and virtual infrastructure, damaging in fact critical National capabilities.
This scenario forces all national institutions to a review of their defense strategies, because of the difficulties to identify the actors of a cyberattack. It then becomes necessary to gain a broader view of the problem to acquire more detailed information, useful to identify such sources of cyber-attacks. This new point of view can be achieved by using the analytical method developed by the authors and applied to data streams owing across the cyberspace. In this way we can collect, detect, isolate and analyze the behavior of those malware that are acting as cyber weapons, through the implementation of an honeypot-based system such as the one presented in this paper.

3. Analyzing the Internet Stability in Presence of Disasters
Francesco Palmieri (Seconda Universit`a di Napoli, Italy), Ugo Fiore (Universit`a Federico II, Italy), Aniello Castiglione (University of Salerno, Italy), Fang-Yie Leu (Tunghai University, Italy), Alfredo De Santis ((University of Salerno, Italy)

Abstract: The Internet is now a critical infrastructure for the modern, information-based, e-Society. Stability and survivability of the Internet are thus important, especially in presence of catastrophic events which carry heavy societal and financial impacts. In this work, we analyze the stability of the inter-domain routing system during several large-scale catastrophic events that affected the connectivity of massive parts of the address space, with the objective of acquiring information about degradation of service and recovery capabilities.
Results show that the Internet has maintained good responsiveness: service disruption has been contained and recovery times have been fast, even after catastrophic events. However, combining the view provided by the routing table and the view originated by the analysis of the BGP updates is not a trivial task, as such phenomena need to be analyzed at multiple time scales.

RAMSS – 1st International Workshop on Statistical Methods in Reliability Assessment of Complex Industrial Multi-state Systems

Session Chair: Ilia Frenkel (SCE - Shamoon College of Engineering, Israel)
Location: Lecture Hall G

1. Invited Talk – Statistical Surrogate modeling of computer experiments with different mesh densities
Jeff Wu (Georgia Institute of Technology, United States)

Abstract: This talk considers deterministic computer experiments with real-valued tuning parameters which determine the accuracy of the numerical algorithm. A prominent example is finite element analysis with its mesh density as the tuning parameter. The aim of this work is to integrate computer outputs with different tuning parameters.
Novel nonstationary Gaussian process models are proposed to establish a framework consistent with the results in numerical analysis. Numerical studies show the advantages of the proposed method over existing methods. The methodology is illustrated with a problem in casting simulation. The paper will appear in Technometrics 2014.

2. Some General Properties of Multi-State Physical Models
Paolo Rocchi (IBM & LUISS University, Italy), Gurami Sh. Tsitsiashvili (Far Eastern Branch of Russian Acad. Science, Russia)

Abstract: The present contribution centers on the physical models of the stochastic system, in particular we investigate the general properties of functioning and repair/maintenance states of systems. Each macro-state has a number of substates that assume different patterns. We depict artificial systems with a linear pattern, and biological systems with a mesh patter. The behavior of each pattern, calculated by means of the Boltzmann-like entropy, is consistent with empirical data. Moreover the present work focuses on the reparability function – derived by the Boltzmann-like entropy – which describes common features of repairable systems.

3. Assessing Water Cooling System Performance: L_z-transform Method
Ilia Frenkel (SCE - Shamoon College of Engineering, Israel), Anatoly Lisnianski (The Israel Electric Corporation Ltd., Israel), Lev Khvatskin, Svetlana Daichman (SCE - Shamoon College of Engineering, Israel)

Abstract: Modern high-tech medical equipment requires precise temperature control and effective cooling, which allow medical equipment to be operated for longer periods and increased in availability of the equipment to patients. This paper presents the application of the L_z-transform method to assessing cooling performance of aging multi-state cooling system for MRI equipment. Straightforward Markov method applied to solve this problem will require building of a system model with numerous numbers of states and solving a corresponding system of multiple differential equations. L_z-transform method, which is used for assessing of the system performance for this cooling system, drastically simplified the solution.

4. Genetic Algorithm and Data Mining Techniques for Design Selection in Databases
Christos Koukouvinos, Christina Parpoula (National Technical University of Athens, Greece), Dimitris E. Simos (SBA Research, Austria)

Abstract: Nowadays, variable selection is fundamental to large dimensional statistical modelling problems, since large databases exist in diverse fields of science. In this paper, we benefit from the use of data mining tools and experimental designs in databases in order to select the most relevant variables for classification in regression problems in cases where observations and labels of a real-world dataset are available. Specifically, this study is of particular interest to use health data to identify the most significant variables containing all the necessary important information for classification and prediction of new data with respect to a certain effect (survival or death). The main goal is to determine the most important variables using methods that arise from the field of design of experiments combined with algorithmic concepts derived from data mining and metaheuristics. Our approach seems promising, since we are able to retrieve an optimal plan using only 6 runs of the available 8862 runs.

5. Statistical Inference for Multi-state Systems: The Weibull Case
Andreas Makrides, Alex Karagrigoriou (University of Cyprus & University of the Aegean, Greece)

Abstract: Markov processes are widely used for reliability analysis because the number of failures in arbitrary time intervals in many practical cases can be described as a Poisson process and the time up to the failure and repair time are often exponentially distributed. In this work we focus on the estimation of both the intensity rates and transition probabilities via output performance observations using as an alternative distribution, the well known Weibull distribution.

HCI-KDD I – Special Session on Human-Computer Interaction & Knowledge Discovery

Session Chair: Massimo Ferri (University of Bologna, Italy)

Location: Lecture Hall D

1. Human–Computer Interaction & Knowledge Discovery (HCI-KDD): What is the benefit of bringing those two fields to work together?
Andreas Holzinger (Medical University Graz & Graz University of Technology, Austria)

Abstract: A major challenge in our networked world is the increasing amount of data, which require efficient and user-friendly solutions. A timely example is the biomedical domain: the trend towards personalized medicine has resulted in a sheer mass of the generated (-omics) data. In the life sciences domain, most data models are characterized by complexity, which makes manual analysis very time-consuming and frequently practically impossible. Computational methods may help; however, we must acknowledge that the problem-solving knowledge is located in the human mind and – not in machines. A strategic aim to find solutions for data intensive problems could lay in the combination of two areas, which bring ideal pre-conditions: Human–Computer Interaction (HCI) and Knowledge Discovery (KDD). HCI deals with questions of human perception, cognition, intelligence, decision-making and interactive techniques of visualization, so it centers mainly on supervised methods. KDD deals mainly with questions of machine intelligence and data mining, in particular with the development of scalable algorithms for finding previously unknown relationships in data, thus centers on

automatic computational methods. A proverb attributed perhaps incorrectly to Albert Einstein illustrates this perfectly: “Computers are incredibly fast, accurate, but stupid. Humans are incredibly slow, inaccurate, but brilliant. Together they may be powerful beyond imagination”. Consequently, a novel approach is to combine HCI & KDD in order to enhance human intelligence by computational intelligence.

2. Making sense of Open Data Statistics with Information from Wikipedia

Daniel Hienert, Dennis Wegener, Siegfried Schomisch (GESIS – Leibniz Institute for the Social Sciences, Germany)

Abstract: Today, more and more open data statistics are published by governments, statistical offices and organizations like the United Nations, The World Bank or Eurostat. This data is freely available and can be consumed by end users in interactive visualizations. However, additional information is needed to enable laymen to interpret these statistics in order to make sense of the raw data. In this paper, we present an approach to combine open data statistics with historical events. In a user interface we have integrated interactive visualizations of open data statistics with a timeline of thematically appropriate historical events from Wikipedia. This can help users to explore statistical data in several views and to get related events for certain trends in the timeline. Events include links to Wikipedia articles, where details can be found and the search process can be continued. We have conducted a user study to evaluate if users can use the interface intuitively, if relations between trends in statistics and historical events can be found and if users like this approach for their exploration process.

3. Active Learning Enhanced Document Annotation for Sentiment Analysis

Peter Koncz, Ján Paralič (Technical University of Košice, Slovak Republic)

Abstract: Sentiment analysis is a popular research area devoted to methods al-lowing automatic analysis of the subjectivity in textual content. Many of these methods are based on the using of machine learning and they usually depend on manually annotated training corpora. However, the creation of corpora is a time-consuming task, which leads to necessity of methods facilitating this process. Methods of active learning, aimed at the selection of the most informative examples according to the given classification task, can be utilized in order to increase the effectiveness of the annotation. Currently it is a lack of systematical research devoted to the application of active learning in the creation of corpora for sentiment analysis. Hence, the aim of this work is to survey some of the active learning strategies applicable in annotation tools used in the context of sentiment analysis. We evaluated compared strategies on the domain of product reviews. The results of experiments confirmed the increase of the corpus quality in terms of higher classification accuracy achieved on the test set for most of the evaluated strategies (more than 20% higher accuracy in comparison to the random strategy).

4. On Graph Entropy Measures for Knowledge Discovery from Publication Network Data

Andreas Holzinger, Bernhard Ofner, Christof Stocker (Medical University Graz, Austria), André Calero Valdez, Anne Kathrin Schaar, Martina Ziefle (Human-Computer Interaction Center, Germany), Matthias Dehmer (UMIT Tyrol, Austria)

Abstract: Many research problems are extremely complex, making interdisciplinary knowledge a necessity; consequently cooperative work in mixed teams is a common and increasing research procedure. In this paper, we evaluated information-theoretic network measures on publication networks. For the experiments described in this paper we used the network of excellence from the RWTH Aachen University, described in [1]. Those measures can be understood as graph complexity measures, which evaluate the structural complexity based on the corresponding concept. We see that it is challenging to generalize such results towards different measures as every measure captures structural information differently and, hence, leads to a different entropy value. This calls for exploring the structural interpretation of a graph measure [2] which has been a challenging problem.

RISI I – Resilience and Privacy – 3rd International Workshop on Resilience and IT-Risk in Social Infrastructures

Session Chair: Isao Echizen (National Institute of Informatics, Japan)
Location: Lecture Hall E

1. Invited Keynote – Social Issues of Big Data and Cloud: Privacy, Confidentiality, and Public Utility

Koichiro Hayashi (Institute of Information Security, Yokohama, Japan)

Abstract: Business people and academia are now excited about Big Data and Cloud Computing as the new and most innovative means for enhancing productivity and customer satisfaction. Simultaneously, there are strong concerns about privacy not only among privacy advocates but among consumers in general, and how to strike a right balance is the main theme in every field of science. However, it is quite strange that very little attention has been paid to the concept of confidentiality, which must be the core element of privacy. This paper first tries to analyze the following two dichotomies as a basis for possible policy considerations: (1) privacy approach in the United States versus confidentiality approach in the United Kingdom, though they share the same common law tradition, and (2) clear demarcation between Information Service and Telecommunications in the United States, dating back to the Computer Inquiry in the 1970s.
This paper also analyzes the features of the Cloud and discusses the possibility of treating it as a new type of Public Utility, namely Information Utility. This hypothesis should be rejected, because there are crucial differences in market structures, regardless of clear similarities in service features. Instead, this paper emphasizes the necessity of protecting confidentiality as an industrial norm.
Taking into account the long tradition of free market for computing industries, self-regulation is basically preferable to government regulation. But from a different viewpoint of “nudge”, a hybrid combination of libertarianism and paternalism, this paper concludes by proposing five short recommendations including fair contract terms as well as unbundling confidentiality from privacy.

2. Estimating the Value of Personal Information with SNS Utility

Memiko Otsuki (The Graduate University for Advanced Studies, Japan), Noboru Sonehara (National Institute of Informatics, Japan)

Abstract: Along with the dramatic growth in the use of the Internet, online services such as social networking sites have become more and more popular and sophisticated. However, at the same time, the collection of life-log data, and in particular the use of this collected personal information, has widely raised public concern regarding privacy protection. In this study, we divide personal information into three categories and find that people are more sensitive about their personal identifiers than other types of information such as demographic information or preferences. We also attempt to measure the value compatibility with online services by using survey questions that ask online users how much they are willing to pay to protect (limited disclosure or complete non-disclosure) their personal information. The responses revealed that people are willing to shoulder the cost to keep using online services if they think the service is attractive enough.

3. Anonymizing Face Images by Using Similarity-Based Metric

Tomoya Muraki, Shintaro Oishi, Masatsugu Ichino (University of Electro-Communications, Japan), Isao Echizen (National Institute of Informatics, Japan), Hiroshi Yoshiura (University of Electro-Communications, Japan)

Abstract: Vast numbers of face images are posted and circulated daily on social network and photo-sharing sites. Some face images are linked to the person’s name, like those on user profile pages, while others are anonymized due to privacy concerns. If an anonymized face image is linked to a named one, that person’s privacy is infringed. One way to overcome this privacy problem is to anonymize face images when they are posted on social networks. However, current face anonymization methods fail to meet two key requirements: being provably secure against deanonymization and enabling users to control the trade-off between security and usability (similarity to the original face) of the anonymized face images. We are developing a similarity-based method for face anonymization that meets both requirements in those cases where a new face image of a person is to be posted when many face images including those of that person are already posted. The basic idea is to hide the new face image in s face images that are equally similar to the face image of the same person. We theoretically demonstrated that the probability of an attacker correctly linking the anonymized face image to an image of the same person is less than 1/s. We also showed theoretically and confirmed experimentally, with 150 sample face images, that the larger the

s, the less usable the anonymized face image. The security of our method holds in spite of future improvements in face recognition tools.

10:30 – 11:00 Coffee Break

11:00 – 12:30 Parallel Sessions

Tutorial

Location: Lecture Hall A

Challenges in Data Protection - Privacy by Design (Part II)

Stefan Katzenbeisser, TU Darmstadt & CASED, Germany

SeCIHD II – Cyber Security and Dependability II – 3rd International Workshop on Security and Cognitive Informatics for Homeland Defense

Session Chair: Aniello Castiglione (University of Salerno, Italy)

Location: Lecture Hall B

1. Dependency Analysis for Critical Infrastructure Security Modelling: A Case Study within the Grid'5000 Project

   Thomas Schaberreiter (University of Luxembourg & CRP Henri Tudor, Luxembourg & University of Oulo, Finland), Sébastien Varrette, Pascal Bouvry (University of Luxembourg, Luxembourg), Juha Röning (University of Oulo, Finland), Djamel Khadraoui (CRP Henri Tudor, Luxembourg)

   Abstract: Critical infrastructure (CI) services (like electricity, telecommunication or transport) are constantly consumed by the society and are not expected to fail. A common definition states that CIs are so vital to our society that a disruption would have a severe impact on both the society and the economy. CI security modelling was introduced in previous work to enable on-line risk monitoring in CIs that depend on each other by exchanging on-line risk alerts expressed in terms of a breach of Confidentiality, a breach of Integrity and degrading Availability (CIA). One important aspect for the accuracy of the model is the decomposition of CIs into CI security modelling elements (CI services, base measurements and dependencies). To assist in CI decomposition and provide more accurate results a methodology based on dependency analysis was presented in previous work.
   In this work a proof-of-concept validation of the CI decomposition methodology is presented. We conduct a case study in the context of the Grid'5000 project, an academic computing grid with clusters distributed at several locations in France and Luxembourg. We show how a CI security model can be established by following the proposed CI decomposition methodology and we provide a discussion of the resulting model as well as experiences during the case study.

2. How to Estimate a Technical VaR Using Conditional Probability, Attack Trees and a Crime Function

   Wolfgang Boehmer (Technische Universität Darmstadt, Germany)

   Abstract: According to the Basel II Accord for banks and Solvency II for the insurance industry, not only should the market and financial risks for the institutions be determined, also the operational risks (opRisk). In recent decades, Value at Risk (VaR) has prevailed for market and financial risks as a basis for assessing the present risks. Occasionally, there are suggestions as to how the VaR is to be determined in the field of operational risk. However, existing proposals can only be applied to an IT infrastructure to a certain extent, or to parts of them e.g. such as VoIP telephony. In this article, a proposal is discussed to calculate a technical Value at Risk (t-VaR). This proposal is based on risk scenario technology and uses the conditional probability of the Bayes theorem. The vulnerabilities have been determined empirically for an insurance company in 2012. To determine the threats, attack trees and threat actors are used. The attack trees are weighted by a function that is called the criminal energy. To verify this approach the t-VaR was calculated for VoIP telephony for an insurance company. It turns out that this method

achieves good and sufficient results for the IT infrastructure as an effective method to meet the Solvency II's requirements.

3. Using Probabilistic Analysis for the Certification of Machine Control Systems
Atif Mashkoor (Software Competence Center Hagenberg, Austria), Osman Hasan (National University of Sciences and Technology, Pakistan), Wolfgang Beer (Software Competence Center Hagenberg, Austria)

Abstract: Traditional testing techniques often reach their limits when employed for the assessment of critical Machine Control Systems as they contain a large amount of random and unpredictable components. The probabilistic analysis approach can assist in their evaluation by providing a subjective evidence of their safety and reliability. The synergy of probabilistic analysis and expressiveness of higher-order logic theorem proving results into convincing modelling and reasoning of several stringent safety cases that contribute towards the certification of high-assurance systems.

4. Experimental Investigation in the Impact on Security of the Release Order of Defensive Algorithms
Suliman A. Alsuhibany, Ahmad Alonaizi, Charles Morisset, Chris Smith, Aad van Moorsel (Newcastle University, UK)

Abstract: In the practical use of security mechanisms such as CAPTCHAs and spam filters, attackers and defenders exchange 'victories,' each celebrating (temporary) success in breaking and defending. While most of security mechanisms rely on a single algorithm as a defense mechanism, we propose an approach based on a set of algorithms as a defense mechanism. When studying sets of algorithms various issues arise about how to construct the algorithms and in which order or in which combination to release them. In this paper, we consider the question of whether the order in which a set of defensive algorithms is released has a significant impact on the time taken by attackers to break the combined set of algorithms. The rationale behind our approach is that attackers learn from their attempts, and that the release schedule of defensive mechanisms can be adjusted so as to impair that learning process. This paper introduces this problem. We show that our hypothesis holds for an experiment using several simplified but representative spam filter algorithms—that is, the order in which spam filters are released has a statistically significant impact on the time attackers take to break all algorithms.

MoCrySEn I – Opening & Invited Talk – 2nd International Workshop on Modern Cryptography and Security Engineering

Session Chair: Dimitris E. Simos (SBA Research, Austria)

Location: Lecture Hall C

1. Invited Talk – Computing Platforms and Cryptography: Advances and Challenges
Tim Güneysu (Ruhr-University Bochum, Germany)

Abstract: *The complexity of modern cryptographic systems often demands for a powerful computation platform - what often increases the overall system cost significantly. Apparently, this raises the question which platform is the most efficient and cheapest one in the context of a specific cryptosystem. This invited talk highlights the requirements of modern cryptosystems with respect to the special features offered by contemporary processors and hardware circuits. Besides an examplary discussion on the optimal platform for the AES block cipher based on the wealth of available performance data, this talk includes an outlook on the efficient implementation of latest cryptosystems, such as code-based and lattice-based cryptography.*

2. Discussion Topics for Modern Cryptography and Security Engineering

HCI-KDD II – Special Session on Human-Computer Interaction & Knowledge Discovery

Session Chair: Andreas Holzinger (Medical University Graz, Austria)

Location: Lecture Hall D

1. Visualization Support for Multi-Criteria Decision Making in Geographic Information Retrieval
   Chandan Kumar (University of Oldenburg, Germany), Wilko Heuten (OFFIS - Institute for Information Technology, Germany), Susanne Boll (University of Oldenburg, Germany)

   Abstract: The goal of geographic information retrieval (GIR) is to provide information about geo-entities to end-users and assist their spatial decision making. In the current means of GIR interfaces, users could easily visualize the geo-entities of interest on a map interface via sequential querying or browsing of individual categories. However, there are several decision making scenarios when the user needs to explore and investigate the geospatial database with multiple criteria of interests, which is not well supported by the sequential querying or browsing functionality of current GIR interfaces. There is a need for more sophisticated visual interfaces to enable end-users in discovering knowledge hidden in multi-dimensional geospatial databases. In this paper we discuss some of the HCI issues in realizing such multi-criteria decision making scenario based on the user requirement analysis. To tackle the human centered aspects we propose different heatmap based interfaces to support multi-criteria visualizations in GIR, i.e., to facilitate the knowledge based exploration of geospatial databases with less information overload.

2. Immersive Interactive Information Mining with Application to Earth Observation Data Retrieval
   Mohammadreza Babaee, Gerhard Rigoll (Technische Universität München Germany), Mihai Datcu (German Aerospace Center, Germany)

   Abstract: The exponentially increasing amount of Earth Observation (EO) data requires novel approaches for data mining and exploration. Visual analytic systems have made valuable contribution in understanding the structure of data by providing humans with visual perception of data. However, these systems have limitations in dealing with large-scale high-dimensional data. For instance, the limitation in dimension of the display screen prevents visualizing high-dimensional data points. In this paper, we propose a virtual reality based visual analytic system, so called *Immersive Information Mining*, to enable knowledge discovery from the EO archive. In this system, Dimension Reduction (DR) techniques are applied to high-dimensional data to map into a lower-dimensional space to be visualized in an immersive 3D virtual environment. In such a system, users are able to navigate within the data volume to get visual perception. Moreover, they can manipulate the data and provide feedback for other processing steps to improve the performance of data mining system.

3. Transfer Learning for Content-Based Recommender Systems Using Tree Matching
   Naseem Biadsy, Lior Rokach, Armin Shmilovici (Ben-Gurion University, Israel)

   Abstract: In this paper we present a new approach to content-based transfer learning for solving the data sparsity problem in cases when the users' preferences in the target domain are either scarce or unavailable, but the necessary information for the preferences exists in another domain. Training a system to use such information across domains is shown to produce better performance. Specifically, we represent users' behavior patterns based on topological graph structures. Each behavior pattern represents the behavior of a set of users, when the users' behavior is defined as the items they rated and the items' rating values. In the next step, a correlation is found between behavior patterns in the source domain and target domain. This mapping is considered a bridge between the two. Based on the correlation and content-attributes of the items, a machine learning model is trained to predict users' ratings in the target domain. When our approach is compared to the popularity approach and KNN-cross-domain on a real world dataset, the results show that our approach outperforms both methods on an average of 83%.

4. Mobile Movie Recommendations with Linked Data
   Vito Claudio Ostuni, Giosia Gentile, Tommaso Di Noia, Roberto Mirizzi, Davide Romito, Eugenio Di Sciascio (Polytechnic University of Bari, Italy)

   Abstract: The recent spread of the so called Web of Data has made available a vast amount of interconnected data, paving the way to a new generation of ubiquitous applications able to exploit the information encoded in it. In this

paper we present Cinemappy, a location-based application that computes contextual movie recommendations. Cinemappy refines the recommendation results of a content-based recommender system by exploiting contextual information related to the current spatial and temporal position of the user. The content-based engine leverages graph information within DBpedia, one of the best-known datasets publicly available in the Linked Open Data (LOD) project.

RISI II – Resilience and Safety – 3rd International Workshop on Resilience and IT-Risk in Social Infrastructures

Session Chair: Sven Wohlgemuth (TU Darmstadt & CASED, Germany)

Location: Lecture Hall E

1. ICHIGAN Security – A Security Architecture that Enables Situation-Based Policy Switching
   Hiroshi Maruyama (The Research Organization of Information and Systems, Japan), Kiyoshi Watanabe (Microsoft Services, Japan), Sachiko Yoshihama, Naohiko Uramoto (IBM Research Tokyo, Japan), Yoichiro Takehora (Keynote Systems, Inc., Japan), Kazuhiro Minami (The Research Organization of Information and Systems, Japan)

   Abstract: Project ICHIGAN is a voluntary-based attempt to build a reference IT architecture for local governments that can withstand large-scale natural disasters. This architecture is unique in that 1) it has the concept of phases of the situation for which different priorities on non-functional requirements are applied, and 2) the functionalities and services provided by the IT systems in the suffered area will be taken over by those of the “coupled” local government. These features pose specific challenges on the information security policy, especially because different policies need to be applied for the different modes. This paper describes two key elements to enable the policy; policy templates and deferred authentication.

2. Using Twitter’s Mentions for Efficient Emergency Message Propagation
   Kelly Y. Itakura, Noboru Sonehara (National Institute of Informatics, Japan)

   Abstract: Using social media such as Twitter for emergency message propagation in times of crisis is widely thought to be a good addition to other traditional emergency population warning systems such as televisions. At the same time, most studies on Twitter influence propagation focus on retweetability of tweets. In this paper, we propose the importance of Twitter’s mention function as another method of message propagation. Specifically, we show that graphs constructed from Twitter’s retweet, mention, and reply functions show structural differences suggesting that using the mention function is the most efficient method of reaching the mass audience. Moreover, we show that influencers are the most prominent on the mention graph. From these analysis we conclude that we need further research in the direction of non-traditional methods of population warning systems. Further, this is the first paper that characterizes the structural differences of the retweet/mention/reply graphs in Twitter.

3. Towards a Risk based Assessment of QoS Degradation for Critical Infrastructure
   Moussa Ouedraogo (Public Research Center Henri Tudor, Luxembourg), Manel Khodja (USTHB, Algeria), Djamel Khadraoui (Public Research Center Henri Tudor, Luxembourg)

   Abstract: In this paper, we first present an attack-graph based estimation of security risk and its aggregation from lower level components to an entire service. We then presents an initiative towards appreciating how the quality of service (QoS) parameters of a service may be affected as a result of fluctuations in the cyber security risk level. Because the service provided by critical infrastructure is often vital, providing an approach that enables the operator to foresee any QoS degradation as a result of a security event is paramount. We provide an illustration of the risk estimation approach along with a description of an initial prototype developed using a multi-agent platform.

Tutorial

Location: Lecture Hall F

Secure Enterprise – wide Identity Management and Role Modeling

Ludwig Fuchs (University of Regensburg, Germany)

Abstract: In today's increasingly open business environment companies provide access to resources to a greater number of users, and more heterogeneous types of users, than ever before. As a result of improper account management users accumulate a number of excessive rights over time, resulting in the so called identity chaos. Studies show that major security problems and compliance violations arise because of employees gaining unauthorized access to resources as a result of manually handling user accounts. Role-based Identity Management has become a means to solve the identity chaos. It is concerned with the storage, administration, and usage of digital identities during their lifecycle in the organization. Roles acting as intermediary between employees and their access rights are an essential element of IdM.
They allow organizations to ease and secure provisioning processes, i.e. the allocation of digital and non-digital assets to employees, and access to resources.

The tutorial motivates the benefits and challenges of role-based Identity Management within enterprises by focusing on the task of role modeling, i.e. the definition of suitable business roles for employees. It provides detailed information about into current research trends and bridges the gap to practical usage in industry projects by giving insight into a tool-supported methodology for cleansing identity-related data and modeling business roles.

12:30 – 14:00 Lunch

14:00 – 14:30 Opening ARES / CD-ARES Conference

Location: Lecture Hall A

- Prof. Günther Pernul (*Universität Regensburg, Germany)*
  - Program Committee Co-Chair & Local Host ARES 2013
- Dr. Edgar Weippl *(Vienna University of Technology and SBA Research, Austria)*
- Prof. Dr. A Min Tjoa *(Vienna University of Technology and SBA Research, Austria)*

14:30 – 16:00 ARES I – ARES BEST PAPER Session – 8th International Conference on Availability, Reliability and Security

Session Chair: Edgar Weippl (SBA Research, Austria)

Location: Lecture Hall A

1. Laribus: Privacy-Preserving Detection of Fake SSL Certificates with a Social P2P Notary Network
   Andrea Micheloni, Karl-Peter Fuchs, Dominik Herrmann, Hannes Federrath (University of Hamburg, Germany)

   Abstract: In this paper we present Laribus, a peer-to-peer network designed to detect local man-in-the-middle attacks against SSL/TLS. With Laribus clients can validate the authenticity of a certificate presented to them by retrieving it from different vantage points on the network. Unlike previous solutions, clients do not have to trust a central notary service, nor do they have to rely on the cooperation of website owners. The Laribus network is based on a Social Network graph, which allows users to form Notary Groups that improve both privacy and availability. It integrates several well-known techniques, such as secret sharing, ring signatures, layered encryption, range queries and a Distributed Hash Table (DHT), to achieve privacy-aware queries, scalability and decentralization. We present the design and core components of Laribus, discuss its security properties and also provide results from a simulation-based feasibility study.

2. Reliability Prediction for Component-Based Software Systems with Architectural-Level Fault Tolerance Mechanisms
Thanh-Trung Pham, Xavier Défago (Japan Advanced Institute of Science and Technology (JAIST), Japan)

Abstract: This paper extends the core model of a recent component-based reliability prediction approach to offer an explicit and flexible definition of reliability-relevant behavioral aspects (i.e. error detection and error handling) of software fault tolerance mechanisms, and an efficient evaluation of their reliability impact in the dependence of the whole system architecture and usage profile. Our approach is validated with the reporting service of a document exchange server, by modeling the reliability, conducting a reliability prediction and sensitivity analyses, and demonstrating its ability to support design decisions.

3. A Statistical Approach for Fingerprinting Probing Activities
Elias Bou-Harb, Mourad Debbabi, Chadi Assi (NCFTA & Concordia University, Canada)

Abstract: Probing is often the primary stage of an intrusion attempt that enables an attacker to remotely locate, target, and subsequently exploit vulnerable systems. This paper attempts to investigate whether the perceived traffic refers to probing activities and which exact scanning technique is being employed to perform the probing. Further, this work strives to examine probing traffic dimensions to infer the 'machinery' of the scan; whether the probing activity is generated from a software tool or from a worm/botnet and whether the probing is random or follows a certain predefined pattern. Motivated by recent cyber attacks that were facilitated through probing, limited cyber security intelligence related to the mentioned inferences and the lack of accuracy that is provided by scanning detection systems, this paper presents a new approach to fingerprint probing activity. The approach leverages a number of statistical techniques, probabilistic distribution methods and observations in an attempt to understand and analyze probing activities. To prevent evasion, the approach formulates this matter as a change point detection problem that yielded motivating results. Evaluations performed using 55 GB of real darknet traffic shows that the extracted inferences exhibit promising accuracy and can generate significant insights that could be used for mitigation purposes.

16:00 – 16:30 Coffee Break

16:30 – 18:00 Parallel Sessions

ARES II – Risk Management & Security Models – 8th International Conference on Availability, Reliability and Security

Session Chair: David Chadwick (University of Kent, UK)
Location: Lecture Hall A

1. Reputation-Controlled Business Process Workflows
Benjamin Aziz (University of Portsmouth, UK), Geoff Hamilton (Dublin City University, Ireland)

Abstract: This paper presents a model solution for controlling the execution of BPEL business processes based on reputation constraints at the level of the services, the service providers and the BPEL workflow. The reputation constraints are expressed as part of an SLA and are then enforced at runtime by a reputation monitoring system. We use our model to demonstrate how trust requirements based on such reputation constraints can be upheld in a real world example of a distributed map processing defined as a BPEL workflow.

2. Conflict Management in Obligation with Deadline Policies
Nada Essaouini (Télécom Bretagne, France & Cadi Ayyad University, ENSA of Marrakesh) Frédéric Cuppens, Nora Cuppens-Boulahia (Télécom Bretagne, France), Anas Abou El Kalam (Cadi Ayyad University, ENSA of Marrakesh)

Abstract: A security policy defines the rules to ensure the security properties of an information system. These rules are often expressed as permissions, prohibitions and obligations which could lead to conflicting situations.We are interested in this work in managing conflict between obligations with deadlines. We define a process based on the situation calculus to provide a plan of actions, when it exists, which fulfills all obligations in their deadlines. To

illustrate our approach, we take an example of obligation rules with deadline concerning completion of patient medical records.

3. Federated Identity Management and Usage Control - Obstacles to Industry Adoption
Jostein Jensen, Åsmund Ahlmann Nyre (Norwegian University of Science and Technology, Norway)

Abstract: Federated identity management and usage control technologies have received considerable attention from the research community during the past decade. We have investigated the views of, and attitudes towards, adopting federated identity management and usage control technologies in the oil and gas industry in Norway through two case studies. Although the industry combines extensive inter-organisational collaboration and information sharing with high demands for security, the adoption is thus far low. In this paper we review the results of the case studies jointly and attempt to give an industry-view on the obstacles to adoption. Further, we propose a set of strategies to overcome the obstacles and improve the rate of adoption. More empirical research should be carried out to complement the views put forth in this paper, and to supplement the suggested strategies to facilitate technology adoption.

CD-ARES I – Economic, ethical, legal, multilingual, organizational and social aspects – International Cross Domain Conference and Workshop

Location: Lecture Hall B

1. Sensor Data Meets Social Networks - Reflecting on Benefits in the Case of a Patient Room
Fabienne Kuhn, Andreas Spichiger, Reinhard Riedl (Bern University of Applied Sciences, Switzerland)

Abstract: In a hospital, information exchange is essential to save lives and to prevent life endangering mistakes. Information exchange is supported by a hospital information system (HIS). From a theoretical perspective, the deployment of an HIS is promising because it reduces errors and duplication of information. In practice, however, there are some major problems concerning the usage of such a system. One way to deal with these problems is introduced in this paper: the integration of sensor data into social media. The paper concentrates on the conceptual benefits and risks such an integration may generate. It focuses on the case of a patient room.

2. Older users' wish list for technology attributes. A comparison of household and medical technologies
Simon Himmel, Martina Ziefle, Chantal Lidynia (RWTH Aachen University, Germany), Andreas Holzinger (Medical University Graz, Austria)

Abstract: Facing the increasing user diversity and broad diffusion of technology in work-related and private contexts, the sensible tailoring of technology functionalities, attributes, and interfaces – with reference to the requirements and needs of users – is a key prerequisite of a successful rollout and broad acceptance of technologies. However, user diversity and the specific using contexts of technologies have not been sufficiently researched yet. In this study, we examine the wish list regarding attributes for different technologies in a wide age range. Using qualitative and quantitative methodologies, we explored the different specifications for household and medical devices and assessed which attributes users expect for each of the two different technology types. Exploring user diversity, we analyzed effects of age, gender, and health status on the perception of technology requirements. Results show that not only user diversity but also the specific technology type present as critical factors in the definition of proper attributes of technology. The findings may be useful for humancentered product development.

3. Evaluating the Energy Efficiency of OLTP operations: A case study on PostgreSQL
Raik Niemann (University of Applied Science Hof & Goethe University Frankfurt, Germany), Nikolaos Korfiatis, Roberto Zicari (Goethe University Frankfurt, Germany), Richard Göbel (University of Applied Science Hof, Germany)

Abstract: With the continuous increase of online services as well as energy costs, energy consumption becomes a significant cost factor for the evaluation of data center operations. A significant contributor to that is the performance of database servers which are found to constitute the backbone of online services. From a software approach, while a set of novel data management technologies appear in the market e.g. key-value based or in-memory databases, classic relational database management systems (RDBMS) are still widely used. In addition

from a hardware perspective, the majority of database servers is still using standard magnetic hard drives (HDDs) instead of solid state drives (SSDs) due to lower cost of storage per gigabyte, disregarding the performance boost that might be given due to high cost.
In this study we focus on a software based assessment of the energy consumption of a database server by running three different and complete database workloads namely TCP-H, Star Schema Benchmark -SSB as well a modified benchmark we have derived for this study called W22. We profile the energy distribution among the most important server components and by using different resource allocation we assess the energy consumption of a typical open source RDBMS (PostgreSQL) on a standard server in relation with its performance (measured by query time). Results confirm the well-known fact that even for complete workloads, optimization of the RDBMS results to lower energy consumption.

MoCrySEn II – Symmetric-Key Cryptography (Modern Cryptography Track) – 2nd International Workshop on Modern Cryptography and Security Engineering

Session Chair: Tim Güneysu (Ruhr-University Bochum, Germany)
Location: Lecture Hall C

1. Differential Cryptanalysis and Boomerang Cryptanalysis of LBlock

Jiageng Chen, Atsuko Miyaji (Japan Advanced Institute of Science and Technology, Japan)

Abstract: LBlock is a lightweight block cipher proposed in ACNS 2011. It has a 64-bit block size and 80-bit key size which is the typical parameter setting accepted by most of the recent proposed lightweight block ciphers. It has fast hardware implementation efficiency and it still remains rather secure considering the recent results and the security margin it provides. In this paper, we investigate the differential behavior of the cipher in detail and propose (multiple) differential attack and boomerang attack against it. We are able to construct 15-round multiple differential paths which can lead to 17-round attack with complexity as low as $2^{67.52}$. Also 16-round boomerang distinguisher can be build which leads us to 18-round boomerang (rectangle) attack with complexity $2^{70.8473}$. These are the best differential attacks for LBlock in the single key scenario, which helps us understanding the differential behavior of the cipher.

2. Information-Theoretically Secure Aggregate Authentication Code: Model, Bounds, and Constructions

Asato Kubai, Junji Shikata, Yohei Watanabe (Yokohama National University, Japan)

Abstract: In authentication schemes where many users send authenticated messages to a receiver, it is desirable to aggregate them into a single short authenticated message in order to reduce communication complexity. In this paper, in order to realize such a mechanism in information-theoretic security setting, we first propose aggregate authentication codes. Specifically, we newly propose a model and a security definition for aggregate authentication codes. We also show tight lower bounds on sizes of entities' secret-keys and (aggregated) tags. Furthermore, we present optimal (i.e., most efficient) constructions for aggregate authentication codes.

3. On Constructions of MDS Matrices from Companion Matrices for Lightweight Cryptography

Kishan Chand Gupta, Indranil Ghosh Ray (Indian Statistical Institute, India)

Abstract: Maximum distance separable (MDS) matrices have applications not only in coding theory but also are of great importance in the design of block ciphers and hash functions. It is highly nontrivial to find MDS matrices which could be used in lightweight cryptography. In a crypto 2011 paper, Guo et. al. proposed a new MDS matrix $Serial(1, 2, 1, 4)^4$ over F_2^8. This representation has a compact hardware implementation of the AES MixColumn operation. No general study of MDS properties of this newly introduced construction of the form $Serial(z_0,..., zd\text{-}1)^d$ over F_{2n} for arbitrary d and n is available in the literature. In this paper we study some properties of MDS matrices and provide an insight of why $Serial(z_0,..., z_{d\text{-}}1)^d$ leads to an MDS matrix. For efficient hardware implementation, we aim to restrict the values of z_i's in $\{1, \alpha, \alpha^2, \alpha + 1\}$, such that $Serial(z_0,..., z_{d\text{-}}1)^d$ is MDS for $d = 4$ and 5, where α is the root of the constructing polynomial of F_{2n}. We also propose more generic constructions of MDS matrices e.g. we construct lightweight 4×4 and 5×5 MDS matrices over F_{2n} for all $n \geq 4$. An algorithm is presented to check if a given matrix is MDS. The algorithm follows from the basic properties of MDS matrix and is easy to implement.

FARES I – Session on Organizational Security Aspects (Special OSA Session) – 8th International Workshop on Frontiers in Availability, Reliability and Security

Session Chair: Simon Tjoa, St. Pölten University of Applied Sciences, Austria
Location: Lecture Hall D

1. Organizational Security Architecture for Critical Infrastructure
   Jonathan Blangenois (University of Namur, Belgium & Public Research Centre Henri Tudor, Luxembourg), Guy Guemkam (University of Namur, Belgium & Université de Pierre et Marie Curie, France) Christophe Feltus, Djamel Khadraoui (Public Research Centre Henri Tudor, Luxembourg)

   Abstract: The governance of critical infrastructures requires a fail-safe dedicated security management organization. This organization must provide the structure and mechanisms necessary for supporting the business processes execution, including: decision-making support and the alignment of this latter with the application functions and the network components. Most research in this field focuses on elaborating the SCADA system which embraces components for data acquisition, alert correlation and policy instantiation. At the application layer, one of the most exploited approaches for supporting SCADA is built up on multi-agent system technology. Notwithstanding the extent of existing work, no model allows to represent these systems in an integrated manner and to consider different layers of the organization. Therefore, we propose an innovative version of ArchiMate® for multi-agent purpose with the objective to enrich the agent society collaboration and, more particularly, the description of the agent's behavior. Our work is has been illustrated in the context of a critical infrastructure in the field of a financial acquiring/issuing mechanism for card payments.

2. IT Service Continuity: Achieving Embeddedness through Planning
   Marko Niemimaa, Jonna Järveläinen (University of Turku, Finland)

   Abstract: Business customers and regulations as well as different IT service management frameworks expect that IT services are continuously operating. A service interruption might have severe impact on customer relationships, business, sales or image of the company. Therefore, organisations spend enormous amounts of time in continuity and recovery planning for IT services, and several continuity planning methodologies have been introduced. However, the connection between continuity planning and continuity management is somewhat unclear, and embedding the continuity practices into organisations have not been discussed in detail in planning methodologies. This paper will focus on how IT service continuity planning embeds continuity by reviewing continuity planning methods. The continuity planning practices that influence achieving embeddedness are analysed from qualitative and quantitative data from large organisations operating in Finland. The findings suggest that a number of planning practices support the transition from planning to embeddedness, such as creating awareness, increasing commitment, integrating the continuity practices into organisational processes and learning from incidents.

3. An Approach Based on Model-Driven Engineering to Define Security Policies Using OrBAC
   Denisse Munante, Laurent Gallon, Philippe Aniorté (University of Pau, France)

   Abstract: In the field of access control, many security breaches occur because of a lack of early means to evaluate if access control policies are adequate to satisfy privileges requested by subjects which try to perform actions on objects. This paper proposes an approach based on UMLsec, to tackle this problem. We propose to extend UMLsec, and to add OrBAC elements. In particular, we add the notions of context, inheritance and separation. We also propose a methodology for modeling a security policy and assessing the security policy modeled, based on the use of MotOrBAC. This assessment is proposed in order to guarantee security policies are well-formed, to analyse potential conflicts, and to simulate a real situation.

SecBPM – Workshop on Resilient and Secure BPM - Tackling current Frontiers

Location: Lecture Hall E

1. MERCOR: Security Requirements Structuring / Resilient BMP - Status Quo and Challenges
   Arnt Syring, Thomas Koslowski (University Freiburg, Germany)

2. Requirements and acceptance of secure business processes - first insights from case studies
   Torsten Eymann (University Bayreuth, Germany)

3. IT-Security Audits for SMEs
   Stefan Fenz (Xylem Technologies, Austria)

4. Formalizing Risk- and Compliance-Management
   Stefan Fenz (TU Wien, Austria)

5. Demonstration
   Martin Jurisch (Aristaflow, Germany)

19:30 – 23:00 Mayor's Reception

Tuesday, 03 September 2013

08:00 – 17:30 Registration for all events

09:00 – 10:30 Plenary Session

Keynote

Location: Lecture Hall A

Data Protection in Social Networks: Going Beyond Access Control

Elena Ferrari (DiSTA STRICT SociaLab, University of Insubria, Italy)

Abstract: With the increasing popularity of On-line Social Networks (OSNs), protection of personal information has gained attention in the research community. This has resulted in many proposals, ranging from access control models to tools for privacy settings suggestion. However, none of the research proposals appeared so far nor the privacy settings currently offered by commercial OSNs provides a comprehensive solution to the fundamental issue of unintended information disclosure to a public that can reach up to millions of users. One of the key reasons is that the social web vision requires to deeply rethink access control and privacy enhancing technologies both in terms of models and architectural solutions for their enforcement. In this talk, after an introduction to the problem of data protection in OSNs, we will discuss the most challenging research questions and issues and report preliminary research results.

10:30 – 11:00 Coffee Break

11:00 – 11:20 Parallel Sessions

ARES III – Software Security – 8th International Conference on Availability, Reliability and Security

Location: Lecture Hall A

1. Estimating Software Vulnerabilities A Case Study Based on the Misclassification of Bugs in MySQL Server

   Jason L. Wright, Jason W. Larsen, Miles A. McQueen (Idaho National Laboratory, USA)

   Abstract: Software vulnerabilities are an important part of the modern software economy. Being able to accurately classify software defects as a vulnerability, or not, allows developers and end users to expend appropriately more effort on fixing those defects which have security implications. However, we demonstrate in this paper that the expected number of misclassified bugs (those not marked as also being vulnerabilities) may be quite high and thus human efforts to classify bug reports as vulnerabilities appears to be quite ineffective. We conducted an experiment using the MySQL bug report database to estimate the number of misclassified bugs yet to be identified as vulnerabilities. The MySQL database server versions we evaluated currently have 76 publicly reported vulnerabilities. Yet our experimental results show, with 95% confidence, that the MySQL bug database has between 499 and 587 misclassified bugs for the same software. This is an estimated increase of vulnerabilities between 657% and 772% over the number currently identified and publicly reported in the National Vulnerability Database and the Open Source Vulnerability Database.

2. Validating Security Design Pattern Applications Using Model Testing
Takanori Kobashi (Waseda University, Japan), Nobukazu Yoshioka (GRACE Center, Japan), Takao Okubo (Information Security Division, Japan), Haruhiko Kaiya (Architecture Research Division, Japan), Hironori Washizaki, Yoshiaki Fukazawa (Waseda University, Japan)

Abstract: Software developers are not necessarily security specialists, security patterns provide developers with the knowledge of security specialists. Although security patterns are reusable and include security knowledge, it is possible to inappropriately apply a security pattern or that a properly applied pattern does not mitigate threats and vulnerabilities. Herein we propose a method to validate security pattern applications. Our method provides extended security patterns, which include requirement- and design-level patterns as well as a new model testing process using these patterns. Developers specify the threats and vulnerabilities in the target system during an early stage of development, and then our method validates whether the security patterns are properly applied and assesses whether these vulnerabilities are resolved.

3. PyTrigger: A System to Trigger & Extract User-Activated Malware Behavior
Dan Fleck, Arnur Tokhtabayev, Alex Alarif, Angelos Stavrou (George Mason University, USA) Tomas Nykodym (Binghamton University, USA)

Abstract: We introduce PyTrigger, a dynamic malware analysis system that automatically exercises a malware binary extracting its behavioral profile even when specific user activity or input is required. To accomplish this, we developed a novel user activity record and playback framework and a new behavior extraction approach. Unlike existing research, the activity recording and playback includes the context of every object in addition to traditional keyboard and mouse actions. The addition of the context makes the playback more accurate and avoids dependencies and pitfalls that come with pure mouse and keyboard replay. Moreover, playback can become more efficient by condensing common activities into a single action. After playback, PyTrigger analyzes the system trace using a combination of multiple states and behavior differencing to accurately extract the malware behavior and user triggered behavior from the complete system trace log. We present the algorithms, architecture and evaluate the PyTrigger prototype using 3994 real malware samples. Results and analysis are presented showing PyTrigger extracts additional behavior in 21% of the samples.

4. Isolation of Malicious External Inputs in a Security Focused Adaptive Execution Environment
Aaron Paulos, Partha Pal, Richard Schantz, Brett Benyo (BBN Technologies, USA), David Johnson, Mike Hibler, Eric Eide (University of Utah, USA)

Abstract: Reliable isolation of malicious application inputs is necessary for preventing the future success of an observed novel attack after the initial incident. In this paper we describe, measure and analyze, Input-Reduction, a technique that can quickly isolate malicious external inputs that embody unforeseen and potentially novel attacks, from other benign application inputs. The Input-Reduction technique is integrated into an advanced, security-focused, and adaptive execution environment that automates diagnosis and repair. In experiments we show that Input-Reduction is highly accurate and efficient in isolating attack inputs and determining casual relations between inputs. We also measure and show that the cost incurred by key services that support reliable reproduction and fast attack isolation is reasonable in the adaptive execution environment.

CD-ARES II – Context-Oriented Information Integration I – International Cross Domain Conference and Workshop

Location: Lecture Hall B

1. Chaining Data and Visualization Web Services for Decision Making in Information Systems
Ahmet Sayar (Kocaeli University, Turkey), Marlon E. Pierce (Indiana University, USA)

Abstract: Decision making in information systems increasingly relies on analyses of data in visual formats which are created from distributed heterogeneous data belonging to the separate organizations. This paper presents distributed service architecture for creating and managing the production of knowledge from distributed collections of data sources through integrated data-views. Web Services provide key low level capability but do not define an information or data architecture. These are left to domain specific capabilities metadata and domain specific common data model. Datasets are considered to be defined with domain specific spatial and non-spatial

attributes for displaying and querying. We propose blueprint architecture and define the principles and requirements for general information systems domains.

2. A Fully Reversible Data Transform Technique Enhancing Data Compression of SMILES Data
Shagufta Scanlon, Mick Ridley (University of Bradford, UK)

Abstract: The requirement to efficiently store and process SMILES data used in Chemoinformatics creates a demand for efficient techniques to compress this data. General-purpose transforms and compressors are available to transform and compress this type of data to a certain extent, however, these techniques are not specific to SMILES data. We develop a transform specific to SMILES data that can be used alongside other general-purpose compressors as a pre-processor and post-processor to improve the compression of SMILES data. We test our transform with six other general-purpose compressors and also compare our results with another transform on our SMILES data corpus, we also compare our results with untransformed data.

3. Personalized Web Search Using Emotional Features
Jianwei Zhang (Tsukuba University of Technology, Japan), Katsutoshi Minami, Yukiko Kawai (Kyoto Sangyo University, Japan), Yuhki Shiraishi (Tsukuba University of Technology, Japan), Tadahiko Kumamoto (Chiba Institute of Technology, Japan)

Abstract: Re-ranking and re-retrieval of search results are useful techniques for satisfying users' search intentions, since current search engines cannot always return user-desired pages at the top ranks. In this paper, we propose a system for personalized Web search considering users' emotional aspects. Given a query topic, the system presents the major emotion tendency on this topic that search results returned from search engines are reflecting. The system also enables users to specify the polarities and strengths of their emotions (e.g., happy or sad, glad or angry, peaceful or strained) on this topic and offers a re-ranking list of initial search results based on the similarity of emotions. Particularly, the system can automatically obtain Web pages with minor emotion tendency on the query topic by extracting sub-queries with opposite emotions and conducting a re-retrieval. Experimental evaluations show the re-ranking and the re-retrieval achieve encouraging search results in comparison with initial search results.

MoCrySEn III – Algorithmic Cryptanalysis (Modern Cryptography Track) – 2nd International Workshop on Modern Cryptography and Security Engineering

Session Chair: Nicolas Sendrier (INRIA, France)
Location: Lecture Hall C

1. A Comparison Between Two off-the-Shelf Algebraic Tools for Extraction of Cryptographic Keys from Corrupted Memory Images
Abdel Alim Kamal (Menofia University, Egypt), Roger Zahno, Amr M. Youssef (Concordia University, Canada)

Abstract: Cold boot attack is a class of side channel attacks which exploits the data remanence property of random access memory (RAM) to retrieve its contents which remain readable shortly after its power has been removed. Specialized algorithms have been previously proposed to recover cryptographic keys of several ciphers from decayed memory images. However, these techniques were cipher-dependent and certainly uneasy to develop and fine tune. On the other hand, for symmetric ciphers, the relations that have to be satisfied between the subround key bits in the key schedule always correspond to a set of nonlinear Boolean equations. In this paper, we investigate the use of an off-the-shelf SAT solver (CryptoMiniSat), and an open source Gröbner basis tool (PolyBoRi) to solve the resulting system of equations. We also provide the pros and cons of both approaches and present some simulation results for the extraction of AES and Serpent keys from decayed memory images using these tools.

2. Cryptanalysis of 2-layer Nonlinear Piece In Hand Method
Xuyun Nie (University of Electronic Science and Technology of China, China & Technische Universität Darmstadt, Germany & Chinese Academy of Sciences, China & Network and Data Security Key Laboratory of Sichuan Province, China) Albrecht Petzoldt, Johannes Buchmann (Technische Universität Darmstadt, Germany)

Abstract: Piece in Hand method is a security enhancement method for Multivariate Public Key Cryptosystems (MPKCs). Since 2004, many types of this method have been proposed. In this paper, we consider the 2-layer nonlinear Piece in Hand method as proposed by Tsuji et al. in 2009. The key point of this method is to introduce an invertible quadratic polynomial map on the plaintext variables to construct perturbation of the original MPKC. Through our analysis, we find that the security of the enhanced scheme is mainly relying on the quadratic polynomials of this auxiliary map. The two examples proposed by Tsuji et al. for this map can not resist the Linearization Equation attack. Given a valid ciphertext, we can easily get a public key which is equivalent to the original MPKC. If there is an algorithm that can recover the plaintext corresponding to a valid ciphertext of the original MPKC, we can construct an algorithm that can recover the plaintext corresponding to a valid ciphertext of the enhanced MPKC.

3. On the Security of LBlock against the Cube Attack and Side Channel Cube Attack

Saad Islam, Mehreen Afzal, Adnan Rashdi (National University of Sciences and Technology, Pakistan)

Abstract: In this research, a recently proposed lightweight block cipher LBlock, not tested against the cube attack has been analyzed. 7, 8 and 9 round LBlock have been successfully attacked with complexities of $O(2^{10.76})$, $O(2^{11.11})$ and $O(2^{47.00})$ respectively. For the case of side channel cube attack, full version of LBlock has been attacked using a single bit leakage model with the complexity of $O(2^{55.00})$ cipher evaluations. For this purpose, a generic practical platform has been developed to test various stream and block ciphers against the latest cube attack.

HCI-KDD III – Special Session on Human-Computer Interaction & Knowledge Discovery

Session Chair: Andreas Holzinger (Medical University Graz, Austria)

Location: Lecture Hall D

1. ChEA2: Gene-Set Libraries from ChIP-X Experiments to Decode the Transcription Regulome

Yan Kou, Edward Y. Chen, Neil R. Clark, Qiaonan Duan, Christopher M. Tan, Avi Ma'ayan (Icahn School of Medicine at Mount Sinai, USA)

Abstract: ChIP-seq experiments provide a plethora of data regarding transcription regulation in mammalian cells. Integrating spurious ChIP-seq studies into a computable resource is potentially useful for further knowledge extraction from such data. We continually collect and expand a database where we convert results from ChIP-seq experiments into gene-set libraries. The manual portion of this database currently contains 200 transcription factors from 221 publications for a total of 458,471 transcription-factor/target interactions. In addition, we automatically compiled data from the ENCODE project which includes 920 experiments applied to 44 cell-lines profiling 160 transcription factors for a total of ~1.4 million transcription-factor/target-gene interactions. Moreover, we processed data from the NIH Epigenomics Roadmap project for 27 different types of histone marks in 64 different human cell-lines. All together the data was processed into three simple gene-set libraries where the set label is either a mammalian transcription factor or a histone modification mark in a particular cell line, organism and experiment. Such gene-set libraries are useful for elucidating the experimentally determined transcriptional networks regulating lists of genes of interest using gene-set enrichment analyses. Furthermore, from these three gene-set libraries, we constructed regulatory networks of transcription factors and histone modifications to identify groups of regulators that work together. For example, we found that the Polycomb Repressive Complex 2 (PRC2) is involved with three distinct clusters each interacting with different sets of transcription factors. Notably, the combined dataset is made into web-based application software where users can perform enrichment analyses or download the data in various formats. The open source ChEA2 web-based software and datasets are available freely online at http://amp.pharm.mssm.edu/ChEA2.

2. On the Prediction of Clusters for Adverse Reactions and Allergies on Antibiotics for Children to improve Biomedical Decision Making

Pinar Yildirim (Okan University, Turkey), Ljiljana Majnarić (University J.J. Strossmayer Osijek, Croatia), Ozgur Ilyas Ekmekci (Okan University, Turkey), Andreas Holzinger (Medical University Graz, Austria)

Abstract: In this paper, we report on a study to discover hidden patterns in survey results on adverse reactions and allergy (ARA) on antibiotics for children. Antibiotics are the most commonly prescribed drugs in children and most likely to be associated with adverse reactions. Record on adverse reactions and allergy from antibiotics considerably affect the prescription choices. We consider this a biomedical decision problem and explore hidden

knowledge in survey results on data extracted from the health records of children, from the Health Center of Osijek, Eastern Croatia. We apply the K-means algorithm to the data in order to generate clusters and evaluate the results. As a result, some antibiotics form their own clusters. Consequently, medical professionals can investigate these clusters, thus gaining useful knowledge and insight into this data for their clinical studies.

3. A Study on the Influence of Semantics on the Analysis of Micro-blog Tags in the Medical Domain
Carlos Vicient, Antonio Moreno (Universitat Rovira i Virgili, Spain)

Abstract: One current research topic in Knowledge Discovery is the analysis of the information provided by users in Web 2.0 social applications. In particular, some authors have devoted their attention to the analysis of micro-blogging messages in platforms like Twitter. A common shortcoming of most of the works in this field is their focus on a purely syntactical analysis. It can be argued that a proper semantic treatment of social tags should lead to more structured, meaningful and useful results that a mere syntactic-based approach. This work reports the analysis of a case study on medical tweets, in which the results of a semantic clustering process over a set of hashtags is shown to provide much better results than a clustering based on their syntactic co-occurrence.

4. Graphic-Based Concept Retrieval
Massimo Ferri (University of Bologna, Italy)

Abstract: Two ways of expressing concepts in the context of image retrieval are presented. One, Keypics, is on the side of an image owner, who wants the image itself to be found on the Web; the second, Trittico, is on the side of the image searcher. Both are based on the paradigm of human intermediation for overcoming the semantic gap. Both require tools capable of qualitative analysis, and have been experimented by using persistent homology.

SecSE I – 7th International Workshop on Secure Software Engineering

Session Chair: Martin Gilje Jaatun (SINTEF ICT, Norway)

Location: Lecture Hall F

1. Invited Talk - BSIMM4: The Building Security In Maturity Model
Gary McGraw (Cigital, USA)

http://bsimm.com

Abstract: The Building Security In Maturity Model (BSIMM) is the result of a multi-year study of real-world software security initiatives. We present the model as built directly out of data observed in fifty-one software security initiatives, from firms including: Adobe, Aon, Bank of America, Box, Capital One, The Depository Trust & Clearing Corporation (DTCC), EMC, F-Secure, Fannie Mae, Fidelity, Google, Intel, Intuit, JPMorgan Chase & Co., Mashery, McKesson, Microsoft, Nokia, Nokia Siemens Networks, QUALCOMM, Rackspace, Salesforce, Sallie Mae, SAP, Scripps Networks, Sony Mobile, Standard Life, SWIFT, Symantec, Telecom Italia, Thomson Reuters, Visa, VMware, Wells Fargo, and Zynga. The BSIMM is a measuring stick for software security. The best way to use the BSIMM is to compare and contrast your own initiative with the data presented in the BSIMM. You can then identify goals and objectives of your own and look to the BSIMM to determine which further activities make sense for you. The BSIMM data show that high maturity initiatives are well rounded-carrying out numerous activities in all twelve of the practices described by the model. The model also describes how mature software security initiatives evolve, change, and improve over time.

SecOnT I – 2nd International Workshop on Security Ontologies and Taxonomies

Session Chair: Stefan Fenz (University of Technology, Austria)

Location: Lecture Hall G

1. Introductory Talk
Stefan Fenz (Vienna University of Technology, Austria)

Abstract: (i) security ontology applications (risk and compliance management, awareness, incident handling, etc.), (ii) recent developments on the European and international level, (iii) emerging domains which could be supported

by security ontologies (e.g., smart grid area), (iv) current challenges of the domain, (v) current limitations of security ontologies and (vi) potential strategies to enable ontology-based knowledge sharing (incentives and barriers).

2. A Reference Model of Information Assurance & Security
Yulia Cherdantseva (Cardiff University, UK), Jeremy Hilton (Cranfield University, UK)

Abstract: Information Assurance & Security (IAS) is a dynamic domain which changes continuously in response to the evolution of society, business needs and technology. This paper proposes a Reference Model of Information Assurance & Security (RMIAS), which endeavours to address the recent trends in the IAS evolution, namely diversification and deperimetrisation. The model incorporates four dimensions: Information System Security Life Cycle, Information Taxonomy, Security Goals and Security Countermeasures. In addition to the descriptive knowledge, the RMIAS embeds the methodological knowledge. A case study demonstrates how the RMIAS assists with the development and revision of an Information Security Policy Document.

3. An Ontology for Malware Analysis
David A. Mundie, David M. McIntire (Carnegie Mellon University, USA)

Abstract: Malware analysis is an information security field that needs a more scientific basis for communicating requirements; hiring, training, and retaining staff; building training curricula; and sharing information among analysis teams. Our group is building an OWL-based malware analysis ontology to provide that more scientific approach. We have built a malware analysis dictionary and taxonomy, and are currently combining those with a competency model with the goal of creating an ontology-based competency framework. This paper describes the state of the work and the methodology used.

4. A Usability Evaluation of the NESSoS Common Body of Knowledge
Kristian Beckers, Maritta Heisel (University of Duisburg-Essen, Germany)

Abstract: The common body of knowledge (CBK) of the Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSoS) is a ontology that contains knowledge objects (methods, tools, notations, etc.) for secure systems engineering. The CBK is intended to support one of the main goals of the NESSoS NoE, namely to create a long-lasting research community on engineering secure software services and systems and to bring together researchers and practitioners from security engineering, service computing, and software engineering. Hence, the usability of the CBK is of utmost importance to stimulate participations in the effort of collecting and distributing knowledge about secure systems engineering. This paper is devoted to identifying and ameliorating usability deficiencies in the initial version of the CBK and its current implementation in the SMW+ framework. We report on usability tests that we performed on the initial version of the CBK and the suggestions for improvement that resulted from the usability tests. We also show some exemplary solutions, which we already implemented. We discuss our experiences so that other researchers can benefit from them.

SeCIHD III – Network Security and Privacy I – 3rd International Workshop on Security and Cognitive Informatics for Homeland Defense

Session Chair: Francesco Palmieri (Second University of Naples, Italy)
Location: Lecture Hall H

1. A Multiple-Key Management Scheme in Wireless Sensor Networks
Jung-Chun Liu, Yi-Li Huang, Fang-Yie Leu (TungHai University, Taiwan), Ilsun You (Korean Bible University, South Korea), Feng-Ching Chiang, Chao-Tung Yang, William Cheng-Chung Chu (TungHai University, Taiwan)

Abstract: In a wireless sensor network (WSN), in order to provide a secure communication environment for all the sensor nodes, we often securely authenticate network nodes and protect all the messages delivered among them. When a sensor node (or simply a node or a sensor) newly joins a WSN, it is required for the Key Distribution Server (KDS) to distribute those generated security keys to this node and all the existing nodes before they can securely communicate with each other. But due to the wireless nature, when a node broadcasts a message M, all its neighbors can receive M. To securely protect this message, a security mechanism is required. Therefore, in this paper we propose a Multiple-key Management Scheme (MMaS for short), in which a sensor N receives two sets of

keys from the KDS when the system starts up. The first set, named communication keys, is used by N to securely communicate with its neighbor sensors; the other, called the individual key, is employed to encrypt messages delivered between N and the KDS. When N would like to communicate with another node, e.g., M, they exchange their IDs with each other so as to correctly identify their common keys (CKs), which are used to individually generate a shared key (SK) on both sides for encrypting/decrypting messages transmitted between them. When N leaves the underlying network, the CKs currently related to N can be reused by a newly joining sensor, e.g., M. However, when M joins the network, if no such used ID is available, M will be given a new ID and CKs by the KDS. The KDS will encrypt the CKs, that will be used by an existing node H to communicate with M, with the individual key of H so that only H rather than M can correctly decrypt the CKs, with which to securely communicate with M. The security analysis shows that the proposed system is secure.

2. VisSecAnalyzer: A Visual Analytics Tool for Network Security Assessment
Igor Kotenko, Evgenia Novikova (St. Petersburg Institute for Informatics and Automation (SPIIRAS), Russia)

Abstract: Visualization is the essential part of Security Information and Event Management (SIEM) systems. The paper suggests a common framework for SIEM visualization which allows incorporating different visualization technologies and extending easily the application functionality. To illustrate the framework, we developed a SIEM visualization component VisSecAnalyzer. The paper demonstrates its possibilities for the tasks of attack modeling and security assessment. To increase the efficiency of the visualization techniques we applied the principles of the human information perception and interaction.

3. A Denial of Service attack to GSM networks via Attach Procedure
Nicola Gobbo (Universit`a degli Studi di Padova, Italy), Alessio Merlo (Universit`a degli Studi E-Campus, Italy) Mauro Migliardi (Universit`a degli Studi di Padova, Italy)

Abstract: Mobile Network Operators (MNOs) keep a strict control over users accessing the networks by means of the Subscribe Identity Module (SIM). This module grants the user to access the network, by performing the registration and authentication of the user's device. Without a valid SIM module and a successful authentication, mobile devices are not granted access and, hence, they are not allowed to inject any traffic in the mobile infrastructure. Nevertheless, in this paper we describe an attack to the security of a mobile network allowing an unauthenticated malicious mobile device to inject traffic in the mobile operator's infrastructure. We show that even with devices without any SIM module it is possible to inject high levels of signaling traffic in the mobile infrastructure, causing significant service degradation up to a full-edged Denial of Service (DoS) attack.

12:30 - 14:00 Lunch

14:00 – 15:30 Parallel Sessions

ARES IV – Risk planning & Threat Modeling – 8th International Conference on Availability, Reliability and Security

Location: Lecture Hall A

1. A Problem-based Threat Analysis in Compliance with Common Criteria
Kristian Beckers (University of Duisburg-Essen, Germany), Denis Hatebur (ITESYS Institute for Technical Systems GmbH, Germany), Maritta Heisel (University of Duisburg-Essen, Germany)

Abstract: In order to gain their customers' trust, software vendors can certify their products according to security standards, e.g., the Common Criteria (ISO 15408). A Common Criteria certification requires a comprehensible documentation of the software product, including a detailed threat analysis. In our work, we focus on improving that threat analysis. Our method is based upon an attacker model, which considers attacker types like software attacker that threaten only specific parts of a system. We use OCL expressions to check if all attackers for a specific domain have been considered. For example, we propose a computer-aided method that checks if all software systems have either considered a software attacker or documented an assumption that excludes software attackers. Hence, we propose a structured method for threat analysis that considers the Common Criteria's (CC)

demands for documentation of the system in its environment and the reasoning that all threats are discovered. We use UML4PF, a UML profile and support tool for Jackson's problem frame method and OCL for supporting security reasoning, validation of models, and also to generate Common Criteria-compliant documentation. Our threat analysis method can also be used for threat analysis without the common criteria, because it uses a specific part of the UML profile that can be adapted to other demands with little effort. We illustrate our approach with the development of a smart metering gateway system.

2. Detecting Insider Threats: a Trust-Aware Framework

Federica Paci (University of Trento, Italy), Carmen Fernandez Gago, Francisco Moyano (University of Malaga, Spain)

Abstract: The number of insider threats hitting organizations and big enterprises is rapidly growing. Insider threats occur when trusted employees misuse their permissions on organizational assets. Since insider threats know the organization and its processes, very often they end up undetected. Therefore, there is a pressing need for organizations to adopt preventive mechanisms to defend against insider threats. In this paper, we propose a framework for insiders identification during the early requirement analysis of organizational settings and of its IT systems. The framework supports security engineers in the detection of insider threats and in the prioritization of them based on the risk they represent to the organization. To enable the automatic detection of insider threats, we extend the SI* requirement modeling language with an asset model and a trust model. The asset model allows associating security properties and sensitivity levels to assets. The trust model allows specifying the trust level that a user places in another user with respect to a given permission on an asset. The insider threats identification leverages the trust levels associated with the permissions assigned to users, as well as the sensitivity of the assets to which access is granted. We illustrate the approach based on a patient monitoring scenario.

3. Run-Time Risk Management in Adaptive ICT Systems

Mike Surridge, Bassem Nasser, Xiaoyu Chen, Ajay Chakravarthy, Panos Melas (IT Innovation Centre, UK)

Abstract: We will present results of the SERSCIS project related to risk management and mitigation strategies in adaptive multi-stakeholder ICT systems. The SERSCIS approach involves using semantic threat models to support automated design-time threat identification and mitigation analysis. The focus of this paper is the use of these models at run-time for automated threat detection and diagnosis. This is based on a combination of semantic reasoning and Bayesian inference applied to run-time system monitoring data. The resulting dynamic risk management approach is compared to a conventional ISO 27000 type approach, and validation test results presented from an Airport Collaborative Decision Making (A-CDM) scenario involving data exchange between multiple airport service providers.

CD-ARES III – Data / Information Management as a Service – International Cross Domain Conference and Workshop

Location: Lecture Hall B

1. MetaExtractor: A System for Metadata Extraction from Structured Data Sources

Alexandra Pomares-Quimbaya, Miguel Eduardo Torres-Moreno, Fabián Roldán (Pontificia Universidad Javeriana, Colombia)

Abstract: The extraction of metadata used during the planning phase in mediation systems assumes the existence of a metadata repository that in most cases must be created with high human involvement. This dependency rises complexity of maintenance of the system and therefore the reliability of the metadata itself. This article presents MetaExtractor, a system which extracts structure, quality, capability and content metadata of structured data sources available on a mediation system. MetaExtractor is designed as a Multi-Agent System(MAS) where each agent specializes in the extraction of a particular type of metadata. The MAS cooperation capability allows the creation and maintenance of the metadata repository. MetaExtractor is useful to reduce the number of data sources selected during query planning in large scale mediation systems due to its ability to prioritize data sources that better contribute to answer a query. The work reported in this paper presents the general architecture of MetaExtractor and emphasizes on the extraction logic of content metadata and the strategy used to prioritize data sources accordingly to a given query.

2. Proxy Service for Multi-tenant Database Access

Haitham Yaish, Madhu Goyal (Centre for Quantum Computation & Intelligent Systems & University of Technology Sydney, Australia), George Feuerlicht (University of Technology Sydney, Australia & University of Economics Prague, Czech Republic)

Abstract: The database of multi-tenant Software as a Service (SaaS) applications has challenges in designing and developing a relational database for multi-tenant applica-tions. In addition, combining relational tables and virtual relational tables to make them work together and act as one database for each single tenant is a hard and complex problem to solve. Based on our multi-tenant Elastic Extension Tables (EET), we are proposing in this paper a multi-tenant database proxy service to combine multi-tenant relational tables and virtual relational tables, to make them act as one database for each single tenant. This combined database is suitable to run with multi-tenant SaaS single instance applications, which allow tenants designing their database and automatically configuring its behavior during application runtime execution. In addition, these applications allow retrieving tenants data by simply calling functions from this service which spare tenants from spending money and efforts on writing SQL queries and backend data management codes, and instead allowing them to focus on their business and to create their web, mobile, and desktop applications. The feasibility and effectiveness of the proposed service are verified by using experimental data on some of this service functions.

3. Extracting Correlated Patterns on Multicore Architectures

Alain Casali (Aix Marseille Université, France), Christian Ernst (Ecole des Mines de St Etienne, France)

Abstract: In this paper, we present a new approach relevant to the discovery of correlated patterns, based on the use of multicore architectures. Our work rests on a full KDD system and allows one to extract Decision Correlation Rules based on the Chi-squared criterion that include a target column from any database. To achieve this objective, we use a levelwise algorithm as well as contingency vectors, an alternate and more powerful representation of contingency tables, in order to prune the search space. The goal is to parallelize the processing associated with the extraction of relevant rules. The parallelization invokes the PPL (Parallel Patterns Library), which allows a simultaneous access to the whole available cores / processors on modern computers. We finally present first results on the reached performance gains.

MoCrySEn IV – Public-Key Cryptography (Modern Cryptography Track) – 2nd International Workshop on Modern Cryptography and Security Engineering

Session Chair: Nicolas Sendrier (INRIA, France)

Location: Lecture Hall C

1. Code-Based Public-Key Encryption Resistant to Key Leakage

Edoardo Persichetti (University of Warsaw, Poland)

Abstract: Side-channel attacks are a major issue for implementation of secure cryptographic schemes. Among these, key-leakage attacks describe a scenario in which an adversary is allowed to learn arbitrary information about the private key, the only constraint being the number of bits learned. In this work, we study key-leakage resilience according to the model presented by Akavia, Goldwasser and Vaikuntanathan at TCC '09. As our main contribution, we present a code-based hash proof system; we obtain our construction by relaxing some of the requirements from the original definition of Cramer and Shoup. We then propose a leakage-resilient public-key encryption scheme that makes use of this hash proof system. To do so, we adapt a framework featured in a previous work by Alwen et al. regarding identity-based encryption (EUROCRYPT '10). Our construction features error-correcting codes as a technical tool, and, as opposed to previous work, does not require the use of a randomness extractor.

2. Packed Homomorphic Encryption based on Ideal Lattices and its Application to Biometrics

Masaya Yasuda, Takeshi Shimoyama, Jun Kogure (Fujitsu Laboratories LTD, Japan), Kazuhiro Yokoyama (Rikkyo University, Japan), Takeshi Koshiba (Saitama University, Japan)

Abstract: Among many approaches for privacy-preserving biometric authentication, we focus on the approach with homomorphic encryption, which is public key encryption supporting some operations on encrypted data. In biometric authentication, the Hamming distance is often used as a metric to compare two biometric feature vectors. In this paper, we propose an efficient method to compute the Hamming distance on encrypted data using

the homomorphic encryption based on ideal lattices. In our implementation of secure Hamming distance of 2048-bit binary vectors with a lattice of 4096 dimension, encryption of a vector, secure Hamming distance, and decryption respectively take about 19.89, 18.10, and 9.08 milliseconds (ms) on an Intel Xeon X3480 at 3.07 GHz. We also propose a privacy-preserving biometric authentication protocol using our method, and compare it with related protocols. Our protocol has faster performance and shorter ciphertext size than the state-of-the-art prior work using homomorphic encryption.

3. Discussion on Modern Cryptography

HCI-KDD IV – Special Session on Human-Computer Interaction & Knowledge Discovery

Session Chair: Jan Paralič (Technical University Košice, Slovakia)
Location: Lecture Hall D

1. On Interactive Data Visualization of Physiological Low-Cost-Sensor Data with Focus on Mental Stress
Andreas Holzinger, Manuel Bruschi (Medical University Graz, Austria), Wolfgang Eder (Wolfgang Eder Unternehmensentwicklung, Austria)

Abstract: Emotions are important mental and physiological states influencing perception and cognition and have been a topic of interest in Human-Computer Interaction (HCI) for some time. Popular examples include stress detection or affective computing. The use of emotional effects for various applications in decision support systems is of increasing interest. Emotional and affective states represent very personal data and could be used for burn-out prevention. In this paper we report on first results and experiences of our EMOMES project, where the goal was to design and develop an end-user centered mobile software for interactive visualization of physiological data. Our solution was a star-plot visualization, which has been tested with data from N=50 managers (aged 25-55) taken during a burn-out prevention seminar. The results demonstrate that the leading psychologist could obtain insight into the data appropriately, thereby providing support in the prevention of stress and burnout syndromes.

2. Marking Menus for Eyes-free Interaction Using Smart Phones and Tablets
Jens Bauer, Achim Ebert (TU Kaiserslautern, Germany), Oliver Kreylos, Bernd Hamann (University of California, USA)

Abstract: Large displays are helpful tools for knowledge discovery applications. The increased screen real estate allows for more data to be shown at once. In some cases using virtual reality visualizations helps in creating more useful visualizations. In such settings, traditional input devices are not well-suited. They also do not scale well to multiple users, effectively limiting collaborative knowledge discovery scenarios. Smart phones and tablet computers are becoming increasingly ubiquitous and powerful, even having multi-core CPUs and dedicated Graphic Processing Units (GPUs). Given their built-in sensors they can serve as replacements for currently-used input devices, and provide novel functionality not achieved with traditional devices. Furthermore, their ubiquity ensures that they scale well to multi-user environments, where users can use their own devices. We present an application-independent way to integrate smart phones and tablets into knowledge discovery applications as input devices with additional functionality. This approach is based on Marking Menus, but extends the basic idea by employing the special capabilities of current consumer-level smart phones and tablets.

3. On Visual Analytics And Evaluation In Cell Physiology: A Case Study
Fleur Jeanquartier, Andreas Holzinger (Medical University Graz, Austria)

Abstract: In this paper we present a case study on a visual analytics (VA) process on the example of cell physiology. Following the model of Keim, we illustrate the steps required within an exploration and sense making process. Moreover, we demonstrate the applicability of this model and show several shortcomings in the analysis tools functionality and usability. The case study highlights the need for conducting evaluation and improvements in VA in the domain of biomedical science. The main issue is the absence of a complete toolset that supports all analysis tasks including the many steps of data preprocessing as well as end-user development. Another important issue is to enable collaboration by creating the possibility of evaluating and validating datasets, comparing it with data of other similar research groups.

SecSE II – 7th International Workshop on Secure Software Engineering

Session Chair: Martin Gilje Jaatun (SINTEF ICT, Norway)

Location: Lecture Hall F

1. Secure Engineering and Modelling of a Metering Devices System

Jose Fran. Ruiz (Fraunhofer SIT, Germany), Marcos Arjona, Antonio Maña (University of Malaga, Spain), Niklas Carstens (Mixed Mode GmbH, Germany)

Abstract: This paper presents a security engineering process for the modelling of security-sensitive systems using a real use case of metering devices. The process provides a security framework that can be used with other existing processes (such as the agile ones). It helps to develop and model systems bearing in mind their heterogeneity, real-time and dynamic behaviors. Besides, due to the critical nature of some of these systems (nuclear, emergency systems, military, etc.) it provides tools for identifying, working and solving security threats by using the knowledge of domain experts. This is very important because threats, properties, solutions, etc. that are valid or relevant in a given domain, are not applicable to other domains and are subject to constant changes. The security requirements of the systems are fulfilled by means of domain-specific security knowledge. These artefacts contain the specific information of a domain (security properties, elements, assumptions, threats, tests, etc.). The solutions are presented as Security Patterns. Each one describes an implementation solution by using one or several Security Building Blocks (SBBs). The security engineering process presented here describes how to model a security-enhanced system model using a library of domain security knowledge. The process has been developed along with a MagicDraw plugin that covers all the possible functionalities, making the work with the models and the security elements very simple and easy for the user.

2. The Use And Usefulness of Threats in Goal-Oriented Modelling

Per Håkon Meland, Erlend Andreas Gjære (SINTEF ICT, Norway), Stéphane Paul (Thales Research and Technology, France)

Abstract: Both goal and threat modelling are well-known activities related to high-level requirements engineering. While goals express why a system is needed, threats tell us why security for our system is needed. Still, you will often find that goals and threats are treated in separate modelling processes, perhaps not being influenced by each other at all. The research question we try to address in here is to what extent should we include threats in goal-oriented modelling? There is for instance a trade-off between expressiveness, usability and usefulness that must be considered. To improve this situation we believe that a well-defined methodology with good tool support will make the modelling process easier, and give a more useful result. In this paper we first give an overview of previous work on the use of threats within goal-modelling. We explain the use of threats within a goal-oriented sociotechnical security modelling language and how tool support enables reuse of threats and automatic analysis of threat propagation in the models. This is exemplified with a case study from Air Traffic Management (ATM) from which we extract some of the the practical challenges that we have. We are able to conclude that threats provide a useful foundation and justification for the security requirements we derive from goal modelling, but this should not be considered to be a replacement for risk assessment methods. Having goals and threats before thinking of the technical solutions of a system allows us to raise awareness on situations that are not just exceptions from regular execution flow.

3. Modelling and Analysis of Release Order of Security Algorithms Using Stochastic Petri Nets

Suliman A. Alsuhibany, Aad van Moorsel (Newcastle University, UK)

Abstract: While security algorithms are utilized to protect system resources from misuse, using a single algorithm such as CAPTCHAs and Spam-Filters as a defence mechanism can work to protect a system against current attacks. However, as attackers learn from their attempts, this algorithm will eventually become useless and the system is no longer protected. We propose to look at a set of algorithms as a combined defence mechanism to maximize the time taken by attackers to break a system. When studying sets of algorithms, diverse issues arise in terms of how to construct them and in which order or in which combination to release them. In this paper, we propose a model based on Stochastic Petri Nets, which describe the interaction between an attacker, the set of algorithms used by a system, and the knowledge gained by the attacker with each attack. In particular, we investigate the interleaving of dependent algorithms, which have overlapping rules, with independent algorithms, which have a disjoint set of rules. Based on the proposed model, we have analyzed and evaluated how the order can impact the time taken by an attacker to break a set of algorithms. Given the mean time to security failure (MTTSF) for a system to reach a

failure state, we identify an improved approach to the release order of a set of algorithms in terms of maximizing the time taken by the attacker to break them. Further, we show a prediction of the attacker's knowledge acquisition progress during the attack process.

SecOnT II – 2nd International Workshop on Security Ontologies and Taxonomies

Session Chair: Stefan Fenz (Vienna University of Technology, Austria)
Location: Lecture Hall G

1. A Bootstrapping Approach for Developing a Cyber-security Ontology Using Textbook Index Terms

Arwa Wali (New Jersey Institute of Technology, USA), Soon Ae Chun (Columbia University & CUNY College of Staten Island, UAS), James Geller (New Jersey Institute of Technology, USA)

Abstract: Developing a domain ontology with concepts and relationships between them is a challenge, since knowledge engineering is a labor intensive process that can be a bottleneck and is often not scalable. Developing a cyber-security ontology is no exception. A security ontology can improve search for security learning resources that are scattered in different locations in different formats, since it can provide a common controlled vocabulary to annotate the resources with consistent semantics. In this paper, we present a bootstrapping method for developing a cyber-security ontology using both a security textbook index that provides a list of terms in the security domain and an existing security ontology as a scaffold. The bootstrapping approach automatically extracts the textbook index terms (concepts), derives a relationship to a concept in the security ontology for each and classifies them into the existing security ontology. The bootstrapping approach relies on the exact and approximate similarity matching of concepts as well as the category information obtained from external sources such as Wikipedia. The results show feasibility of our method to develop a more comprehensive and scalable cyber-security ontology with rich concepts from a textbook index. We provide criteria used to select a scaffold ontology among existing ontologies. The current approach can be improved by considering synonyms, deep searching in Wikipedia categories, and domain expert validation.

2. Towards an Ontology for Cloud Security Obligations

Karin Bernsmed, Astrid Undheim, Per Håkon Meland, Martin Gilje Jaatun (SINTEF ICT, Norway)

Abstract: This paper presents an ontology for Cloud security obligations, which is based on a number of industry accepted standards and guidelines. The ontology terms and relationships have been defined in the W3C ontology language OWL and includes a number of technical security controls that can be implemented by public Cloud providers. This paper outlines the ontology and demonstrates how it can be used in two different application areas.

3. On Identifying Proper Security Mechanisms

Jakub Breier, Ladislav Hudec (Slovak University of Technology, Slovakia)

Abstract: Selection of proper security mechanisms that will protect the organization's assets against cyber threats is an important non-trivial problem. This paper introduces the approach based on statistical methods that will help to choose the proper controls with respect to actual security threats. First, we determine security mechanisms that support control objectives from ISO/IEC 27002 standard and assign them meaningful weights. Then we employ a factor analysis to reveal dependencies among control objectives. Then this knowledge can be reflected to security mechanisms, that inherit these dependencies from control objectives.

4. Taxonomy for Port Security Systems

Tove Gustavi, Pontus Svenson (Swedish Defence Research Agency, Sweden)

Abstract: In this paper we describe the construction of a taxonomy for port security systems that we performed as part of the EU FP-7 project SUPPORT (Security UPgrade for PORTs). The purpose of the taxonomy is to enable port stakeholders to exchange information and to provide them with computer-based automatic decision support systems, assisting the human operator in the assessment of threat levels for a number of pre-defined threats. The decision support system uses text based automatic reasoning and high-level information fusion to identify threat indicators in the input data. Thus, the existence of a taxonomy containing well defined terms that can be used by the reasoning system is essential. In the paper we describe the method used to construct the taxonomy, viz. first

constructing a draft taxonomy and then gathering feedback on this using questionnaires. The questionnaires were motivated by the necessity to embody experience and knowledge from different groups of people involved in the project, most of which are not used to formally defining their vocabulary. Overall, the method proved to work well and produced the expected result, namely a basic taxonomy that can be used by a decision support system, and that can be extended during the project according to need.

SeCIHD IV – Network Security and Privacy II – 3rd International Workshop on Security and Cognitive Informatics for Homeland Defense

Session Chair: Fang-Yie Leu (Tunghai University, Taiwan)

Location: Lecture Hall H

1. PPM: Privacy Policy Manager for Personalized Services
   Shinsaku Kiyomoto, Toru Nakamura (KDDI R & D Laboratories Inc., Japan), Haruo Takasaki (KDDI Research Institute Inc., Japan), Ryu Watanabe, Yutaka Miyake (KDDI R & D Laboratories Inc., Japan

   Abstract: In this paper, we introduce a new architecture for personalized services. The architecture separates access control using a user own privacy policy from data storage for private information, and it supports privacy policy management by users. We design a core module, the Privacy Policy Manager (PPM). The module includes several functionalities: ID management, privacy policy management, control of information flows, and recording the flows.

2. An Attribute Based Private Data Sharing Scheme for People-Centric Sensing Networks
   Bo Liu, Baokang Zhao, Bo Liu, Chunqing Wu (National University of Defense Technology, China)

   Abstract: In recent years, people-centric sensing networks have attracted much research effort. To date, there are still some significant security and privacy challenges in people-centric sensing networks. In this paper, we focus on the private data sharing and protection in people-centric sensing networks. First, we formalize the network model with relay nodes which improves the data forwarding efficiency of networks. Second, we propose a novel Attribute based Private data sharing protocol in People-centric sensing networks (APP). Relying on the technology of ciphertext policy attribute based encryption, our APP protocol can protect the privacy and integrity with efficient approaches of authentication, encryption, transmission and decryption. Also, we propose an associative data indexing scheme to improve the private data sharing performance. Finally, we discuss the performance evaluation of APP protocol in detail and find that it can achieve much better efficiency.

3. Intelligent UBMSS Systems for Strategic Information Management
   Lidia Ogiela, Marek R. Ogiela (AGH University of Science and Technology, Poland)

   Abstract: In this publication will be described the most important features of UBMSS cognitive information systems, as well as security issues connected with these new generation information systems. Such systems are mainly designed to perform an intelligent information management based on semantic analysis of data merit content. In paper will be also presented some possibilities to develop such systems for strategic information management in state or government institution. The paper will describe both UMBSS internal safety features, and external possible application of authentication procedures along with intelligent information management.

4. A New Approach to Develop a Dependable Security Case by Combining Real Life Security Experiences (Lessons Learned) with D-Case Development Process
   Vaise Patu, Shuichiro Yamamoto (Nagoya University, Japan)

   Abstract: Modern information and distributed systems runs for extensive periods of time and are being constantly improved in service objectives under evolving technologies and changing regulations and standards. These systems have become extremely complex and therefore, it is very important that they are to be dependable in order for them to execute their functionalities and purposes correctly or to an acceptable level of services. However, due to the ever-growing complexity of information and distributed systems, it is very difficult to achieve dependability by relying only on conventional technologies such as development processes and formal methods. And therefore the idea of Assurance Case or D-Case (dependability case) has become more and more a popular notion. Recently, D-Case which is an extension form of Assurance Case, is more commonly associated with the safely aspect of

dependability. And because of this regard, safety cases are more well known in comparison to other aspects of dependability such as availability, integrity and confidentiality witch are all related to the security domain. In this paper, we introduce our new approach to the development of a dependable security case.

15:30 – 16:00 Coffee Break

16:00 – 17:30 Parallel Sessions

ARES V – Privacy – 8th International Conference on Availability, Reliability and Security

Location: Lecture Hall A

1. Measuring Anonymity with Plausibilistic Entropy
   Iulian Goriac ("Al.I.Cuza" University, Romania)

   Abstract: To prove that a certain protocol provides a certain security property (e.g. anonymity) one must first formally define that property in the context of a logical framework capable of expressing the relevant aspects of that protocol and then perform the actual inference steps (preferably automatically). After the qualitative aspect of the property is successfully addressed the next issue is the strength of the property – how to express it quantitatively so that it can be compared both to some business requirements and to other implementing protocols. The framework that we build upon is the MAS epistemic logic introduced by Halpern and O'Neill in their approach for defining anonymity both possibilistically and probabilistically. Our contribution employs the highly general plausibilistic approach in order to provide a numeric measure for anonymity that can also be extended to other properties as well. We propose a formula for calculating a particular kind of entropy suited for characterising partially ordered sets used to define plausibility measures and, on top of it, a quantitative definition for anonymity. We believe that the theory presented here is capable of filling the gap between the very general qualitative definition of anonymity and the information intensive probabilistic approach that might not always be applicable.

2. Revisiting Circuit Clogging Attacks on Tor
   Eric Chan-Tin, Jiyoung Shin, Jiangmin Yu (Oklahoma State University, USA)

   Abstract: Tor is a popular anonymity-providing network used by over 500, 000 users daily. The Tor network is made up of volunteer relays. To anonymously connect to a server, a user first creates a circuit, consisting of three relays, and routes traffic through these proxies before connecting to the server. The client is thus hidden from the server through three Tor proxies. If the three Tor proxies used by the client could be identified, the anonymity of the client would be reduced. One particular way of identifying the three Tor relays in a circuit is to perform a circuit clogging attack. This attack requires the client to connect to a malicious server (malicious content, such as an advertising frame, can be hosted on a popular server). The malicious server alternates between sending bursts of data and sending little traffic. During the burst period, the three relays used in the circuit will take longer to relay traffic due to the increase in processing time for the extra messages. If Tor relays are continuously monitored through network latency probes, an increase in network latency indicates that this Tor relay is likely being used in that circuit. We show, through experiments on the real Tor network, that the Tor relays in a circuit can be identified. A detection scheme is also proposed for clients to determine whether a circuit clogging attack is happening. The costs for both the attack and the detection mechanism are small and feasible in the current Tor network.

3. Taxonomy for Social Network Data Types from the Viewpoint of Privacy and User Control
   Christian Richthammer, Michael Netter, Moritz Riesner, Günther Pernul (University of Regensburg, Germany)

   Abstract: The growing relevance and usage intensity of Online Social Networks (OSNs) along with the accumulation of a large amount of user data has led to privacy concerns among researchers and end users. Despite a large body of research addressing OSN privacy issues, little differentiation of data types on social network sites is made and a generally accepted classification and terminology for such data is missing, hence leading to confusion in related discussions. This paper proposes a taxonomy for data types on OSNs based on a thorough literature analysis and a conceptualization of typical OSN user activities. It aims at clarifying discussions among researchers, benefiting

comparisons of data types within and across OSNs and at educating the end user about characteristics and implications of OSN data types. The taxonomy is evaluated by applying it to four major OSNs.

CD-ARES IV – Context-Oriented Information Integration & Location-aware Computing – International Cross Domain Conference and Workshop

Location: Lecture Hall B

1. Index Data Structure for Fast Subset and Superset Queries
   Iztok Savnik (University of Primorska & Jozef Stefan Institute, Slovenia)

   Abstract: A new data structure set-trie for storing and retrieving sets is proposed. Efficient manipulation of sets is vital in a number of systems including datamining tools, object-relational database systems, and rule-based expert systems. Data structure set-trie provides efficient algorithms for set containment operations. It allows fast access to subsets and supersets of a given parameter set. The performance of operations is analyzed empirically in a series of experiments on real-world and artificial datasets. The analysis shows that sets can be accessed in O(c * |set|) time where |set| represents the size of parameter set and c is a constant.

2. Opinion Mining in Conversational Content within Web Discussions and Commentaries
   Kristína Machová, Lukáš Marhefka(Technical University, Slovakia)

   Abstract: The paper focuses on the problem of opinion classification related to web discussions and commentaries. It introduces various approaches known in this field. It also describes novelty methods, which have been designed for short conversational content processing with emphasis on dynamic analysis. This dynamic analysis is focused mainly on processing of negations and intensifiers within the opinion analysis. The contribution describes implementations of these methods for the Slovak language. The Slovak dictionaries have been created to support these implementations of lexicon based approach. In addition, the paper describes test results of the presented implementations and discussion of these results as well.

3. Diagnosis of Higher-Order Discrete-Event Systems
   Gianfranco Lamperti (Università degli Studi di Brescia, Italy), Xiangfu Zhao (Zhejiang Normal University, China)

   Abstract: Preventing major events, like the India blackout in 2012 or the Fukushima nuclear disaster in 2011, is vital for the safety of society. Automated diagnosis may play an important role in this prevention. However, a gap still exists between the complexity of systems such these and the effectiveness of state-of-the-art diagnosis techniques. The contribution of this paper is twofold: the definition of a novel class of discrete-event systems (DESs), called higherorder DESs (HDESs), and the formalization of a relevant diagnosis technique. HDESs are structured hierarchically in several cohabiting subsystems, accommodated at different abstraction levels, each one living its own life, as happens in living beings. The communication between subsystems at different levels relies on complex events, occurring when specific patterns of transitions are matched. Diagnosis of HDESs is scalable, context-sensitive, and in a way intelligent.

MoCrySEn V – Software and Hardware Implementation of Cryptographic Algorithms (Security Engineering Track) – 2nd International Workshop on Modern Cryptography and Security Engineering

Session Chair: Nicolas Sendrier (INRIA, France)

Location: Lecture Hall C

1. Improving the Efficiency of Elliptic Curve Scalar Multiplication using Binary Huff Curves
   Gerwin Gsenger, Christian Hanser (Graz University of Technology, Austria)

   Abstract: In 2010, Joye et. al brought the so-called Huff curve model, which was originally proposed in 1948 for the studies of Diophantine equations, into the context of elliptic curve cryptography. Their initial work describes Huff curves over fields of large prime characteristic and details unified addition laws. Devigne and Joye subsequently extended the model to elliptic curves over binary fields and proposed fast differential addition formulas that are

well-suited for use with the Montgomery ladder, which is a side-channel attack resistant scalar multiplication algorithm. Moreover, they showed that, in contrast to Huff curves over prime fields, it is possible to convert (almost) all binary Weierstrass curves into Huff form. We have implemented generalized binary Huff curves in software using a differential Montgomery ladder and detail the implementation as well as the optimizations to it. We provide timings, which show speed-ups of up to 7.4% for binary NIST curves in Huff form compared to the reference implementation on Weierstrass curves. Furthermore, we present fast formulas for mapping between binary Weierstrass and generalized binary Huff curves and vice versa, where in the back conversion step an implicit y-coordinate recovery is performed. With these formulas, the implementation of the differential Montgomery ladder on Huff curves does not require more effort than its counterpart on Weierstrass curves. Thus, given the performance gains discussed in this paper, such an implementation is an interesting alternative to conventional implementations. Finally, we give a list of Huff curve parameters corresponding to the binary NIST curves specified in FIPS 186-3.

2. Speeding Up the Fixed-Base Comb Method for Faster Scalar Multiplication on Koblitz Curves
Christian Hanser, Christian Wagner (Graz University of Technology, Austria)

Abstract: Scalar multiplication is the most expensive arithmetical operation on elliptic curves. There are various methods available, which are optimized for different settings, such as high speed, side-channel resistance and small memory footprint. One of the fastest methods for fixed-base scalar multiplications is the so-called fixed-base comb scalar multiplication method, which is due to Lim and Lee. In this paper, we present a modification to this method, which exploits the possibility of exchanging doublings for much cheaper applications of the Frobenius endomorphism on binary Koblitz curves.We have implemented the findings in software and compare the performance of the implementation to the performance of the reference WTNAF implementation and the performance of the conventional comb multiplication methods. For single scalar multiplications, we are able to achieve performance improvements over the WTNAF method of up to 25% and of up to 42% over the conventional comb methods. Finally, we emphasize that the implementation of the τ-comb method is straight-forward and requires only little effort. All in all, this makes it a good alternative to other fixed-base multiplication methods.

3. Fast Software Polynomial Multiplication on ARM Processors using the NEON Engine
Danilo Câmara, Conrado P. L. Gouvêa, Julio López, Ricardo Dahab (University of Campinas, Brazil)

Abstract: Efficient algorithms for binary field operations are required in several cryptographic operations such as digital signatures over binary elliptic curves and encryption. The main performance-critical operation in these fields is the multiplication, since most processors do not support instructions to carry out a polynomial multiplication. In this paper we describe a novel software multiplier for performing a polynomial multiplication of two 64-bit binary polynomials based on the VMULL instruction included in the NEON engine supported in many ARM processors. This multiplier is then used as a building block to obtain a fast software multiplication in the binary field F2m, which is up to 45% faster compared to the best known algorithm. We also illustrate the performance improvement in point multiplication on binary elliptic curves using the new multiplier, improving the performance of standard NIST curves at the 128- and 256-bit levels of security. The impact on the GCM authenticated encryption scheme is also studied, with new speed records. We present timing results of our software implementation on the ARM Cortex-A8, A9 and A15 processors.

WSDF – 6th International Workshop on Digital Forensics

Session Chair: Martin Mulazzani (SBA Research, Austria)

Location: Lecture Hall D

1. A Comprehensive Literature Review of File Carving
Rainer Poisel, Simon Tjoa (St. Pölten University of Applied Sciences, Austria)

Abstract: File carving is a recovery technique allowing file recovery without knowledge about contextual information such as file system metadata. Due to recent advancements in research, file carving has become an essential technique for both general data recovery and digital forensics investigations. During the last few years a considerable amount of publications has been published on the topic of file carving. Out of around 130 publications in this field we selected 70 key papers with major contributions to the topic in order to identify potential fields of future research activities. The first contribution of this paper is a survey on state-of-the-art literature supporting

researchers and practitioners in gaining a comprehensive view on the progress in file carving research. In addition to that, the second major contribution of this paper is a (preliminary) file carving ontology. The purpose of the ontology presented within this paper is to push forward recovery approaches that are based on knowledge bases processable by computer systems.

2. fastdd: An Open Source Forensic Imaging Tool
Paolo Bertasi, Nicola Zago (University of Padova, Italy)

Abstract: Nowadays electronic devices are ubiquitous and their storage capacity has steadily been growing over time. It is not surprising that acquiring a copy of the storage of such devices has become a crucial task in digital forensics, resulting in the development of fast and still reliable tools. In this work we introduce fastdd, a new disk imaging tool that achieves unmatched performance while having fewer resource requirements than the currently available tools and being designed to be easily extendable. After reviewing the existing programs for disk image acquisition, we compare their functionalities and performance to fastdd, demonstrating that our tool is fast, lightweight, hence suitable to be used in embedded devices.

3. Artificial Ageing of Mobile Devices Using a Simulated GSM/GPRS Network
Rolf Stöbe, Hans Höfken, Marko Schuba (Aachen University of Applied Sciences, Germany), Michael Breuer (State Office of Criminal Investigation, Germany)

Abstract: The analysis of mobile devices is a fast moving area in digital forensics. Investigators frequently are challenged by devices which are not supported by existing mobile forensic tools. Low level techniques like de-soldering the flash memory chip and extracting its data provide an investigator with the exhibits internal memory, however, the interpretation of the data can be difficult as mobile device and flash chip manufacturers use their own proprietary techniques to encode and store data. The approach presented in this paper helps investigators to analyze this proprietary encoding by feeding a reference device identical to the exhibit with real data in a controlled way. This “artificial ageing” of the reference device is achieved using an isolated GSM/GPRS network plus additional software in a lab environment. After the ageing process is completed, the internal memory of the reference device can be acquired and used to reverse engineer the high level file system and the encoding of the data previously fed to the phone, like received SMS messages or calls. When sufficient knowledge about the interpretation of the memory image has been built up, it can be applied to the original evidence in order to analyze data and files relevant for the case. The successful operation of the solution is demonstrated in a proof of concept for SMS messages.

4. Model-Based Generation of Synthetic Disk Images for Digital Forensic Tool Testing
York Yannikos, Christian Winter (Fraunhofer SIT, Germany)

Abstract: Testing digital forensic tools is important to determine relevant tool properties like effectiveness and efficiency. Since many different forensic tool categories exist, different testing techniques and especially suitable test data are required. Considering test data for disk analysis and data recovery tools, synthetic disk images provide significant advantages compared to disk images created from real-world storage devices. In this work we propose a framework for generating synthetic disk images for testing digital forensic analysis tools. The framework provides functionality for building models of real-world scenarios in which data on a storage device like a hard disk is created, changed, or deleted. Using such a model our framework allows simulating actions specified in the model in order to generate synthetic disk images with realistic characteristics. These disk images can then be used for testing the performance of forensic disk analysis and data recovery tools.

SecSE III – 7th International Workshop on Secure Software Engineering

Session Chair: Martin Gilje Jaatun (SINTEF ICT, Norway)

Location: Lecture Hall F

1. Software Vulnerability Detection using Backward Trace Analysis and Symbolic Execution
Hongzhe Li, Taebeom Kim, Munkhbayar Bat-Erdene, Heejo Lee (Korea University, South Korea)

Abstract: Software vulnerability has long been considered an important threat to the safety of software systems. When source code is accessible, we can get much help from the information of source code to detect

vulnerabilities. Static analysis has been used frequently to scan code for errors that cause security problems when source code is available. However, they often generate many false positives. Symbolic execution has also been proposed to detect vulnerabilities and has shown good performance in some researches. However, they are either ineffective in path exploration or could not scale well to large programs. During practical use, since most of paths are actually not related to security problems and software vulnerabilities are usually caused by the improper use of security-sensitive functions, the number of paths could be reduced by tracing sensitive data backwardly from security-sensitive functions so as to consider paths related to vulnerabilities only. What's more, in order to leave ourselves free from generating bug triggering test input, formal reasoning could be used by solving certain program conditions. In this research, we propose backward trace analysis and symbolic execution to detect vulnerabilities from source code. We first find out all the hot spot in source code file. Based on each hot spot, we construct a data flow tree so that we can get the possible execution traces. Afterwards, we do symbolic execution to generate program constraint(PC) and get security constraint(SC) from our predefined security requirements along each execution trace. A program constraint is a constraint imposed by program logic on program variables. A security constraint(SC) is a constraint on program variables that must be satisfied to ensure system security. Finally, this hot spot will be reported as a vulnerability if there is an assignment of values to program inputs which could satisfy PC but violates SC, in other words, satisfy $PC \wedge \overline{SC}$. We have implemented our approach and conducted experiments on test cases which we randomly choose from Juliet Test Suites provided by US National Security Agency(NSA). The results show that our approach achieves Precision value of 83.33% , Recall value of 90.90% and F1_Value of 86.95% which gains the best performance among competing tools. Moreover, our approach can efficiently mitigate path explosion problem in traditional symbolic execution.

2. Automated Synthesis and Ranking of Secure BPMN Orchestrators

Vincenzo Ciancia, Fabio Martinelli, Ilaria Matteucci, Marinella Petrocchi (National Research Council, Italy), Jose Antonio Martín, Ernesto Pimentel (Universidad de Málaga, Spain)

Abstract: We describe a formal methodology for the automatic synthesis of a secure orchestrator for a set of BPMN processes. The synthesized orchestrator is able to guarantee that all the processes that are started reach their end, and the resulting orchestrator process is secure, that is, it does not allow discloure of certain secret messages. In this work we present an implementation of a forth and back translation from BPMN to crypto-CCS, in such a way to exploit the PaMoChSA tool for synthesizing orchestrators. Furthermore, we study the problem of ranking orchestrators based on quantitative valuations of a process, and on the temporal evolution of such valuations and their security, as a function of the knowledge of the attacker.

3. Structured Pattern-Based Security Requirements Elicitation for Clouds

Kristian Beckers, Maritta Heisel (University Duisburg-Essen, Germany), Isabelle Côté, Ludger Goeke, Selim Güler (ITESYS Institute for technical Systems GmbH, Germany)

Abstract: Economic benefits make cloud computing systems a very attractive alternative to traditional IT-systems. However, numerous concerns about the security of cloud computing services exist. Potential cloud customers have to be confident that the cloud services they acquire are secure for them to use. Therefore, they have to have a clear set of security requirements covering their security needs. Eliciting these requirements is a difficult task, because of the amount of stakeholders and technical components to consider in a cloud environment. That is why we propose a structured, pattern-based method supporting eliciting security requirements. The method guides a potential cloud customer to model a cloud system via our cloud system analysis pattern. The instantiated pattern establishes the context of a cloud scenario. Then, the information of the instantiated pattern can be used to fill-out our textual security requirements patterns. The presented method is tool-supported. Our tool supports the instantiation of the cloud system analysis pattern and automatically transfers the information from the instance to the security requirements patterns. In addition, we have validation conditions that check e.g., if a security requirement refers to at least one element in the cloud. We illustrate our method using an online-banking system as running example.

SeCIHD V – Multimedia Technology for Homeland Defense – 3rd International Workshop on Security and Cognitive Informatics for Homeland Defense

Session Chair: Shinsaku Kiyomoto (KDDI, JAPAN)
Location: Lecture Hall H

1. Fully Distributed Secure Video Surveillance Via Portable Device With User Awareness
   Arcangelo Castiglione, Ciriaco D'Ambrosio, Alfredo De Santis (Universit`a di Salerno, Itlay), Francesco Palmieri (Seconda Universit`a di Napoli, Italy)

   Abstract: Internet-based video surveillance systems are now widespread in the modern e-Society, since they can be used to manage multiple physical security problems in a lot of contexts. Moreover, the growing diffusion of portable device, along with the necessity of keeping specific environments and motion events under control, brought out the need for more flexible and proactive systems, which allow the management of such scenarios. However, most of the state of the art video surveillance systems are known to be unscalable, unreliable, insecure, and do not provide adequate guarantees for user awareness when a determined situation of interest occurs. Furthermore, almost all the currently defined systems, lack in operation flexibility: they are designed for a specific context and can not be easily adapted to other ones. In this work, we propose a general-purpose video surveillance system, which is fully distributed and accessible through ubiquitous portable devices. Such system, whose architecture is based on a self-organizing overlay network built on top of a mixture of already existing physical network connections, provides an high degree of reliability for the interactions among all its components, and ensures to its users, regardless of where they are located, the ability to receive notifications upon the occurrence of interesting events.

2. Computer Karate Trainer in Tasks of Personal and Homeland Security Defense
   Tomasz Hachaj (Pedagogical University of Krakow, Poland), Marek R. Ogiela (AGH University of Science and Technology, Poland)

   Abstract: In this paper will be presented a new possibility of using GDL (Gesture Description Language) approach for recognition of basic combat techniques from martial arts. The GDL approach allows not only to analyze the several Shorin-Ryu Karate techniques but also to support the training and teaching activities of such arts. Moreover the GDL allow performing the human behavioral analysis, which may be important for recognition of dangerous situations while ensuring the homeland security.

3. Trustworthiness Evaluation of Multi-Sensor Situation Recognition in Transit Surveillance Scenarios
   Francesco Flammini (Ansaldo STS, Italy), Stefano Marrone (Seconda Università di Napoli, Italy), Nicola Mazzocca (Università "Federico II" di Napoli, Italy), Alfio Pappalardo, Concetta Pragliola (Ansaldo STS, Italy), Valeria Vittorini (Università "Federico II" di Napoli, Italy)

   Abstract: Physical Security Information Management (PSIM) systems are a recent introduction in the surveillance of critical infrastructures, like those used for mass-transit. In those systems, different sensors are integrated as separate event detection devices, each of them generating independent alarms. In order to lower the rate of false alarms and provide greater situation awareness for surveillance operators, we have developed a framework – namely DETECT – for correlating information coming from multiple heterogeneous sensors. DETECT uses detection models based on (extended) Event Trees in order to generate higher level warnings when a known threat scenario is being detected. In this paper we extend DETECT by adopting probabilistic models for the evaluation of threat detection trustworthiness on reference scenarios. The approach also allows for a quantitative evaluation of model sensitivity to sensor faults. The results of a case-study in the transit system domain demonstrate the increase of trust one could expect when using scenarios characterized in a probabilistic way for the threat detection instead of single-sensor alarms. Furthermore, we show how a model analysis can serve at design time to support decisions about the type and redundancy of detectors.

17:30-23:00 Conference Dinner

Wednesday, 04 September 2013

08:00 – 17:30 Registration for all events

09:00 – 10:30 Parallel Sessions

Keynote

Location: Lecture Hall A

Six Research Challenges for the Security and Privacy of Health Information Technology

Carl A. Gunter (University of Illinois, United States)

Abstract: Health Information Technology (HIT) has the potential to improve the health of individuals of all ages, aid medical research, and reduce the costs of delivering healthcare, but its effective use and acceptance by the public and healthcare professionals depend on employing proper protections for the security and privacy of health information. While considerable progress can be made by applying current best practices for managing data, there are a number of areas specific to HIT where more research is needed to provide technology to support better practices. At least six key areas need to be addressed: (1) access controls and audit, (2) encryption and trusted base, (3) automated policy, (4) mobile health (mHealth), (5) identification and authentication, and (6) data segmentation and de-identification. This talk will discuss each of these challenges and some of the efforts being made to address them.

RaSIEM I – 2nd International Workshop on Recent Advances in Security Information and Event Management

Session Chair: Elsa Prieto (Atos Research & Innovation, Spain)

Location: Lecture Hall F

1. Invited Presentation – Elastic Detector

   Pasquale Puzio (SecludIT and EURECOM)

   Abstract: New cloud IT infrastructures bring new security challenges, brought by elasticity, programmability and multi-tenancy. The goal of Elastic Detector is to be an advanced security probe that collects cloud infrastructure events to a SIEM. Elastic Detector does a first set of security analysis on virtual servers, the cloud software stack and the virtual firewalls and networks. Correlation with other security events, for example brought by traditional (e.g. non-cloud) IT infrastructures, are then performed at the SIEM level. The goal of this presentation is to make an overview of the new security challenges brought by cloud infrastructures and to show how Elastic Detector addresses them. A demo of an integration of Elastic Detector with OSSIM will be shown in the context of security management of a public cloud infrastructure.

10:30 – 11:00 Coffee Break

11:00 – 12:30 Parallel Sessions

ARES VI – Hardware & Network Security – 8th International Conference on Availability, Reliability and Security

Location: Lecture Hall A

1. High Availability for IPsec VPN Platforms: ClusterIP Evaluation
   Daniel Palomares, Daniel Migault (France Telecom, France), Wolfgang Velasquez (France Telecom & Institut Télécom, France), Maryline Laurent (Institut Télécom, France)

   Abstract: To manage the huge demand on traffic, the Internet Service Providers (ISP) are offloading its mobile data from Radio Access Networks (RAN) to Wireless Access Networks (WLAN). While these RANs are considered trusted networks, WLANs need to build a similar trusted zone in order to offer the same security level and Quality of Service (QoS) to End-Users (EU). Although IPsec is widely implemented to create trusted environments through untrusted networks, the industry is increasingly interested in providing IPsec-based services with High Availability (HA) features in order to ensure reliability, QoS and security. Even though IPsec is not originally well suited to provide HA features, some mechanisms like VRRP or ClusterIP can work together with IPsec in order to offer HA capabilities. ClusterIP is actually used by *strongSwan* (an open source IPsecbased VPN solution) to build a cluster of IPsec Security Gateways (SG) offering HA features. This paper concentrates on how to build a cluster of IPsec SGs based on ClusterIP. We describe the main issues to overcome HA within IPsec. Then, we measure how HA may affect the EU experience, and provide recommendations on how to deploy ClusterIP. Finally, our tests over an HTTP connection showed that ClusterIP allows fast recovering during a failure.

2. ARMORED: CPU-bound Encryption for Android-Driven ARM Devices
   Johannes Götzfried, Tilo Müller (Friedrich-Alexander-Universität, Germany)

   Abstract: As recently shown by attacks against Android-driven smartphones, ARM devices are vulnerable to cold boot attacks. At the end of 2012, the data recovery tool FROST was released which exploits the remanence effect of RAM to recover user data from a smartphone, at worst its disk encryption key. Disk encryption is supported in Android since version 4.0 and is today available on many smartphones. With ARMORED, we demonstrate that Android's disk encryption feature can be improved to withstand cold boot attacks by performing AES entirely without RAM. ARMORED stores necessary keys and intermediate values of AES inside registers of the ARM microprocessor architecture without involving main memory. As a consequence, cold boot attacks on encryption keys in RAM appear to be futile. We developed our implementation on a PandaBoard and tested it successfully on real phones. We also present a security and a performance analysis for ARMORED.

3. Minimizing the Costs of Side-Channel Analysis Resistance Evaluations in Early Design Steps
   Thomas Korak, Thomas Plos, Andreas Zankl (Graz University of Technology, Austria)

   Abstract: Evaluating the side-channel analysis (SCA) resistance of an implementation is often a challenging task for a chip designer. Reducing the time required for evaluation allows faster redesign cycles and lowers consequently also product costs. In this work we present several ways to speed up the evaluation of implementations of symmetric cryptographic primitives according to their resistance against SCA attacks. We cover the recording of the traces, the preprocessing steps as well as mitigation techniques for implemented countermeasures. The focus in this work is put on constrained devices, e.g., for radio-frequency identification applications, so only a subset of common countermeasures is covered. In a practical example we show how to speed up the SCA resistance evaluation of an application-specific integrated circuit (ASIC) chip for near-field communication (NFC) applications. The chip has the Advanced Encryption Standard (AES) with two countermeasures implemented: the random insertion of dummy rounds and shuffling. During our evaluation we found ways to mitigate the impact of both countermeasures. Our mitigation techniques show the importance of practically performing SCA attacks on prototypes in order to identify small leakages which might be used to enhance an attack. Altogether we are able to decrease the number of required traces for revealing the secret AES key from more than

$3.1 \bullet 10^6$ to less than 20 000 which corresponds to a reduction of the evaluation time from 16 days to less than 3 hours.

CD-ARES V – Security and Privacy – International Cross Domain Conference and Workshop

Location: Lecture Hall B

1. Combining Goal-oriented and Problem-oriented Requirements Engineering Methods

Kristian Beckers, Stephan Faßbender, Maritta Heisel (University of Duisburg-Essen, Germany), Federica Paci (University Trento, Italy)

Abstract: Several requirements engineering methods exist that differ in their abstraction level and in their view on the system-to-be. Two fundamentally different classes of requirements engineering methods are goal- and problem-based methods. Goal-based methods analyze the goals of stakeholders towards the system-to-be. Problem-based methods focus on decomposing the development problem into simple sub-problems. Goal-based methods use a higher abstraction level that consider only the parts of a system that are relevant for a goal and provide the means to analyze and solve goal conflicts. Problem-based methods use a lower abstraction level that describes the entire system-to-be. A combination of these methods enables a seamless software development, which considers stakeholders' goals and a comprehensive view on the system-to-be at the requirements level. We propose a requirements engineering method that combines the goalbased method SI* and the problem-based method Problem Frames. We propose to analyze the issues between different goals of stakeholders first using the SI* method. Our method provides the means to use the resulting SI* models as input for the problem frame method. These Problem Frame models can be refined into architectures using existing research. Thus, we provide a combined requirements engineering method that considers all stakeholder views and provides a detailed system specification. We illustrate our method using an E-Health example.

2. GPRS Security for Smart Meters

Martin Gilje Jaatun, Inger Anne Tøndel (SINTEF ICT, Norway), Geir M. Køien (University of Agder, Norway)

Abstract: Many Smart Grid installations rely on General Packet Radio Service (GPRS) for wireless communication in Advanced Metering Infrastructures (AMI). In this paper we describe security functions available in GPRS, explaining authentication and encryption options, and evaluate how suitable it is for use in a Smart Grid environment. We conclude that suitability of GPRS depends on the chosen authentication and encryption functions, and on selecting a reliable and trustworthy mobile network operator.

3. Cloud-based Privacy Aware Preference Aggregation Service

Sourya Joyee De, Asim K. Pal (Indian Institute of Management Calcutta, India)

Abstract: Each day newer security and privacy risks are emerging in the online world. Users are often wary of using online services because they are not entirely confident of the level of security the provider is offering, particularly when such services may involve monetary transactions. Often the level of security in the algorithms underlying online and cloud-based services cannot be controlled by the user but is decided by the service provider. We propose a cloud-based Privacy Aware Preference Aggregation Service (PAPAS) that enables users to match preferences with other interested users of the service to find partners for negotiation, peer-groups with similar interests etc while also allowing users the ability to decide the level of security desired from the service, especially with respect to correct output and privacy of inputs of the protocol. It also lets users express their level of trust on the provider enabling or disabling it to act as a mediating agent in the protocols. Along with this we analyze the security of a preference hiding algorithm in the literature based on the security levels we propose for the PAPAS framework and suggest an improved version of the multi-party privacy preserving preference aggregation algorithm that does not require a mediating agent.

MoCrySEn VI – Interaction between Cryptographic Theory and Implementation Issues (Security Engineering Track) – 2nd International Workshop on Modern Cryptography and Security Engineering

Session Chair: Dimitris E. Simos (SBA Research, Austria)
Location: Lecture Hall C

1. Optimal Parameters for XMSS^{MT}
   Andreas Hülsing, Lea Rausch, Johannes Buchmann (TU Darmstadt, Germany)

   Abstract: We introduce Multi Tree XMSS (XMSS^{MT}), a hash-based signature scheme that can be used to sign a virtually unlimited number of messages. It is provably forward and hence EU-CMA secure in the standard model and improves key and signature generation times compared to previous schemes. XMSS^{MT} has – like all practical hash-based signature schemes – a lot of parameters that control different trade-offs between security, runtimes and sizes. Using linear optimization, we show how to select provably optimal parameter sets for different use cases.

2. Solving the Discrete Logarithm Problem for Packing Candidate Preferences
   James Heather, Chris Culnane, Steve Schneider (University of Surrey, UK), Sriramkrishnan Srinivasan, Zhe Xia (Wuhan University of Technology, China)

   Abstract: Ranked elections are used in many places across the world, and a number of end-to-end verifiable voting systems have been proposed to handle these elections recently. One example is the vVote system designed for the Victorian State Election, Australia. In this system, many voters will give a full ranking of up to 38 candidates. The easiest way to do this is to ask each voter to reorder ciphertexts representing the different candidates, so that the ciphertext ordering represents the candidate ranking. But this requires sending 38 ciphertexts per voter through the mixnets, which will take a long time. In this paper, we explore how to "pack" multiple candidate preferences into a single ciphertext, so that these preferences can be represented in the least number of ciphertexts possible, while maintaining efficient decryption. Both the packing and the unpacking procedure are performed publicly: we still provide 38 ciphertexts, but they are combined appropriately before they enter the mixnets, and after decryption, a meet-in-the-middle algorithm can be used to recover the full candidate preferences despite the discrete logarithm problem.

3. SPA on MIST Exponentiation Algorithm with Multiple Computational Sequences
   Chien-Ning Chen (Nanyang Technological University, Singapore), Jheng-Hong Tu, Sung-Ming Yen (National Central University, Taiwan)

   Abstract: The MIST algorithm is a randomized version of the division chain exponentiation algorithm and is a side-channel countermeasure. When analyzing the MIST algorithm by ordinary simple power analysis (with only one square-multiply sequence obtained), an attacker cannot retrieve the secret exponent due to the ambiguous relationship between the square-multiply sequence and the computation. We point out the MIST algorithm is still vulnerable to simple power analysis observing multiple power consumption traces and propose a practical method with detailed steps to deduce the secret exponent from multiple square-multiply sequences. Further countermeasures such as exponent blinding are required to prevent the analysis proposed in this paper.

ECTCM I – 1st International Workshop on Emerging Cyberthreats and Countermeasures

Session Chair: Markus Zeilinger (University of Applied Sciences Upper Austria, Austria)
Location: Lecture Hall D

1. GVScan: Scanning Networks for Global Vulnerabilities
   Fabrizio Baiardi, Fabio Corò, Federico Tonelli (University of Pisa, Italy), Luca Guidi (ENEL Engineering and Research SpA, Italy)

   Abstract: A global vulnerability is a set of vulnerabilities in one or several nodes of an ICT infrastructure. These vulnerabilities enable some attacks that may be sequentialized so that the privileges that each

attack requires are acquired through the previous ones. Current vulnerability scanners cannot discover global vulnerabilities because they analyze each node in isolation, without correlating the vulnerabilities in the same or in distinct nodes. To discover global vulnerabilities, an analysis has to correlate node vulnerabilities according to the architecture and the topology of the infrastructure. After defining a formal analysis to discover global vulnerabilities and the corresponding attack sequences, we present GVScan, a tool to automate the analysis based upon a classification of vulnerabilities. A first application of GVScan to a real infrastructure is described together with an evaluation of its accuracy.

2. Counteract DNS Attacks on SIP Proxies Using Bloom Filters

Ge Zhang, Simone Fischer-Hübner (Karlstad University, Sweden)

Abstract: SIP proxies play an important part in VoIP services. A Denial of Service (DoS) attack on them may cause the failure of the whole network. We investigate such a DoS attack by exploiting DNS queries. A SIP proxy needs to resolve domain names for processing a message. However, a DNS resolution may take a while. To avoid being blocked, a proxy suspends the processing task of the current message during its name resolution, so that it can continue to deal with other messages. Later when the answer is received, the suspended task will be resumed. It is an asynchronous implementation of DNS queries. Unfortunately, this implementation consumes memory storage and also brings troubles like a race condition. An attacker can collect a list of domain names which take seconds to resolve. Then, the attacker sends to a victim SIP proxy messages which contain these domain names. As a result, the victim proxy has to suspend a number of messages in a short while. Our experiments show that a SIP proxy can be easily crashed by such an attack and thus be not available anymore. To solve the problem, we analyzed the reasons that make a DNS query time-consuming, and then proposed a prevention scheme using bloom filters to blacklist suspicious DNS authoritative servers. Results of our experiments show it efficiently mitigates the attack with a reasonable false positive rate.

3. A Grammatical Inference Approach to Language-Based Anomaly Detection in XML

Harald Lampesberger (Christian Doppler Laboratory for Client-Centric Cloud Computing, Austria)

Abstract: False-positives are a problem in anomaly-based intrusion detection systems. To counter this issue, we discuss anomaly detection for the eXtensible Markup Language (XML) in a language-theoretic view. We argue that many XML-based attacks target the syntactic level, i.e. the tree structure or element content, and syntax validation of XML documents reduces the attack surface. XML offers so-called schemas for validation, but in real world, schemas are often unavailable, ignored or too general. In this work-in-progress paper we describe a grammatical inference approach to learn an automaton from example XML documents for detecting documents with anomalous syntax. We discuss properties and expressiveness of XML to understand limits of learnability. Our contributions are an XML Schema compatible lexical datatype system to abstract content in XML and an algorithm to learn visibly pushdown automata (VPA) directly from a set of examples. The proposed algorithm does not require the tree representation of XML, so it can process large documents or streams. The resulting deterministic VPA then allows stream validation of documents to recognize deviations in the underlying tree structure or datatypes.

4. Universal Peer-to-Peer Network Investigation Framework

Mark Scanlon, M-Tahar Kechadi (University College Dublin, Ireland)

Abstract: Peer-to-Peer (P2P) networking has fast become a useful technological advancement for a vast range of cybercriminal activities. Cybercrimes from copyright infringement and spamming, to serious, high financial impact crimes, such as fraud, distributed denial of service attacks (DDoS) and phishing can all be aided by applications and systems based on the technology. The requirement for investigating P2P based systems is not limited to the more well known cybercrimes listed above, as many more legitimate P2P based applications may also be pertinent to a digital forensic investigation, e.g, VoIP and instant messaging communications, etc. Investigating these networks has become increasingly difficult due to the broad range of network topologies and the ever increasing and evolving range of P2P based applications. This paper introduces the Universal Peer-to-Peer Network Investigation Framework (UP2PNIF); a framework which enables significantly faster and less labour intensive investigation of newly discovered P2P networks through the exploitation of the commonalities in network functionality. In combination with a reference database of known network protocols and characteristics, it is envisioned that any known P2P network can be instantly investigated using the framework. The framework can intelligently determine the best

methodology dependant on the focus of the investigation resulting in a significantly expedited evidence gathering process.

ARES-IND I – ARES Industrial Track

Session Chairs: Kari Jussila (Aalto University School of Science, Finland)
Juhani Anttila (International Academy for Quality (IAQ), Finland)
Location: Lecture Hall E

1. Introductory Talk

Juhani Anttila (International Academy for Quality (IAQ), Finland)

2. The Scourge of Internet Personal Data Collection

Esma Aïmeur, Manuel Lafond (Université de Montréal, Canada)

Abstract: In today's age of exposure, websites and Internet services are collecting personal data—with or without the knowledge or consent of users. Not only does new technology provide an abundance of methods for organizations to gather and store information, but people are also willingly sharing data with increasing frequency, exposing their intimate lives on social media websites such as Facebook, Twitter, Youtube, Myspace and others. Moreover, online data brokers, search engines, data aggregators and many other actors of the web are profiling people for various purposes such as the improvement of marketing through better statistics and an ability to predict consumer behaviour. Other less known reasons include understanding the newest trends in education, gathering people's medical history or observing tendencies in political opinions. People who care about privacy use the Privacy Enhancing Technologies (PETs) to protect their data, even though clearly not sufficiently. Indeed, as soon as information is recorded in a database, it becomes permanently available for analysis. Consequently even the most privacy aware users are not safe from the threat of re-identification. On the other hand, there are many people who are willing to share their personal information, even when fully conscious of the consequences. A claim from the advocates of open access information is that the preservation of privacy should not be an issue, as people seem to be comfortable in a world where their tastes, lifestyle or personality are digitized and publicly available. This paper deals with Internet data collection and voluntary information disclosure, with an emphasis on the problems and challenges facing privacy nowadays.

3. User Interface Harmonization for IT Security Management: User-Centered Design in the PoSecCo Project

Beatriz Gallego-Nicasio Crespo (Atos Research and Innovation, Spain)

Abstract: Quoting the National Institute of Standards and Technology (NIST), "the configuration of an information system and its components has a direct impact on the security posture of the system. [..] How those configurations are established and maintained requires a disciplined approach for providing adequate security" [1]. However, fitting the functional user needs is only one product success factor. In order to influence the acceptance of a software system by its target group of users, some factors such as the complexity of the system and its ease of use are also critical. The design approach followed by a user-centered engineering process focuses on the solution as a whole rather than on single components of the system, and on the user interface robustness rather than on system robustness. In this paper, we describe how usability and quality in use concepts, as defined by the standard ISO/IEC PDTR 9126-2/3/4 (Software Quality Metrics) [2], have been introduced in the design phases of the PoSecCo prototype. This paper summarizes the results of the analysis conducted in the PoSecCo project (www.posecco.eu), to group the six different organizational user roles of the project's integrated prototype (auditors and service provider's employees) into three main interface user group profiles: designers group, analytical group and consumers group. These three user group profiles define similar characteristics and requirements for what concern the usage of a graphical interface: visual attractiveness, general interaction with the functionalities offered and with the data managed by the system; reducing the effort and simplifying the subsequent design and implementation phases. The requirements associated to the user group profiles, as well as the task descriptions and information architecture, have been taken into account during the selection of the suitable technologies to implement the PoSecCo user interface, and in the development phases, in order to provide a harmonized and usable user interface for IT auditors and professionals of the security policy and configuration management areas.

RaSIEM II – 2nd International Workshop on Recent Advances in Security Information and Event Management

Session Chair: Roland Rieke (Fraunshofer SIT, Germany)

Location: Lecture Hall F

1. A Scalable SIEM Correlation Engine and its Application to the Olympic Games IT Infrastructure

   Valerio Vianello, Vincenzo Gulisano, Ricardo Jimenez-Peris, Marta Patiño-Martínez (Universidad Politécnica de Madrid, Spain), Rubén Torres, Rodrigo Díaz, Elsa Prieto (Atos Research & Innovation, Spain)

   Abstract: The security event correlation scalability has become a major concern for security analysts and IT administrators when considering complex IT infrastructures that need to handle gargantuan amounts of events or wide correlation window spans. The current correlation capabilities of Security Information and Event Management (SIEM), based on a single node in centralized servers, have proved to be insufficient to process large event streams. This paper introduces a step forward in the current state of the art to address the aforementioned problems. The proposed model takes into account the two main aspects of this field: distributed correlation and query parallelization. We present a case study of a multiple-step attack on the Olympic Games IT infrastructure to illustrate the applicability of our approach.

2. Reconsidering Intrusion Monitoring Requirements in Shared Cloud Platforms

   Kahina Lazri (Orange Labs & L2TI Laboratory, France), Sylvie Laniepce (Orange Labs, France), Jalel Ben-Othman (L2TI Laboratory, France)

   Abstract: Multi-tenancy is the core feature that enables efficiency and cost effectiveness of cloud computing. However, it brings several new security concerns. Ensuring strong isolation between co-localized tenants remains the most critical issue. This work aims at highlighting new attack strategies brought by the resource sharing paradigm in multi-tenant elastic IaaS Clouds in order to understand impacts of these attacks on the design of Intrusion Detection Systems in Cloud. The first part of this paper surveys the literature related to accepted vulnerabilities. Several Proofs of Concept are described and classified according to the results of the exploitation of these vulnerabilities. In the second part, we argue the existence of new attack strategies able to take advantage of the mechanisms which enable autonomic elasticity. These mechanisms are by nature sensitive to VMs resource consumption which can be easily manipulated by attacks. Finally, we give a representation of the presented vulnerabilities to engage a discussion on the limitations of pure user-centric security monitoring approaches for guaranteeing VM security

3. The Ontology of Metrics for Security Evaluation and Decision Support in SIEM Systems

   Igor Kotenko, Olga Polubelova, Igor Saenko, Elena Doynikova (St.Petersburg Institute for Informatics and Automationof the Russian Academy of Sciences (SPIIRAS), Russia)

   Abstract: Analysis of computer network security is a serious challenge. Many security metrics has been proposed for this purpose, but their effective use for rapid and reliable security evaluation and generation of countermeasures in SIEM systems remains an important problem. The use of ontologies for security information representation in SIEM systems contributes largely to the success of this task. However, most of works on ontological security data representation does not take into account the ontologies of security metrics. This paper proposes a new approach on using security metrics which is based on their ontological representation and serves for comprehensive security evaluation and subsequent countermeasure generation. The novelty of the proposed approach is that ontology of security metrics is viewed as a core component of a countermeasure decision support system. The proposed solutions are tested on a specific example.

4. Addressing security issues of Electronic Health Record systems through enhanced SIEM technology

   Cesario Di Sarno, Valerio Formicola (University of Naples Parthenope, Italy), Mario Sicuranza, Giovanni Paragliola (CAR-CNR, Italy)

Abstract: Electronic Health Records (EHR) are digital documents containing citizen medical information that can be used for advanced eHealth services, like emergency patient summary retrieving, historical data and events analysis, remote medical report access, e-Prescription. In this work we present the case study of an EHR management infrastructure, namely the InFSE, which implements a federated network of regional autonomous districts deployed on national scale. Despite the adoption of access control mechanisms based on authenticated transactions and assertions, the InFSE can be illegitimately used to retrieve patient health data and violate the citizen's privacy. We propose an enhanced Security Information and Event Management (SIEM) system, namely MASSIF, which is able to discover business logic anomalies and protect the identities of involved parties. In particular we focus on the software modules that perform sophisticated data aggregation and analysis, and provide fault and intrusion tolerant storage facilities, namely the Generic Event Translator, the Security Probes and the Trustworthy Event Storage. The components have been integrated on the widely used open source OSSIM SIEM and validated on a realistic testbed based on elements of the InFSE infrastructure.

12:30 – 14:00 Lunch

14:00 – 15:30 Parallel Sessions

ARES VII – Cryptography & Security Models – 8th International Conference on Availability, Reliability and Security

Location: Lecture Hall A

1. Scope of Security Properties of Sanitizable Signatures Revisited

Hermann de Meer, Henrich C. Pöhls, Joachim Posegga, Kai Samelin (University of Passau, Germany)

Abstract: Sanitizable signature schemes allow for altering signed data in a signer-controlled way by a semi-trusted third party. This is contrary to standard digital signature schemes, which do not permit any modifications by any party without invalidating the signature. Due to transparency, a strong privacy notion, outsiders cannot see if the signature for a message was created by the signer or by the semi-trusted party. Accountability allows the signer to prove to outsiders if a message was original or touched by the semi-trusted party. Currently, block-level accountability requires to drop transparency. We allow for accountability for sanitizable signatures with transparency on the block-level. Additionally, we generalize the concept of block-level properties to groups. This offers a even more fine-grained control and leads to more efficient schemes. We prove that group-level definitions imply both the block-level and message-level notions. We derive a provably secure construction, achieving our enhanced notions. A further modification of our construction achieves efficient grouplevel non-interactive public accountability. This construction only requires a constant amount of signature generations to achieve this property. Finally, we have implemented our constructions and the scheme introduced by *Brzuska* et al. at PKC'09 and provide a detailed performance analysis of our reference implementations.

2. The Common Limes Security Model for Asset Flow Control in Decentralized, Insecure Systems

Eckehard Hermann (University of Applied Sciences Upper Austria, Austria), Rüdiger Grimm (University Koblenz-Landau, Germany)

Abstract: Information and knowledge are assets. Therefore, authorization conflicts about information flow are subject to security concerns. The protection of information flow in a decentralized system is an important security objective in the business world. Once information is given away, there is an asymmetric relationship between the owner and the recipient of the information, because the owner has no control over a proper use or misuse by the recipient. The Common Limes Security Model (the "Limes model" for short) presented in this paper is a substantial extension of a simple model in [9]. It provides provable policies for asset (information) flow control. Rule elements are history and conflict functions maintained by the asset owners and protected by contracts between communication partners. If correctly implemented and enforced the rules of the Limes model guarantee the protection of assets from an unauthorized flow.

They allow an information object to stay in a secure state in a decentralized, i.e. in an insecure environment. This paper defines the model and proves the security of its rules.

3. Pretty Understandable Democracy - A Secure and Understandable Internet Voting Scheme

Jurlind Budurushi, Stephan Neumann, Maina M. Olembo, Melanie Volkamer (CASED / TU Darmstadt, Germany)

Abstract: Internet voting continues to raise interest. A large number of Internet voting schemes are available, both in use, as well as in research literature. While these schemes are all based on different security models, most of these models are not adequate for high-stake elections. Furthermore, it is not known how to evaluate the understandability of these schemes (although this is important to enable voters' trust in the election result). Therefore, we propose and justify an adequate security model and criteria to evaluate understandability. We also describe an Internet voting scheme, Pretty Understandable Democracy, show that it satisfies the adequate security model and that it is more understandable than Pretty Good Democracy, currently the only scheme that also satisfies the proposed security model.

CD-ARES VI – Risk management and Business continuity– International Cross Domain Conference and Workshop

Location: Lecture Hall B

1. A Method for Re-Using existing ITIL processes for creating an ISO 27001 ISMS process applied to a high availability video conferencing cloud scenario

Kristian Beckers (University of Duisburg-Essen, Germany), Stefan Hofbauer (Amadeus Data Processing GmbH, Germany), Gerald Quirchmayr (University of Vienna, Austria & University of South Australia, Australia), Christopher C. Wills (CARIS Research Ltd., UK)

Abstract: Many companies have already adopted their business processes to be in accordance with defined and organized standards. Two standards that are sought after by companies are IT Infrastructure Library (ITIL) and ISO 27001. Often companies start certifying their business processes with ITIL and continue with ISO 27001. For small and medium-sized businesses, it is difficult to prepare and maintain the ISO 27001 certification. The IT departments of these companies often do not have the time to fully observere standards as part of their daily routine. ITIL and ISO 27001 perfectly fit into companies and help reduce errors through the standardization and comparability of products and services between themselves and other companies and partners. ISO 27001 specifically looks at security risks, countermeasures and remedial actions. We start with the processes that need to be in place for implementing ITIL in an organisation's business processes. We use a cloud service provider as a running example and compare ITIL processes with ISO 27001 processes. We identify which aspects of these two standards can be better executed. We propose a mapping between ITIL and ISO 27001 that makes them easier to understand and assists with the certification process. We show further how to prepare for audits as well as re-certification. Often, these two processes are seen separately and not in conjunction, where synergies can be exploited. Legal requirements, compliance and data security play an integral part in this process. In essence, we present checklists and guidelines for companies who want to prepare for standardization or that are already certified, but want to improve their business processes. We illustrate our method using an high availability video conferencing cloud example.

2. Towards Improved Understanding and Holistic Management of the Cyber Security Challenges in Power Transmission Systems

Inger Anne Tøndel (SINTEF ICT, Norway), Bodil Aamnes Mostue (SINTEF Technology and Society, Norway), Martin Gilje Jaatun (SINTEF ICT, Norway), Gerd Kjølle (SINTEF Energy Research, Norway)

Abstract: Information and Communication Technology (ICT) is increasingly utilised in the electrical power transmission system. For the power system, ICT brings a lot of benefits, but it also introduces new types of vulnerabilities and threats. Currently the interdependencies between the power and ICT system are not fully understood, including how threats (both malicious and accidental) towards the ICT system may impact on power delivery. This paper addresses the need for improved understanding between ICT

security and power experts. It explains important terms used differently in the two disciplines, identifies main impacts on power systems that may result from ICT incidents, and proposes a set of indicators that can be used as a basis for selecting measures.

3. Seeking Risks: Towards a Quantitative Risk Perception Measure
Åsmund Ahlmann Nyre (Norwegian University of Science and Technology & SINTEF ICT, Norway), Martin Gilje Jaatun (SINTEF ICT, Norway)

Abstract: Existing instruments for measuring risk perception have focused on an abstract version of the concept, without diving into the the details of what forms the perception of likelihood and impact. However, as information security risks become increasingly complex and difficult for users to understand, this approach may be less feasible. The average user may be able to imagine the worst case scenario should an asset be compromised by an attacker, but he has few means to determine the likelihood of this happening. In this paper we therefore propose a different approach to measuring risk perception. Based on well established concepts from formal risk analysis, we define an instrument to measure users' risk perception that combines the strengths of both traditional risk perception and formal risk analysis. By being more explicit and specific concerning possible attackers, existing security measures and vulnerabilities, users will be more able to give meaningful answers to scale items, thereby providing a better and more explanatory measure of risk perception. As part of the instrument development we also elaborate on construct definitions, construct types and the relationship between these and the corresponding risk perception instrument. Although it remains to be verified empirically, the validity of the measure is discussed by linking it to well established theory and practice.

MoCrySEn VII – Database Encryption & Software and Hardware Implementation of Cryptographic Algorithms (Security Engineering Track) – 2nd International Workshop on Modern Cryptography and Security Engineering

Session Chair: Dimitris E. Simos (SBA Research, Austria)
Location: Lecture Hall C

1. Cumulus4j: A Provably Secure Database Abstraction Layer
Matthias Huber, Matthias Gabel, Marco Schulze, Alexander Bieber (Karlsruhe Institute of Technology (KIT), NightLabs Consulting GmbH, Germany)

Abstract: Cloud Computing has huge impact on IT systems. It offers advantages like exibility and reduced costs. Privacy and security issues, however, remain a major drawback. While data can be secured against external threats using standard techniques, service providers themselves have to be trusted to ensure privacy. In this paper, we present a novel technique for secure database outsourcing. We provide the security notion Ind-ICP that focuses on hiding relations between values. We prove the security of our approach and present benchmarks showing the practicability of this solution. Furthermore, we developed a plug-in for a persistence layer. Our plug-in de- and encrypts sensitive data transparently to the client application. By using encrypted indices, queries can still be executed efficiently.

2. Code-Based Identification and Signature Schemes in Software
Sidi Mohamed El Yousfi Alaoui (CASED, Germany), Pierre-Louis Cayrel (Laboratoire Hubert Curien, France), Rachid El Bansarkhani, Gerhard Hoffmann (Technische Universität Darmstadt, Germany)

Abstract: In this paper we present efficient implementations of several code-based identification schemes, namely the Stern scheme, the Véron scheme and the Cayrel-Véron-El Yousfi scheme. We also explain how to derive and implement signature schemes from the previous identification schemes using the Fiat-Shamir transformation. For a security of 80 bits and a document to be signed of size 1 kByte, we reach a signature in about 4 ms on a standard CPU.

3. Discussion on Security Engineering

ECTCM II – 1st International Workshop on Emerging Cyberthreats and Countermeasures

Session Chair: Peter Schoo (Fraunhofer AISEC, Germany)

Location: Lecture Hall D

1. Hiding Privacy Leaks in Android Applications Using Low-Attention Raising Covert Channels

   Jean-Francois Lalande (Université d'Orléans, France), Steffen Wendzel (Fraunhofer FKIE, Germany)

   Abstract: Covert channels enable a policy-breaking communication not foreseen by a system's design. Recently, covert channels in Android were presented and it was shown that these channels can be used by malware to leak confidential information (e.g., contacts) between applications and to the Internet. Performance aspects as well as means to counter these covert channels were evaluated. In this paper, we present novel covert channel techniques linked to a minimized footprint to achieve a high covertness. Therefore, we developed a malware that slowly leaks collected private information and sends it synchronously based on four covert channel techniques. We show that some of our covert channels do not require any extra permission and escape well know detection techniques like TaintDroid. Experimental results confirm that the obtained throughput is correlated to the user interaction and show that these new covert channels have a low energy consumption – both aspects contribute to the stealthiness of the channels. Finally, we discuss concepts for novel means capable to counter our covert channels and we also discuss the adaption of network covert channel features to Android-based covert channels.

2. ANANAS – A Framework For Analyzing Android Applications

   Thomas Eder, Michael Rodler, Dieter Vymazal, Markus Zeilinger (University of Applied Sciences Upper Austria, Austria)

   Abstract: Android is an open software platform for mobile devices with a large market share in the smartphone sector. The openness of the system as well as its wide adoption lead to an increasing amount of malware developed for this platform. ANANAS is an expandable and modular framework for analyzing Android applications. It takes care of common needs for dynamic malware analysis and provides an interface for the development of plugins. Adaptability and expandability have been main design goals during the development process. An abstraction layer for simple user interaction and phone event simulation is also part of the framework. It allows an analyst to script the required user simulation or phone events on demand or adjust the simulation to his needs. Six plugins have been developed for ANANAS. They represent well known techniques for malware analysis, such as system call hooking and network traffic analysis. The focus clearly lies on dynamic analysis, as five of the six plugins are dynamic analysis methods.

3. Cuteforce Analyzer: A Distributed Bruteforce Attack on PDF Encryption with GPUs and FPGAs

   Bianca Danczul, Jürgen Fuß, Stefan Gradinger, Bernhard Greslehner-Nimmervoll, Wolfgang Kastl, Florian Wex (University of Applied Sciences Upper Austria, Austria)

   Abstract: Working on cryptanalytic tasks using a heterogeneous cluster with different types of processors (CPU, GPU, FPGA) can be an advantage over classical homogeneous clusters. In this paper we demonstrate that distributing cryptanalytics tasks to different types of processors can lead to better performance than can be achieved using a single type of processor. To this end we have built a framework for the management of a heterogeneous cluster and implanted a password bruteforcer for password protected PDF documents. Our results show that such a framework can be implemented with little overhead in terms of performance.

4. Collaboratively Exchanging Warning Messages Between Peers While under Attack

   Mirko Haustein, Herbert Sighart (Cassidian / EADS Deutschland GmbH, Germany), Dennis Titze, Peter Schoo (Fraunhofer AISEC, Germany)

   Abstract: Secure Multi-party Computation (MPC) allows a secure joint cooperation within a distributed group of peers. In this paper we investigate an extended Secure MPC solution that allows mutual information exchange and distribution of warnings among a group of participating peers within an information sharing network. The implementation of this MPC solution is deployed in a peer-to-peer

network. This paper evaluates the performance of the implementation based on two scenarios that stress the network load and thus simulate the implementation under attack. Using a network simulation provides a connection between a simulated network model and real systems by use of System-in-the-loop (SITL) technology for the validation of the considered MPC implementation.

ARES-IND II – ARES Industrial Track

Session Chairs: Kari Jussila (Aalto University School of Science, Finland)
Juhani Anttila (International Academy for Quality (IAQ), Finland)
Location: Lecture Hall E

1. Overview of Recent Advances in CCTV Processing Chain in the INDECT and INSIGMA Projects
   Andrzej Dziech, Jarosław Białas, Andrzej Glowacz, Paweł Korus, Mikołaj Leszczuk, Andrzej Matiolanski (AGH University of Science and Technology, Poland), Remigiusz Baran (Kielce University of Technology, Poland)

   Abstract: Intelligent monitoring is currently one of the most prominent research areas. Numerous aspects of such schemes need to be addressed by implementation of various modules covering a wide range of algorithms, beginning from video analytic modules, through quality assessment, up to integrity verification. The goal of this paper is to provide a brief overview of the most recent research results regarding various aspects of the video surveillance processing chain. Specifically, the paper describes a scheme for automatic recognition of the make and model of passing vehicles, the state-of-the-art in quality assessment for recognition tasks, and a system for verification of digital evidence integrity. Concluding remarks highlight the perspectives for further development of the described techniques, and the related research directions.

2. TRESCCA - Trustworthy Embedded Systems for Secure Cloud Computing
   Gunnar Schomaker (OFFIS, Germany), Andreas Herrholz (CoSynth, Germany), Guillaume Duc (Institut Mines-Telecom, France), Renaud Pacalet (Institut Mines-Telecom, France), Salvatore Raho (Virtual Open Systems, France), Miltos Grammatikakis (Technological Educational Institute of Crete, Greece), Marcello Coppola (ST Microelectronics, France), Ignacio Garcia Vega (Wellness Telecom, Spain)

   Abstract: Cloud Computing is an inevitable trend. In the near future almost every consumer electronic device will be connected to an ecosystem of third-party service partners, providing applications like payment systems, streamed content, etc using or producing sensitive data. The challenge is, that current cloud operators and their end users do not always trust each other. This lack of trust limits the potential of the cloud computing market. The TRESCCA project aims to lay the foundations of a secure and trustable cloud platform, by ensuring strong logical and physical security on the client devices, using both hardware security and virtualization techniques, while considering the whole cloud service architecture. The project will propose and demonstrate hardware/software solutions allowing stakeholders to delegate the processing of their sensitive data to a remote processing engine, opening up a new field of cloud services and applications. The TRESCCA approach avoids undesirable paradigm shifts, both in the software and in the hardware by complementing existing legacy solutions by non-intrusive add-ons.

3. Discussion

RaSIEM III – 2nd International Workshop on Recent Advances in Security Information and Event Management

Session Chair: Mohammed Achemlal (France Télécom-Orange, France)
Location: Lecture Hall F

1. Experiences and Challenges in Enhancing Security Information and Event Management Capability using Unsupervised Anomaly Detection
   Stefan Asanger (University of Cape Town, South Africa), Andrew Hutchison (T-Systems South Africa, South Africa)

Abstract: Security Information and Event Management (SIEM) systems are important components of security and threat management in enterprises. To compensate for the shortcomings of rule-based correlation in this field, there has been an increasing demand for advanced anomaly detection techniques. Such implementations, where prior training data is not required, have been described previously. In this paper, we focus on the requirements for such a system and provide insight into how diverse security events need to be parsed, unified and preprocessed to meet the requirements of unsupervised anomaly detection algorithms. Specific focus is given to the detection of suspicious authentication attempts, password guessing attacks and unusual user account activities in a large-scale Microsoft Windows domain network. In the course of this paper we analyze a comprehensive dataset of 15 million Windows security events from various perspectives using the *k*-nearest neighbor algorithm. Key considerations on how to effectively apply anomaly detection are proposed in order to produce accurate and convincing results. The effectiveness of our approach is discussed using sample anomalies that were detected in the analyzed data.

2. Fraud Detection in Mobile Payment Utilizing Process Behavior Analysis
Roland Rieke, Maria Zhdanova, Jürgen Repp (Fraunhofer SIT, Germany), Romain Giot, Chrystel Gaber (France Télécom-Orange Labs, France)

Abstract: Generally, fraud risk implies any intentional deception made for financial gain. In this paper, we consider this risk in the field of services which support transactions with electronic money. Specifically, we apply a tool for predictive security analysis at runtime which observes process behavior with respect to transactions within a money transfer service and tries to match it with expected behavior given by a process model. We analyze deviations from the given behavior specification for anomalies that indicate a possible misuse of the service related to money laundering activities. We evaluate the applicability of the proposed approach and provide measurements on computational and recognition performance of the tool – Predictive Security Analyzer – produced using real operational and simulated logs. The goal of the experiments is to detect misuse patterns reflecting a given money laundering scheme in synthetic process behavior based on properties captured from real world transaction events.

3. Invited Presentation – Contemporary SCADA system, their design and usage
Gunnar Björkman (ABB, Germany)

Abstract: Computerized control systems, so called Supervisory, Control and Data Acquisition (SCADA) systems, are regularly used for the supervision and control of the electrical grid. This type of control systems represents a mature technology that has been used since more than 40 years. They can be seen specialized SIEM systems dedicated for a specific process. Among very many other applications, the Event and Alarming Handling functionality is an important part of each SCADA system where a very high amount of events are collected in a short time and where the system must correctly filter, analyze and alert the operators in an intelligent way. Examples when the alarming function has failed and the very severe consequences of such failures will be given.
Another essential part of a SCADA system is the model-based analysis of incoming process events. SCADA systems includes a mathematical model of the supervised process which is used to make advanced, higher level alarming and to make predictions of the future process states and recommendations for how to operate the process to avoid potential disturbances. In order to make this model-based analysis the process models must be created and maintained. This Data Engineering process is also an important, and not to be ignored, part in the use of SCADA systems.
This presentation will give an overview of contemporary SCADA system for the electrical grid, a short description of their evolution, their design and usage. Special emphasis will be given to the event and alarming functionality, the model based analysis and to data maintenance.

15:30 – 16:00 Coffee Break

16:00 – 17:30 Parallel Sessions

ARES VIII – Privacy & Network Security – 8th International Conference on Availability, Reliability and Security

Location: Lecture Hall A

1. Limiting MitM to MitE Covert-Channels
   Amir Herzberg (Bar Ilan University, Israel), Haya Shulman (TU Darmstadt, Germany & Bar Ilan University, Israel)

   Abstract: We study covert channels between a MitM attacker, and her MitE 'malware', running within the protected network of a victim organisation, and how to prevent or limit such channels. Our focus is on advanced timing channels, that allow communication between the MitM and MitE, even when hosts inside the protected network are restricted to only communicate to other (local and remote) hosts in the protected network. Furthermore, we assume communication is encrypted with fixed packet size (padding). We show that these do not suffice to prevent covert channels between MitM and MitE; furthermore, we show that even if we restrict communication to a constant rate, e.g., one packet every second, communication from MitE to MitM is still possible. We present efficient traffic shapers against covert channels between MitM and MitE. Our solutions preserve efficiency and bounded delay (QoS), while limiting covert traffic leakage, in both directions.

2. Privacy Panel: Usable and Quantifiable Mobile Privacy
   Debmalya Biswas (Iprova, Switzerland), Imad Aad (University of Bern, Switzerland), Gian Paolo Perrucci (Nespresso, Switzerland)

   Abstract: The ever increasing popularity of apps stems from their ability to provide highly customized services to the user. The flip side is that in order to provide such services, apps need access to very sensitive private information about the user. This leads to malicious apps that collect personal user information in the background and exploit it in various ways. Studies have shown that current app vetting processes which are mainly restricted to install time verification mechanisms are incapable of detecting and preventing such attacks. We argue that the missing fundamental aspect here is a comprehensive and usable mobile privacy solution, one that not only protects the user's location information, but also other equally sensitive user data such as the user's contacts and documents. A solution that is usable by the average user who does not understand or care about the low level technical details. To bridge this gap, we propose privacy metrics that quantify low-level app accesses in terms of privacy impact and transforms them to high-level user understandable ratings. We also provide the design and architecture of our Privacy Panel app that represents the computed ratings in a graphical user-friendly format and allows the user to define policies based on them. Finally, experimental results are given to validate the scalability of the proposed solution.

3. A Privacy-Preserving Entropy-Driven Framework for Tracing DoS Attacks in VoIP
   Zisis Tsiatsikas (University of the Aegean, Greece), Dimitris Geneiatakis (Joint Research Center, Italy), Georgios Kambourakis (Joint Research Center, Italy), Angelos D. Keromytis (Columbia University, USA)

   Abstract: Network audit trails, especially those composed of application layer data, can be a valuable source of information regarding the investigation of attack incidents. Nevertheless, the analysis of log files of large volume is usually both complex (slow) and privacy-neglecting. Especially, when it comes to VoIP, the literature on how audit trails can be exploited to identify attacks remains scarce. This paper provides an entropy-driven, privacy-preserving, and practical framework for detecting resource consumption attacks in VoIP ecosystems. We extensively evaluate our framework under various attack scenarios involving single and multiple assailants. The results obtained show that the proposed scheme is capable of identifying malicious traffic with a false positive alarm rate up to 3.5%.

4. On Secure Multi-Party Computation in Bandwidth-Limited Smart-Meter Systems
   Mario Kirschbaum, Thomas Plos, Jörn-Marc Schmidt (Graz University of Technology, Austria)

Abstract: The emergence of decentralized energy production pushes the deployment of smart-grid solutions. While the availability of fine-grained consumption data via smart-meter measurements provides several advantages for energy providers (e.g., grid automation, accurate forecasts), they also raise concerns about the privacy of the users. In this paper we present an efficient and privacy-aware communication protocol for future smart-grid solutions. The protocol is based on secure multi-party computation (SMC) and allows deducing the aggregated consumption data of a group of smart meters without disclosing the consumption data of individual smart meters. Moreover, by using a special initialization phase the communication effort is significantly reduced compared to classical SMC-based approaches. For aggregating the consumption data of 100 smart meters, our proposed protocol requires less than one second when assuming a communication bandwidth of 100 kbits/s.

Panel Discussion

Location: Lecture Hall B

Threats & Risk Management - Bridging the Gap between Industry needs and Research

Moderated by *Martin Gilje Jaatun (SINTEF, NO)*

Panel discussion with

- *Gary McGraw (Cigital, US)*
- *Greg Soukiassian (BC & RS, France)*
- *Chris Wills (CARIS Research, UK)*

Where do security technologies come from? Grants are proposed by academics and funded by the government. Startups move technologies across the "valley of death" to early adopters. Idea generation is perhaps ten percent of innovation; most of the work is on technology transfer and adoption. Chance plays a big role in terms of creating opportunities, but a company's success depends on its ability to make good opportunities more likely and to capitalize on opportunities that do arise. Taking a great idea from the lab out into the world is hard work with many perils and pitfalls (including the "research valley of death"). Passionate individuals drive technology transfer more than process, with some people believing that the original researchers need to be personally involved all the way along. Prototyping is an important practice, often resulting in "researchware" that proves a concept but is not ready for common use.

Risk management means many different things to different people. Practitioners, researchers, and academics all have their own perspective. International standards such as the ISO/IEC 27K series provide a decent starting point for understanding and debating what risk management is. How should such standards impact research and development of new technologies? What can be done to make standards work in practice for small and medium-sized enterprises? Finally, what impact should standards have on innovation, if any?

RaSIEM IV – Demonstrations & Closing – 2nd International Workshop on Recent Advances in Security Information and Event Management

Session Chair: Roland Rieke (Fraunhofer SIT, Germany)

Location: Lecture Hall F

1. Mobile Money Transfer Scenario

   Chrystel Gaber (France Télécom-Orange Labs, France)

   Abstract: The field of MMT is a growing market segment, particularly in developing countries where banking systems may not be as dense or available as in developed countries. For example, M-Pesa, which was launched in 2007 in Kenya, displayed in December 2011 about 19 million subscribers, namely 70% of all mobile subscribers in Kenya. Orange Money is deployed in 10 countries and gathers around 14% of the mobile subscribers of these countries. In such services, transactions are made with electronic money, called mMoney. The users can convert cash to mMoney through distributors and use it to purchase goods

at merchants, pay bills or transfer it to other users. Like any other money transfer service, this service is exposed to the risk of money laundering, i.e., misuse through disguising illegally obtained funds to make them seem legal, and more generally fraud risk that implies any intentional deception made for financial gain.

The demonstration's objective is to highlight the results of the European FP7 project MASSIF in terms of components integration and their adaptation to the Mobile Money Transfer Scenario. All MASSIF modules are illustrated from the collection of events to the enforcement of countermeasures after a fraud is detected and a component based on process behavior analysis is highlighted. The misuse case showcased is related to money laundering and in particular, a specific use of mules. More details about the misuse case and the way it is detected are detailed and discussed in the article "Fraud Detection in Mobile Payments Utilizing Process Behavior Analysis" also presented in the RaSIEM workshop.

2. Critical Infrastructure Protection Scenario demonstration synopsis
Valerio Formicola (University of Naples Parthenope, Italy)

Abstract: As a consequence of the technology shift and of new economical and socio-political motivations, coordinated and targeted cyber-attacks to Critical Infrastructures (CIs) are increasing and becoming more sophisticated. Mostly, such infrastructures rely on legacy Supervisory Control And Data Acquisition (SCADA) systems that have been designed without having security in mind - originally they were isolated proprietary systems - and that are managed by people with good skills in the specific application domains, but with very limited knowledge of security.
Security of SCADA is traditionally approached by reusing systems designed to protect solely Information Technology (IT) based infrastructures. One of the most effective solutions is represented by Security Information and Events Management (SIEM) systems. Unfortunately, according to the National Institute of Standards and Technology (NIST), securing a Critical Infrastructure is very much different from protecting solely IT-based infrastructures, hence traditional SIEMs are often ineffective for CIs protection.
This demo is aimed at demonstrating the usage of the MASSIF framework to overcome some of the limits of traditional SIEM technologies. In particular the demo shows how the interaction among most of the MASSIF components, allows to deal with internal attacks by processing heterogeneous events coming from a number of data sources.
The demonstration is operated with respect to a very challenging case study, namely the control system of a dam. Since September 2009 dams are classified as critical infrastructures and thus they are being increasingly monitored against malicious faults. Some of the main MASSIF framework features demonstrated by the demo include: i) correlation of heterogeneous data sources; ii) attack prediction; iii) cyber-physical convergence; and iv) decision support for reaction and remediation.

3. Summary of the MASSIF project and link to other SIEM advances
Elsa Prieto (Atos Research & Innovation, Spain)

18:00 – 19:30 Sightseeing Tour

Thursday, 05 September 2013

08:00 – 17:30 Registration for all events

09:00 – 10:30 Parallel Sessions

Tutorial

Location: Lecture Hall A

DNS Security (Part I)

Haya Shulman (TU Darmstadt, Germany)

Abstract: Most caching DNS resolvers rely for their security, against poisoning, on challenge-response defenses, whereby the resolvers validate that the DNS responses contain some 'unpredictable' values, copied from the request. These mechanisms include the 16 bit identifier, source port, and other fields, randomised and validated by different 'patches' to DNS. We investigate the proposed and widely deployed patches, and show how off-path attackers can often circumvent all of them, exposing the resolvers to cache poisoning attacks.

We discuss DNSSEC, which provides the best defense for DNS, as well as some short-term countermeasures.

ARES IX – Threat Modeling & Intrusion Detection – 8th International Conference on Availability, Reliability and Security

Location: Lecture Hall F

1. Detection of Hidden Fraudulent URLs within Trusted Sites Using Lexical Features
   Enrico Sorio, Alberto Bartoli, Eric Medvet (University of Trieste, Italy)

   Abstract: Internet security threats often involve the fraudulent modification of a web site, often with the addition of new pages at URLs where no page should exist. Detecting the existence of such hidden URLs is very difficult because they do not appear during normal navigation and usually are not indexed by search engines. Most importantly, driveby attacks leading users to hidden URLs, for example for phishing credentials, may fool even tech-savvy users, because such hidden URLs are increasingly hosted within trusted sites, thereby rendering HTTPS authentication ineffective. In this work, we propose an approach for detecting such URLs based only on their lexical features, which allows alerting the user before actually fetching the page. We assess our proposal on a dataset composed of thousands of URLs, with promising results.

2. SHPF: Enhancing HTTP(S) Session Security with Browser Fingerprinting
   Thomas Unger (FH Campus Wien, Austria), Martin Mulazzani, Dominik Frühwirt, Markus Huber, Sebastian Schrittwieser, Edgar Weippl (SBA Research, Austria)

   Abstract: Session hijacking has become a major problem in today's Web services, especially with the availability of free off-the-shelf tools. As major websites like Facebook, Youtube and Yahoo still do not use HTTPS for all users by default, new methods are needed to protect the users' sessions if session tokens are transmitted in the clear. In this paper we propose the use of browser fingerprinting for enhancing current state-of-the-art HTTP(S) session management. Monitoring a wide set of features of the user's current browser makes session hijacking detectable at the server and raises the bar for attackers considerably. This paper furthermore identifies HTML5 and CSS features that can be used for browser fingerprinting and to identify or verify a browser without the need to rely on the UserAgent string. We implemented our approach in a framework that is highly configurable and can be added to existing Web applications and server-side session management with ease.

3. An Analysis and Evaluation of Security Aspects in the Business Process Model and Notation

Maria Leitner, Michelle Miller, Stefanie Rinderle-Ma (University of Vienna, Austria)

Abstract: Enhancing existing business process modeling languages with security concepts has attracted increased attention in research and several graphical notations and symbols have been proposed. How these extensions can be comprehended by users has not been evaluated yet. However, the comprehensibility of security concepts integrated within business process models is of utmost importance for many purposes such as communication, training, and later automation within a process-aware information system. If users do not understand the security concepts, this might lead to restricted acceptance or even misinterpretation and possible security problems in the sequel. In this paper, we evaluate existing security extensions of Business Process Model and Notation (BPMN) as BPMN constitutes the de facto standard in business modeling languages nowadays. The evaluation is conducted along two lines, i.e., a literature study and a survey. The findings of both evaluations identify shortcomings and open questions of existing approaches. This will yield the basis to convey security-related information within business process models in a comprehensible way and consequently, unleash the full effects of security modeling in business processes.

4. The Big Four – What We Did Wrong in Advanced Persistent Threat Detection?

Nikos Virvilis, Dimitris Gritzalis (Athens University of Economics & Business (AUEB), Greece)

Abstract: As both the number and the complexity of cyber-attacks continuously increase, it is becoming evident that current security mechanisms have limited success in detecting sophisticated threats. Stuxnet, Duqu, Flame and Red October have troubled the security community due to their severe complexity and their ability to evade detection – in some cases for several years. The significant technical and financial resources needed for orchestrating such complex attacks are a clear indication that perpetrators are well organized and, likely, working under a state umbrella. In this paper we perform a technical analysis of these advanced persistent threats, highlighting particular characteristics and identifying common patterns and techniques. We also focus on the issues that enabled the malware authors to evade detection from a wide range of security solutions and propose technical countermeasures for strengthening our defenses against similar threats.

CD-ARES VII - Security and Privacy & Location Based Applications – International Cross Domain Conference and Workshop

Location: Lecture Hall E

1. A Framework for Combining Problem Frames and Goal Models to Support Context Analysis during Requirements Engineering

Nazila Gol Mohammadi, Azadeh Alebrahim, Thorsten Weyer, Maritta Heisel, Klaus Pohl (University of Duisburg-Essen, Germany)

Abstract: Quality requirements, like security requirements, are difficult to elicit, especially if they cross multiple domains. Understanding these domains is an important issue in the requirements engineering process for the corresponding systems. Well-known requirements engineering approaches, such as goal-oriented techniques provide a good starting point in capturing security requirements in the form of soft-goals in the early stage of the software engineering process. However, such approaches are not sufficient for context and problem analysis. On the other hand, the context and problem modeling approaches like e.g., problem frames, do not address the system goals. Integrating the relevant context knowledge into goal models is a promising approach to address the mutual limitations. In this paper, we propose a framework for combining goal models and problem frames. The framework makes it possible to document the goals of the system together with the corresponding knowledge of the system's context. Furthermore, it supports the process of refining (soft-) goals right up to the elicitation of corresponding security requirements. To show the applicability of our approach, we illustrate its application on a real-life case study concerning Smart Grids.

2. Towards a Pervasive Access Control within Video Surveillance Systems
Dana Al Kukhun (Amman Arab University, Jordan), Dana Codreanu, Ana-Maria Manzat, Florence Sedes (Universite de Toulouse, France)

Abstract: This paper addresses two emerging challenges that multimedia distributed systems have to deal with: the user's constant mobility and the information's sensitivity. The systems have to adapt, in real time, to the user's context and situation in order to provide him with relevant results without breaking the security and privacy policies. Distributed multimedia systems, such as the one proposed by the LINDO project, do not generally consider both issues. In this paper, we apply an access control layer on top of the LINDO architecture that takes into consideration the user's context and situation and recommends alternative resources to the user when he is facing an important situation. The proposed solution was implemented and tested in a video surveillance use case.

TWISNet I – International Workshop on Trustworthy Wireless Industrial Sensor Networks

Session Chair: Markus Wehner (Hochschule für Technik und Wirtschaft Dresden, Germany)
Location: Lecture Hall D

1. Introduction to Wireless Sensor Networks/6LoWPAN
2. Discussion on Scenarios and Threats in WSNs

10:30 – 11:00 Coffee Break

11:00 – 12:30 Parallel Sessions

Tutorial

Location: Lecture Hall A

DNS Security (Part II)
Haya Shulman (TU Darmstadt, Germany)

ARES X – Authentication, Identity Management & Trust – 8th International Conference on Availability, Reliability and Security

Location: Lecture Hall F

1. Towards Web-based Biometric Systems Using Personal Browsing Interests
Lukasz Olejnik, Claude Castelluccia (INRIA, France)

Abstract: We investigate the potential to use browsing habits and browser history as a new authentication and identification system for the Web with potential applications to anomaly and fraud detection. For the first time, we provide an empirical analysis using data from 4, 578 users. We employ the traditional biometric analysis and show that the False Acceptance Rate can be low (FAR = 1.1%), though this results in a relatively high False Rejection Rate (FRR = 13.8%). The scheme may either be utilized by Web service providers (with access to user's browser history) or any Webmaster, using other specialized techniques such as timing based browser cache sniffing or a browser extension. We construct such a proof-of-concept extension.

2. Resource Pool Oriented Trust Management for Cloud Infrastructure
Gansen Zhao, Haiyu Wang, Yong Tang (South China Normal University, China), Chunming Rong (University of Stavanger, Norway)

Abstract: IaaS encourages pooled resource management model, which provides transparency on the management and provision of IT resources. The transparency, hiding physical details of the underlying

resources, makes it difficult for cloud users/services to identify trusted resources for service deployment, resulting in potential risks of deploying critical services on untrusted resources. This paper proposes a pool oriented trust management mechanism for cloud infrastructures, allowing the construction and identification of trusted clusters consisted of trusted resources, with strict membership management to accept only trusted physical resources. Resources of a trusted cluster expose identical trust properties/attributes to cloud users, enabling users to verify the trust on the resources without the need of identifying individual physical resource. Hence, service deployment and migration can be augmented with the above trust verification to ensure that services are always deployed on trusted resources.

3. The Trusted Attribute Aggregation Service (TAAS): Providing an Attribute Aggregation Layer for Federated Identity Management
David W Chadwick, George Inman (University of Kent, UK)

Abstract: We describe a web based federated identity management system loosely based on the user centric Windows CardSpace model. Unlike CardSpace that relies on a fat desktop client (the identity selector) in which the user can only select a single card per session, our model uses a standard web browser with a simple plugin that connects to a trusted attribute aggregation web service (TAAS). TAAS supports the aggregation of attributes from multiple identityproviders (IdPs) and allows the user to select multiple single attribute "cards" in a session, which more accurately reflects real life in which users may present several plastic cards and self-asserted attributes in a single session. Privacy protection, user consent, and ease of use are critical success factors. Consequently TAAS does not know who the user is, the user consents by selecting the attributes she wants to release, and she only needs to authenticate to a single IdP even though attributes may be aggregated from multiple IdPs. The system does not limit the authentication mechanisms that can be used, and it protects the user from phishing attacks by malicious SPs.

4. A Novel Proximity Based Trust Model for Opportunistic Networks
Mai H. EL-Sherief, Marianne A. Azer (Nile University, Egypt)

Abstract: "Trust should be earned". This is a famous quote that we use everyday implicitly or explicitly. Trust often is an inherent characteristic of our daily life, but in the digital community and between devices how can we represent trust? Since our mobile and digital devices became our confidants, we cannot share the information embedded in these devices with other devices without establishing trust. Hence, in this research a proximity based trust model based on Homophily principle is proposed. Earlier social studies have shown that people tend to have similarities with others in close proximity. In such clustered communities of interest people tend to communicate, socialize and potentially trust each other. In this paper, a novel proximity based trust model is built taking into consideration different aspects like cooperation or unselfishness, honesty, similarity and Activity.

IWSMA – 2nd International Workshop on Security of Mobile Applications

Session Chair: Peter Kieseberg (SBA Research, Austria)
Location: Lecture Hall G

1. Privacy-Preserving Publishing of Pseudonym-Based Trajectory Location Data Set
Ken Mano (NTT Corporation, Japan), Kazuhiro Minami, Hiroshi Maruyama (Institute of Statistical Mathematics, Japan)

Abstract: Anonymization is a common technique for publishing a location data set in a privacy-preserving way. However, such an anonymized data set lacks trajectory information of users, which could be beneficial to many locationbased analytic services. In this paper, we present a dynamic pseudonym scheme for constructing alternate possible paths of mobile users to protect their location privacy. We introduce a formal definition of location privacy for pseudonymbased location data sets and develop a polynomial-time verification algorithm for determining whether each user in a given location data set has sufficient number of possible paths to disguise the user's true movements. We also provide the correctness proof of the algorithm.

2. Probabilistic Contract Compliance for Mobile Applications
   Gianluca Dini (Università di Pisa, Italy), Fabio Martinelli (Istituto di Informatica e Telematica Consiglio Nazionale delle Ricerche, Italy) Andrea Saracino (Università di Pisa & Istituto di Informatica e Telematica Consiglio Nazionale delle Ricerche, Italy), Daniele Sgandurra (Istituto di Informatica e Telematica Consiglio Nazionale delle Ricerche, Italy)

   Abstract: We propose PICARD (ProbabIlistic Contract on AndRoiD), a framework to generate probabilistic contracts to detect repackaged applications for Android smartphones. A contract describes the sequences of actions that an application is allowed to perform at run-time, i.e. its legal behavior. In PICARD, contracts are generated from the set of traces that represent the usage profile of the application. Both the contract and the application's run-time behavior are represented through clustered probabilistic automata. At run-time, the PICARD monitoring system verifies the compliance of the application trace with the contract. This approach is useful in detecting repackaged applications, whose behavior is strongly similar to the original application but it differs only from small paths in the traces. In this paper, we discuss the framework of PICARD for describing and generating contracts through probabilistic automata and introduce the notion of ActionNode, a cluster of related system calls, used to represent high level operations. Then, we present a first set of preliminary experiments on repackaged applications, to evaluate the viability of the proposed approach.

3. A Classifier of Malicious Android Applications
   Gerardo Canfora, Francesco Mercaldo, Corrado Aaron Visaggio (University of Sannio. Italy)

   Abstract: Malware for smartphones is rapidly spreading out. This paper proposes a method for detecting malware based on three metrics, which evaluate: the occurrences of a specific subset of system calls, a weighted sum of a subset of permissions that the application required, and a set of combinations of permissions. The experimentation carried out suggests that these metrics are promising in detecting malware, but further improvements are needed to increase the quality of detection.

TWISNet II – International Workshop on Trustworthy Wireless Industrial Sensor Networks

Session Chair: Mike Ludwig (Dresden Elektronik Ingenieurtechnik GmbH, Germany)
Location: Lecture Hall D

1. TWISNet Security Framework: Overall View, Mediation Layer and chosen modules
2. Implementation and Hardware Considerations
3. Exploitation in practical Scenarios

12:30 – 14:00 Lunch

14:00 – 17:30 Plenary Session

Tutorial

Location: Lecture Hall A

Bug Parades, Zombies, and the BSIMM: A Decade of Software Security (extended dance version) (Part I)

Gary McGraw (Cigital, United States)

Abstract: Only ten years ago, the idea of building security in was brand new. Back then, if system architects and developers thought about security at all, they usually concentrated on the liberal application of magic crypto fairy dust. We have come a long way since then. Perhaps no segment of the security industry has evolved more in the last decade than the discipline of software security. Several things happened in the early part of the decade that set in motion a major shift in the way people build software: the release of my book Building Secure Software, the publication of Bill Gates's Trustworthy Computing memo, the publication of Lipner and Howard¹s Writing Secure Code, and a wave of high-profile attacks such as Code Red and Nimda that forced Microsoft, and ultimately other large software companies, to get religion about software security. Now, ten years later, Microsoft has made great strides in software security and building security in---and they¹re publishing their ideas in the form of the SDL.

Right about in the middle of the last ten years (five years in) we all collectively realized that the way to approach software security was to integrate security practices that I term the "Touchpoints" into the software development lifecycle. Now, at the end of a decade of great progress in software security, we have a way of measuring software security initiatives called the BSIMM <http://bsimm.com>.

Using the framework described in my book “Software Security: Building Security In” I will discuss and describe the state of the practice in software security. This tutorial is peppered with real data from the field, based on my work with several large companies as a Cigital consultant. As a discipline, software security has made great progress over the last decade. Of the many large-scale software security initiatives we are aware of, fifty-one---all household names---are currently included in the BSIMM study. Those companies among the fifty-one who graciously agreed to be identified include: Adobe, Aon, Bank of America, Box, Capital One, The Depository Trust & Clearing Corporation (DTCC), EMC, F-Secure, Fannie Mae, Fidelity, Google, Intel, Intuit, JPMorgan Chase & Co., Mashery, McKesson, Microsoft, Nokia, Nokia Siemens Networks, QUALCOMM, Rackspace, Salesforce, Sallie Mae, SAP, Scripps Networks, Sony Mobile, Standard Life, SWIFT, Symantec, Telecom Italia, Thomson Reuters, Visa, VMware, Wells Fargo, and Zynga. The BSIMM was created by observing and analyzing real-world data from leading software security initiatives. The BSIMM can help you determine how your organization compares to other real software security initiatives and what steps can be taken to make your approach more effective. BSIMM is helping transform the field from an art into a measurable science.

This tutorial provides an entertaining review of the software security journey from its "bug of the day" beginnings to the multi-million dollar software security initiatives of today.

Friday, 06 September 2013

08:00 – 12:30 Registration for all events

09:00 – 09:30 Parallel Sessions

ARES XI – Mobile Security – 8th International Conference on Availability, Reliability and Security

Location: Lecture Hall F

1. The Transitivity-of-Trust Problem in Android Application Interaction
   Steffen Bartsch (TU Darmstadt, Germany), Bernhard Berger, Michaela Bunke, Karsten Sohr (Universität Bremen, Germany)

   Abstract: Mobile phones have developed into complex platforms with large numbers of installed applications and a wide range of sensitive data. Application security policies limit the permissions of each installed application. As applications may interact, restricting single applications may create a false sense of security for end users, while data may still leave the mobile phone through other applications. Instead, the information flow needs to be policed for the composite system of applications in a transparent manner. In this paper, we propose to employ static analysis, based on the software architecture and focused on dataflow analysis, to detect information flows between components. Specifically, we aim to reveal transitivity-of-trust problems in multi-component mobile platforms. We demonstrate the feasibility of our approach with two Android applications.

2. Secure Profile Provisioning Architecture for Embedded UICC
   Jaemin Park, Kiyoung Baek, Cheoloh Kang (System R&D Division, Republic of Korea)

   Abstract: Embedded UICC (eUICC) is a new form of UICC, soldered into a device during manufacturing. On the contrary to the traditional UICC, the eUICC is not fully controlled by one specific MNO (Mobile Network Operator) since not removable physically from the device and not issued by the MNO. Thus, the profiles necessary for its operations should be provisioned remotely into the eUICC by new entity. For this remote provisioning, SM (Subscription Manager) is newly introduced by the standardization organization. However, this new ecosystem around eUICCs can cause tremendous security issues unless thorough consideration of security is accompanied during the standardization because the profiles usually include the security-sensitive information. In this paper, a novel secure profile provisioning architecture for eUICCs is proposed. Our architecture mainly defines the overall architecture of the secure profile provisioning for eUICCs.

3. Ultra-lightweight Mutual Authentication Protocols: Weaknesses and Countermeasures
   Zeeshan Bilal, Keith Martin (Royal Holloway University of London. UK)

   Abstract: This paper reviews weaknesses highlighted in existing proposals for a family of mutual authentication protocols belonging to the ultra-lightweight class, which are designed for low-cost RFID systems. This family is suitable for systems where authenticating parties already share secrets, which are updated in each authentication round to counter tracking of the tag. We propose a new ultra-lightweight authentication protocol that builds on the strengths of existing schemes yet incorporates countermeasures to overcome previous weaknesses. Significantly our protocol uses lower resources than previous proposals.

4. A Reputation-Based Clustering Mechanism for MANET Routing Security
   Aida Ben Chehida, Ryma Abassi, Sihem Guemara El Fatmi (University of Carthage, Tunisia)

   Abstract: A Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes having no fixed topology and cooperating with each other. Due to these particularities, classical routing protocols cannot be used and some specific ones have been proposed. Because routing process is fundamental in a MANET deployment,

it constitutes a privileged target of attackers. In this paper we propose a novel reputation-based clustering mechanism to locate malicious nodes and isolate them. In order to reduce network overhead and to handle network topology dynamicity, the proposed mechanism is based on a specific clustering environment. The clustering maintenance complexity is for its part reduced by the use of a reputation based delegation process allowing the cluster-head to delegate its privileges to a chosen cluster member in case of displacement or lack of energy. Moreover, node's reputation handling allows the detection and isolation of malicious nodes. Five modules constitute this mechanism: a monitoring module to detect malicious nodes, a reputation module to update reputation values, an isolation module to discard malicious nodes, an identity recognition module to assess alerts sources and a delegation module to allow clusterhead privileges delegation.

FARES II – Software Security & Testing – 8th International Workshop on Frontiers in Availability, Reliability and Security

Location: Lecture Hall D

1. A Genetic Algorithm Approach for the Most Likely Attack Path Problem
   Mohammed Alhomidi, Martin Reed (University of Essex, UK)

   Abstract: Security attack path analysis has become attractive as a security risk assessment technique that represents vulnerabilities in a network. This paper presents a genetic algorithm approach to find the most likely attack paths in attack graphs. We provide an effective approach to network administrators by showing the paths and steps that attackers will most probably exploit to achieve a specific target. The use of a genetic algorithm is particularly appropriate as it offers a straight-forward approach and, most importantly, a range of solutions. This latter point differs from other approaches which concentrate on a singly most likely path and may ignore other important attack vectors. The paper shows how a genetic algorithm can be developed such that feasible individuals are maintained at each stage by selecting certain attack graph vertices to be the crossover and mutation sites.

2. Model-Assisted Access Control Implementation for Code-centric Ruby-on-Rails Web Application Development
   Seiji Munetoh (The Graduate University for Advanced Studies, Japan), Nobukazu Yoshioka (National Institute of Informatics, Japan)

   Abstract: In a Web application framework suitable for a code-centric development approach, maintaining the faultlessness of the security features is an issue because the security features are dispersed throughout the code during the implementation. In this paper, we propose a method and develop a static verification tool for Web applications that checks the completeness of the security features implementation. The tool generates a navigation model from an application code while retaining the security properties and then checks the consistency of the security properties on the model since access control is relevant to the application behavior. We applied the proposed tool to various Ruby on Rails Web application source codes and then tested their authentication and authorization features. Results showed that the tool is an effective aid in the implementation of security features in code-centric and iterative Web application development.

3. A PEP-PDP Architecture to Monitor and Enforce Security Policies in Java Applications
   Yehia Elrakaiby, Yves Le Traon (University of Luxembourg, Luxembourg)

   Abstract: Security of Java-based applications is crucial to many businesses today. In this paper, we propose an approach to completely automate the generation of a security architecture inside of a target Java application where advanced security policies can be enforced. Our approach combines the use of Aspect-Oriented Programming with the Policy Enforcement Point (PEP) - Policy Decision Point (PDP) paradigm and allows the runtime update of policies.

SecATM I - International Workshop on Security in ATM and other Critical infrastructures

Session Chair: Martin Gilje Jaatun (SINTEF ICT, Norway)

Location: Lecture Hall E

1. Invited talk - Security in the Single European Sky ATM Research programme
   Rainer Kölle (EUROCONTROL, Belgium)

2. Evaluation of Airport Security Training Programs: Perspectives and Issues
   Woohyun Shim, Fabio Massacci, Martina de Gramatica (University of Trento, Italy), Alessandra Tedeschi, Alessandro Pollini (Deep Blue S.r.l. Italy)

   Abstract: While many governments and airport operators have emphasized the importance of security training and committed a large amount of budget to security training programs, the implementation of security training programs was not proactive but reactive. Moreover, most of the security training programs were employed as a demand or a trendchasing activity from the government. In order to identify issues in airport security training and to develop desirable security training procedures in an airport, this preliminary study aims at providing (1) the description of current state of airport security training and training in general, (2) the study design and interview guide for studying airport security training, and (3) expected outcome from the study.

3. ARGUS 3D: Security Enhancements through Innovative Radar Technologies
   Roberta Cardinali, Enrico Anniballi (SESM s.c.a.r.l., Italy), Carlo Bongioanni, Antonio Macera, Fabiola Colone, Pierfrancesco Lombardo (University of Rome "Sapienza", Italy)

   Abstract: This electronic document is a "live" template. The various Conventional civil Air Traffic Control (ATC) systems are able to detect targets and identify collaborative aircrafts in the air space but they don't assure full coverage at low altitudes, in presence of non cooperative targets (NCTs) and aircraft (A/C) with a low value of radar cross section (RCS). This paper describes a new architecture that aims at addressing these limitations, developed in the frame of the ARGUS 3D (AiR GUidance and Surveillance 3D) project funded by the European Union (FP7). This project intends to improve the current ATC systems for civil applications, extending their coverage and making them able to detect, recognize and track NCTs, by means of innovative sensors, such as a new enhanced Primary Surveillance Radar (PSR), passive and bistatic radar network. In this paper a description of the proposed architecture is reported together with the details of the analysis made on simulated and real data and the opinion of the final users summarized.

10:30 – 11:00 Coffee Break

11:00 – 12:30 Parallel Sessions

FARES III – Privacy & Forensics – 8th International Workshop on Frontiers in Availability, Reliability and Security

Location: Lecture Hall F

1. iOS Forensics: How Can We Recover Deleted Image Files with Timestamp in a Forensically Sound Manner?
   Aswami Ariffin (University of South Australia, Australia & CyberSecurity Malaysia, Malaysia), Christian D'Orazio, Kim-Kwang Raymond Choo, Jill Slay (University of South Australia, Australia)

   Abstract: iOS devices generally allow users to synch their images (pictures) and video files using iTunes between Apple products (e.g. an iPhone and a MacBook Pro). Recovering deleted images, particularly in a forensically sound manner, from iOS devices can be an expensive and challenging exercise (due to the hierarchical encrypted file system, etc). In this paper, we propose an operational technique that allows digital forensic practitioners to recover deleted image files by referring to iOS journaling file system. Using an iPhone as a case study, we then conduct a forensic analysis to validate our proposed technique.

2. On the Practicability of Cold Boot Attacks
Michael Gruhn, Tilo Müller (Friedrich-Alexander-Universität, Germany)

Abstract: Even though a target machine uses full disk encryption, cold boot attacks can retrieve unencrypted data from RAM. Cold boot attacks are based on the remanence effect of RAM which says that memory contents do not disappear immediately after power is cut, but that they fade gradually over time. This effect can be exploited by rebooting a running machine, or by transplanting its RAM chips into an analysis machine that reads out what is left in memory. In theory, this kind of attack is known since the 1990s. However, only in 2008, Halderman et al. have shown that cold boot attacks can be well deployed in practical scenarios. In the work in hand, we investigate the practicability of cold boot attacks. We verify the claims by Halderman et al. independently in a systematic fashion. For DDR1 and DDR2, we provide results from our experimental measurements that in large part agree with the original results. However, we also point out that we could not reproduce cold boot attacks against modern DDR3 chips. Our test set comprises 17 systems and system configurations, from which 5 are based on DDR3.

3. Shared Crowds: A Token-Ring Approach to Hide the Receiver
Raphael Wigoutschnigg, Peter Schartner, Stefan Rass (Alpen-Adria Universität Klagenfurt, Austria)

Abstract: Because of the intensive usage of the internet and services provided over the world wide web, the privacy of the users is threatened by various attacks. This paper shows how to build a protocol for anonymous data transmission, with the primary focus on hiding the identity of the receiver (receiver anonymity), using multi path transmission and secret sharing. This protocol extends the crowds system by Reiter and Rubin, which only weakly hides the identity of the receiver. Due to the use of a circular channel topology the receiver is hidden even if timing attacks are mounted. Additionally this protocol gives the participating nodes the possibility to detect active attacks during the channel setup phase. Another positive aspect is the ability to handle some kind of node failures by repairing the virtual channel.

FARES IV – Network & Cloud Security – 8th International Workshop on Frontiers in Availability, Reliability and Security

Location: Lecture Hall D

1. DNSSEC: Interoperability Challenges and Transition Mechanisms

Amir Herzberg (Bar Ilan University, Israel), Haya Shulman (TU Darmstadt, Germany & Bar Ilan University, Israel)

Abstract: Recent cache poisoning attacks motivate protecting DNS with strong cryptography, by adopting DNSSEC, rather than with challenge-response 'defenses'. We discuss the state of DNSSEC deployment and obstacles to adoption. We then present an overview of challenges and potential pitfalls of DNSSEC, including:

- Incremental Deployment: we review deployment status of DNSSEC, and discuss potential for increased vulnerability due to popular practices of incremental deployment, and provide recommendations.
- Long DNSSEC Responses: long DNS responses are vulnerable to attacks, we review cache poisoning attack on fragmented DNS responses, and discuss mitigations.
- Trust Model of DNS: we review the trust model of DNS and show that it may not be aligned with the security model of DNSSEC. We discuss using trust anchor repositories (TARs) to mitigate the trust problem. TARs were proposed to allow transition to DNSSEC and to provide security for early adopters.

2. Enhancing Security Testing via Automated Replication of IT-Asset Topologies
Henk Birkholz, Ingo Sieverdingbeck, Nicolai Kuntze, Carsten Rudolph (Fraunhofer SIT, Germany)

Abstract: Security testing of IT-infrastructure in a production environment can have a negative impact on business processes supported by IT-assets. A testbed can be used to provide an alternate testing environment in order to mitigate this impact. Unfortunately, for small and medium enterprises, maintaining a physical testbed and its consistency with the production environment is a cost-intensive

task. In this paper, we present the Infrastructure Replication Process (IRP) and a corresponding Topology Editor, to provide a cost-efficient method that makes security testing in small and medium enterprises more feasible. We utilize a virtual environment as a testbed and provide a structured approach that takes into account the differences between a physical and a virtual environment. Open standards, such as SCAP, OVAL or XCCDF, and the utilization the Interconnected-asset Ontology—IO—support the integration of the IRP into existing (automated) processes. We use the implementation of a prototype to present a proof-of-concept that shows how typical challenges regarding security testing can be successfully mitigated via the IRP.

3. A Generation Method of Cryptographic Keys for Enterprise Communication Systems
Aleksandar Hudic (SBA Research, Austria), Elise Revell (Kelisec AB), Dimitris E. Simos (SBA Research, Austria)

Abstract: In this work, we initially describe a method patented in [1] for key generation in a symmetric channel between different nodes that are located within a trusted network. In the aftermath, we describe the different phases of the invented method in cryptographic terms and we analyze security aspects with respect to a proper implementation. We conclude by giving some arguments that justify the usage of this method in enterprise communication systems.

SecATM II - International Workshop on Security in ATM and other Critical infrastructures

Session Chair: Martin Gilje Jaatun (SINTEF ICT, Norway)
Location: Lecture Hall E

1. Enhancing CHASSIS: A Method for Combining Safety and Security
Christian Raspotnig (Institute for Energy Technology & University of Bergen, Norway), Vikash Katta (Institute for Energy Technology & Norwegian University of Science and Technology, Norway), Peter Karpati (Institute for Energy Technology, Norway), Andreas L. Opdahl (University of Bergen, Norway)

Abstract: Safety and security assessments aim to keep harm away from systems. Although they consider different causes of harm, the mitigations suggested by the assessments are often interrelated and affect each other, either by strengthening or weakening the other. Considering the relations and effects, a combined process for safety and security could save resources. It also improves the reliability of the system development when compared to having two independent processes whose results might contradict. This paper extends our previous research on a combined method for security and safety assessment, named CHASSIS, by detailing the process in a broader context of system development with the help of feedback from a safety expert. The enhanced CHASSIS method is discussed based on a case from the Air Traffic Management domain.

2. Towards Harmonising the Legislative, Regulatory, and Standards-based Framework for ATM Security: Developing a Software Support Tool
Rainer Koelle (EUROCONTROL, Belgium), Walter Strijland, Stefan Roels (42Solutions)

Abstract: This research-in-progress paper addresses the elementary capabilities and underlying challenges pertaining to the development of a software tool to support the identification and harmonisation of legislation, regulation, standards, and best practices for ATM Security. The consistent application of ATM Security requirements throughout the SESAR Joint Undertaking Work Programme is a challenge. There is a need to provide a tool for security experts, concept developers and technical experts to ensure compliance with the underlying framework for ATM Security. The software tool described in this paper addresses this issue. In particular, it supports functions that allow for the extraction, categorisation, association, and harmonisation of the rules imposed by the framework. The approach and challenges to the design of the envisaged tool capabilities are outlined. Initial lessons learnt are presented based on the findings at the current prototyping stage. It is reasoned that the feasibility stage is completed and that further development can adhere to the identified capabilities and design outline. User interaction specification and development will be facilitated with an iterative user-based agile software development process.

3. Security Blind Spots in the ATM Safety Culture
Howard Chivers (University of York, UK), John Hird (ATM Security, EUROCONTROL, Belgium)

Abstract: In 2008 EUROCONTROL published Information and Communications Technology (ICT) Security Guidance to Air Navigation Service Providers (ANSPs), to assist them in complying with regulatory security requirements. The validation of that guidance included surveys which were conducted to contrast current practice in European ANSPs with a baseline control set based on ISO/IEC 27001:2005. The surveys are confidential and unpublished; however, by identifying the controls that are missing in all the survey responses it is possible to identify potential 'blind spots' in Air Traffic Management (ATM) security while maintaining the anonymity of the respondents. Key issues identified in this way include security management and senior management engagement, system accreditation, the validation and authentication of data used by ATM systems, incident management, and business continuity preparedness. Since little can be said about the original surveys these results are necessarily indicative, so the paper contrasts these findings with contemporaneous audit reports on security in US ATM systems. The two sources prove to be in close agreement, suggesting that the issues identified are systematic difficulties in introducing security into Air Traffic Management culture.

4. Requirements Management in a Combined Process for Safety and Security Assessments
Vikash Katta (Institute for Energy Technology & Norwegian University of Science and Technology, Norway), Christian Raspotnig (Institute for Energy Technology & University of Bergen, Norway), Peter Karpati (Institute for Energy Technology, Norway), Tor Stålhane (Norwegian University of Science and Technology, Norway)

Abstract: Combined Harm Assessment of Safety and Security for Information Systems (CHASSIS) method defines a unified process for safety and security assessments to address both the safety and security aspects during system development process. CHASSIS applies techniques from safety and security fields - e.g. misuse case and HAZOP- to identify and model hazards, threats and mitigations to a system. These mitigations, which are generally specified as safety and security requirements, are interrelated. Defining and maintaining the interdependencies between these requirements are vital to, among other things, estimate how a requirement impacts other requirements and artefacts. In this paper, we present our approach for providing traceability to CHASSIS in order to capture the interdependencies between the safety and security requirements and to demonstrate the history and rational behind their elicitation. The approach, called SaTrAp, constitutes a process model defining what type of artefacts are generated during development and assessment activities, what type of relations between the artefacts should be captured, and how to extract traces. The traceability approach together with its supporting prototype tool was applied on an Air Traffic Management remote tower example which was assessed for safety and security risks using CHASSIS.

12:30 – 14:00 Lunch

14:00 – 15:30 Plenary Session

SecATM III – International Workshop on Security in ATM and other Critical infrastructures

Session Chair: Martin Gilje Jaatun (SINTEF ICT, Norway)

Location: Lecture Hall E

1. Sink or SWIM: Information Security Requirements in the Sky
Martin Gilje Jaatun, Tor Erlend Fægri (SINTEF ICT, Norway)

Abstract: Despite the inherently cooperative nature of air traffic control, the ICT infrastructure supporting it has, metaphorically speaking, largely remained isolated islands of technology. To this day, most of the interaction between ATM centers is based on voice and point-to-point data communication. Speed and accuracy of coordination is thus frequently limited by human capacities. This also imposes severe restrictions on the scale of coordination efforts among ATM centers. There are, however, changes underway. The main ambition of the System-Wide Information Management (SWIM) concept is to realize a

European-wide network of interconnected ATM systems that promises, among other things, to bring substantial gains in efficiency of coordination and improved utilization of valuable airspace. This paper presents challenges, approaches and experiences from ongoing work on security requirements within SWIM.

2. Collaborative Security Management: Developing Ideas in Security Management for Air Traffic Control

Martin Hawley, Paul Thomas (Winsland Ltd, UK), Rainer Koelle (EUROCONTROL, Belgium), Peter Saxton (Capstick Saxton Associates Ltd, UK)

Abstract: Air Traffic Management (ATM) could benefit from a collaborative approach to security management, particularly to improve situational awareness, quantitative risk assessments and the governance of security. Collaboration between organisations is becoming increasingly important in air traffic control as well as security in general. This emphasises the need to adapt security cultures from 'need to know' towards more direct sharing of knowledge and skills. An additional imperative for the air traffic management sector is that as operations and systems become increasingly integrated, Air Navigation Service Providers (ANSPs) become critically dependent on each other. Hence security of the organisation is bound with the security of the whole European system. To create a successful collaborative approach, security managers will need to adopt collaborative leadership skills and approaches. This can be achieved in an evolutionary way, which grows as the challenges to security become more demanding and complex, as the ATM system is modernised.

3. Applying the SecRAM Methodology in a Cloud-based ATM Environment

Antonio Marotta (University of Naples Federico II DIETI, Italy), Gabriella Carrozza, Luigi Battaglia, Patrizia Montefusco, Vittorio Manetti (SESM S.C.A.R.L, Italy)

Abstract: The SESAR ATM Security Risk Assessment Methodology (SecRAM) aims at providing a methodology to be applied by the SESAR Operational Focus Areas (OFAs). To give effectiveness to the evaluation of SecRAM, Air Traffic Management (ATM) operative scenarios are greatly required. In this paper we leverage a Cloud-based approach to build up a virtualized replica of a real Air Control Centre (ACC) in order to realize a vulnerability analysis and to find some possible points of attacks. Then we applied the SecRAM methodology on our test-bed and we built a real threat scenario for which a risk treatment is properly designed.

4. Beyond Traceability: Compared Approaches to Consistent Security Risk Assessments

Franco Bergomi (Thales Global Services / Engineering Shared Services, France), Stéphane Paul (Thales Research and Technology, France), Bjørnar Solhaug (SINTEF ICT, Norway), Raphael Vignon-Davillier (Thales Communications & Security, France)

Abstract: As military and civil software-intensive information systems grow and become more and more complex, structured approaches, called architecture frameworks (AF), were developed to support their engineering. The concepts of these approaches were standardised under ISO/IEC 42010 – Systems and Software Engineering – Architecture Description. An Architecture Description is composed of Views, where each View addresses one or more engineering concerns. As mentioned in the standard, a multi-viewpoint approach requires the capacity to capture the different views, and maintain their mutual consistency. This paper addresses primarily the problem of integrating a model-based security risk assessment view to the mainstream system engineering view(s) and, to a lesser extent, the problem of maintaining the overall consistency of the views. Both business stakes and technical means are studied. We present two specific approaches, namely CORAS and Rinforzando. Both come with techniques and tool support to facilitate security risk assessment of complex and evolving critical infrastructures, such as ATM systems. The former approach offers static import/export relationships between artefacts, whereas the latter offers dynamic relationships. The pros and cons of each technical approach are discussed.

Keynotes, Tutorials & Panel

Elena Ferrari

Director DiSTA STRICT SociaLab, University of Insubria, Italy

Keynote: Data Protection in Social Networks: Going Beyond Access Control
Tuesday, 03.09.2013 (09.00 – 10.30) Lecture Hall A

Abstract: *With the increasing popularity of On-line Social Networks (OSNs), protection of personal information has gained attention in the research community. This has resulted in many proposals, ranging from access control models to tools for privacy settings suggestion. However, none of the research proposals appeared so far nor the privacy settings currently offered by commercial OSNs provides a comprehensive solution to the fundamental issue of unintended information disclosure to a public that can reach up to millions of users. One of the key reasons is that the social web vision requires to deeply rethink access control and privacy enhancing technologies both in terms of models and architectural solutions for their enforcement. In this talk, after an introduction to the problem of data protection in OSNs, we will discuss the most challenging research questions and issues and report preliminary research results.*

Elena Ferrari is a full professor of Computer Science at the University of Insubria, Italy and scientific director of the K&SM Research Center and the STRICT SociaLab. Her research activities are related to various aspects of data management, including access control, privacy and trust, social networks, secure cloud computing and emergency management. In 2009, she received the IEEE Computer Society's Technical Achievement Award for "outstanding and innovative contributions to secure data management". She is an IEEE Fellow and an ACM Distinguished Scientist.

Carl Gunter

Department of Computer Science, University of Illinois at Urbana-Champaign, USA

Keynote: Six Research Challenges for the Security and Privacy of Health Information Technology
Wednesday, 04.09.2013 (09.00 – 10.30) Lecture Hall A

Abstract: *Health Information Technology (HIT) has the potential to improve the health of individuals of all ages, aid medical research, and reduce the costs of delivering healthcare, but its effective use and acceptance by the public and healthcare professionals depend on employing proper protections for the security and privacy of health information. While considerable progress can be made by applying current best practices for managing data, there are a number of areas specific to HIT where more research is needed to provide technology to support better practices. At least six key areas need to be addressed: (1) access controls and audit, (2) encryption and trusted base, (3) automated policy, (4) mobile health (mHealth), (5) identification and authentication, and (6) data segmentation and de-identification. This talk will discuss each of these challenges and some of the efforts being made to address them.*

Carl A. Gunter received his BA from the University of Chicago in 1979 and his PhD from the University of Wisconsin at Madison in 1985. He worked as a postdoctoral researcher at Carnegie-Mellon University and the University of Cambridge in England before joining the faculty of the University of Pennsylvania in 1987 and the University of Illinois in 2004 where he is now a professor in the Computer Science Department and a professor in the College of Medicine. He serves as the director of Illinois Security Lab, the Health Information Technology Center (HITC), and the Strategic Advanced Research Projects on Security (SHARPS). Professor Gunter has made research contributions in the semantics of programming languages, formal analysis of networks and security, and privacy. His recent research focuses on security and privacy issues for the electric power grid and healthcare information technologies.

Gary McGraw
CTO, Cigital, USA

Tutorial: Bug Parades, Zombies, and the BSIMM: A Decade of Software Security (extended dance version)
Thursday, 05.09.2013 (14.00 – 17.30) Lecture Hall A

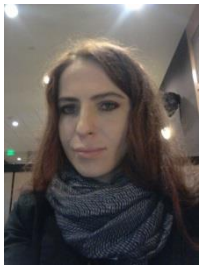
Abstract: *Only ten years ago, the idea of building security in was brand new. Back then, if system architects and developers thought about security at all, they usually concentrated on the liberal application of magic crypto fairy dust. We have come a long way since then. Perhaps no segment of the security industry has evolved more in the last decade than the discipline of software security. Several things happened in the early part of the decade that set in motion a major shift in the way people build software: the release of my book Building Secure Software, the publication of Bill Gates's Trustworthy Computing memo, the publication of Lipner and Howard¹s Writing Secure Code, and a wave of high-profile attacks such as Code Red and Nimda that forced Microsoft, and ultimately other large software companies, to get religion about software security. Now, ten years later, Microsoft has made great strides in software security and building security in---and they¹re publishing their ideas in the form of the SDL.*

Right about in the middle of the last ten years (five years in) we all collectively realized that the way to approach software security was to integrate security practices that I term the "Touchpoints" into the software development lifecycle. Now, at the end of a decade of great progress in software security, we have a way of measuring software security initiatives called the BSIMM <http://bsimm.com>.

Using the framework described in my book ³Software Security: Building Security In² I will discuss and describe the state of the practice in software security. This tutorial is peppered with real data from the field, based on my work with several large companies as a Cigital consultant. As a discipline, software security has made great progress over the last decade. Of the many large-scale software security initiatives we are aware of, fifty-one---all household names---are currently included in the BSIMM study. Those companies among the fifty-one who graciously agreed to be identified include: Adobe, Aon, Bank of America, Box, Capital One, The Depository Trust & Clearing Corporation (DTCC), EMC, F-Secure, Fannie Mae, Fidelity, Google, Intel, Intuit, JPMorgan Chase & Co., Mashery, McKesson, Microsoft, Nokia, Nokia Siemens Networks, QUALCOMM, Rackspace, Salesforce, Sallie Mae, SAP, Scripps Networks, Sony Mobile, Standard Life, SWIFT, Symantec, Telecom Italia, Thomson Reuters, Visa, VMware, Wells Fargo, and Zynga. The BSIMM was created by observing and analyzing real-world data from leading software security initiatives. The BSIMM can help you determine how your organization compares to other real software security initiatives and what steps can be taken to make your approach more effective. BSIMM is helping transform the field from an art into a measurable science.

This tutorial provides an entertaining review of the software security journey from its "bug of the day" beginnings to the multi-million dollar software security initiatives of today.

Gary McGraw is the CTO of Cigital, Inc., a software security consulting firm with headquarters in the Washington, D.C. area and offices throughout the world. He is a globally recognized authority on software security and the author of eight best selling books on this topic. His titles include Software Security, Exploiting Software, Building Secure Software, Java Security, Exploiting Online Games, and 6 other books; and he is editor of the Addison-Wesley Software Security series. Dr. McGraw has also written over 100 peer-reviewed scientific publications, authors a monthly security column for SearchSecurity and Information Security Magazine, and is frequently quoted in the press. Besides serving as a strategic counselor for top business and IT executives, Gary is on the Advisory Boards of Dasient (acquired by Twitter), Fortify Software (acquired by HP), Wall + Main, Inc., and Raven White. His dual PhD is in Cognitive Science and Computer Science from Indiana University where he serves on the Dean¹s Advisory Council for the School of Informatics. Gary served on the IEEE Computer Society Board of Governors and produces the monthly Silver Bullet Security Podcast for IEEE Security & Privacy magazine (syndicated by SearchSecurity).



Haya Shulman
TU Darmstadt, Germany

Tutorial on DNS Security
Thursday, 05.09.2013 (09.00 – 12.30) Lecture Hall A

Abstract: *Most caching DNS resolvers rely for their security, against poisoning, on challenge-response defenses, whereby the resolvers validate that the DNS responses contain some 'unpredictable' values, copied from the request. These mechanisms include the 16 bit identifier, source port, and other fields, randomised and validated by different 'patches' to DNS. We investigate the proposed and widely deployed patches, and show how off-path attackers can often circumvent all of them, exposing the resolvers to cache poisoning attacks.*

We discuss DNSSEC, which provides the best defense for DNS, as well as some short-term countermeasures.

Haya Shulman is a PhD candidate at the Department of Computer Science, Bar Ilan University, Israel. Her Ph.D. was carried out under the supervision of Prof. Dr. Amir Herzberg and is on Network security. Her PhD thesis is on Network security. In 2009 Haya graduated her M.Sc. studies, also in the dept. of Computer Science, with thesis on Secure Execution of Software in Remote, Hostile Environment.
Her research interests are network security and protocols, mainly DNS and routing, focusing on attacks on performance and correctness. Prior to her graduate studies Haya worked as a software developer at Aladdin knowledge systems. In 2011 she received a Checkpoint CPIIS award and in 2013 she received a Feder prize for her research in communication technologies.

Ludwig Fuchs
University of Regensburg, Germany

Tutorial on Secure Enterprise - wide Identity Management and Role Modeling
Monday, 02.09.2013 (11.00 – 12.30) Lecture Hall F

Abstract: *In today's increasingly open business environment companies provide access to resources to a greater number of users, and more heterogeneous types of users, than ever before. As a result of improper account management users accumulate a number of excessive rights over time, resulting in the so called identity chaos. Studies show that major security problems and compliance violations arise because of employees gaining unauthorized access to resources as a result of manually handling user accounts. Role-based Identity Management has become a means to solve the identity chaos. It is concerned with the storage, administration, and usage of digital identities during their lifecycle in the organization. Roles acting as intermediary between employees and their access rights are an essential element of IdM. They allow organizations to ease and secure provisioning processes, i.e. the allocation of digital and non-digital assets to employees, and access to resources.*
The tutorial motivates the benefits and challenges of role-based Identity Management within enterprises by focusing on the task of role modeling, i.e. the definition of suitable business roles for employees. It provides detailed information about into current research trends and bridges the gap to practical usage in industry projects by giving insight into a tool-supported methodology for cleansing identity-related data and modeling business roles.

Dr. Ludwig Fuchs studied Information Systems (Wirtschaftsinformatik) at the University of Regensburg, Germany and had completed his dissertation in the area in 2009. In between 2004 and 2009 he studied and researched at the University of York (UK) and the University of Texas (San Antonio, USA) together with well-known academics in the field of IT security (e.g. Prof. Dr. Ravi Sandhu, "RBAC"). His main research interest comprises Identity Management within mid-sized and large organizations. Over the last seven years, Ludwig Fuchs gathered practical and academic experience and published the results at several international IT security conferences and journals.
His expert knowledge has additionally been underlined throughout his work in several industry projects, bridging the gap between practical requirements and latest academic research results.

Stefan Katzenbeisser
TU Darmstadt & CASED, Germany

Tutorial on Challenges in Data Protection - Privacy by Design

Monday, 02.09.2013 (09.00 – 12.30) Lecture Hall A

Abstract: *The increasing use of networked IT systems brings new challenges regarding the protection of privacy sensitive data. While in the past privacy was mainly assured through regulatory approaches, access control and audits, these mechanisms tend to be inappropriate for largely distributed systems. New technical protection mechanisms come to rescue: they allow to make sensitive data available for various applications, while protecting them from misuse. The tutorial will provide an introduction two technically different approaches. First, data usage control allows to implement fine-granular data-centric access control policies which span across systems boundaries. These approaches gained popularity due to the availability of novel operating systems security concepts, such as strong isolation and virtualization, and can be implemented using concepts like Trusted Computing. Second, cryptographic protocols, based on homomorphic encryption and Secure Multiparty Computation, can be designed, which allow to privately process sensitive data and prevent data leakage to insiders.*

Stefan Katzenbeisser received the Ph.D. degree from the Vienna University of Technology, Austria. After working as a research scientist at the Technical University in Munich, Germany, he joined Philips Research as Senior Scientist in 2006. Since April 2008 he is professor at the Technical University of Darmstadt, heading the Security Engineering group. His current research interests include Digital Rights Management, data privacy, software security and cryptographic protocol design. He is a member of the ACM, IEEE and IACR.

Panel: Threats & Risk Management - Bridging the Gap between Industry needs and Research

Wednesday, 04.09.2013 (16.00 – 17.30) Lecture Hall B

Moderated by *Martin Gilje Jaatun (SINTEF, NO)*

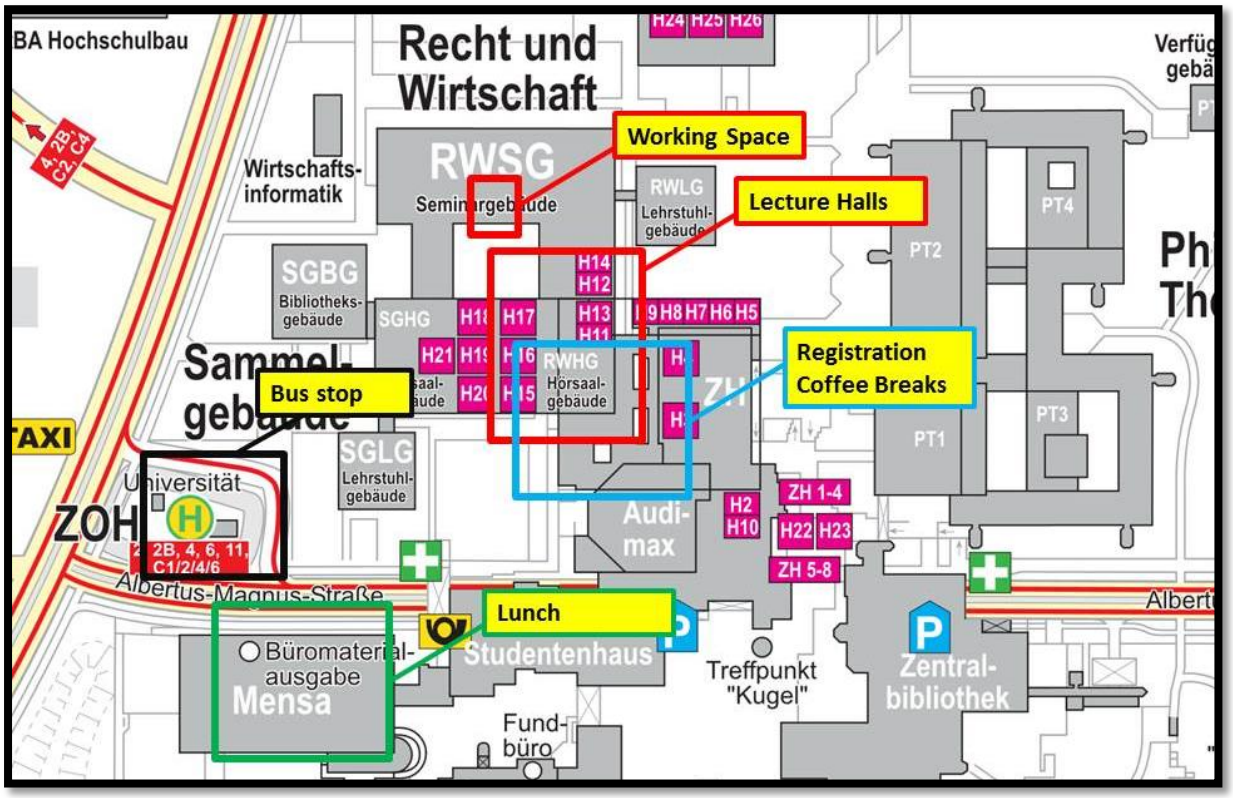
Panel discussion with

- *Gary McGraw (Cigital, US)*
- *Greg Soukiassian (BC & RS, France)*
- *Chris Wills (CARIS Research, UK)*

Where do security technologies come from? Grants are proposed by academics and funded by the government. Startups move technologies across the "valley of death" to early adopters. Idea generation is perhaps ten percent of innovation; most of the work is on technology transfer and adoption. Chance plays a big role in terms of creating opportunities, but a company's success depends on its ability to make good opportunities more likely and to capitalize on opportunities that do arise. Taking a great idea from the lab out into the world is hard work with many perils and pitfalls (including the "research valley of death"). Passionate individuals drive technology transfer more than process, with some people believing that the original researchers need to be personally involved all the way along. Prototyping is an important practice, often resulting in "researchware" that proves a concept but is not ready for common use.

Risk management means many different things to different people. Practitioners, researchers, and academics all have their own perspective. International standards such as the ISO/IEC 27K series provide a decent starting point for understanding and debating what risk management is. How should such standards impact research and development of new technologies? What can be done to make standards work in practice for small and medium-sized enterprises? Finally, what impact should standards have on innovation, if any?

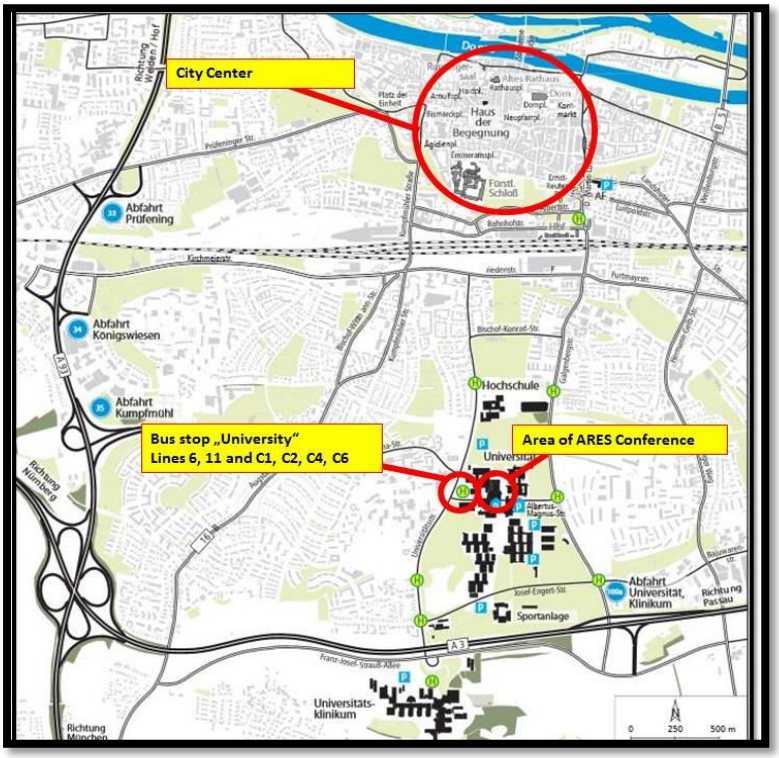
Floor plan


Recht und Wirtschaft
BA Hochschulbau
Wirtschafts-informatik
RWSG
Seminargebäude
RWLG
Lehrstuhl-gebäude
Working Space
Lecture Halls
Registration Coffee Breaks
Bus stop
SGBG
Bibliotheks-gebäude
SGHG
RWHG
Hörsaal-gebäude
SGLG
Lehrstuhl-gebäude
Universität
ZOH
Albertus-Magnus-Straße
Audi-max
ZH
ZH 1-4
ZH 5-8
Lunch
Studentenhaus
Mensa
Büromaterial-ausgabe
Fund-büro
Treffpunkt "Kugel"
Zentral-bibliothek
PT1
PT2
PT3
PT4
TAXI

How to get to the Conference Venue (Universität Regensburg)

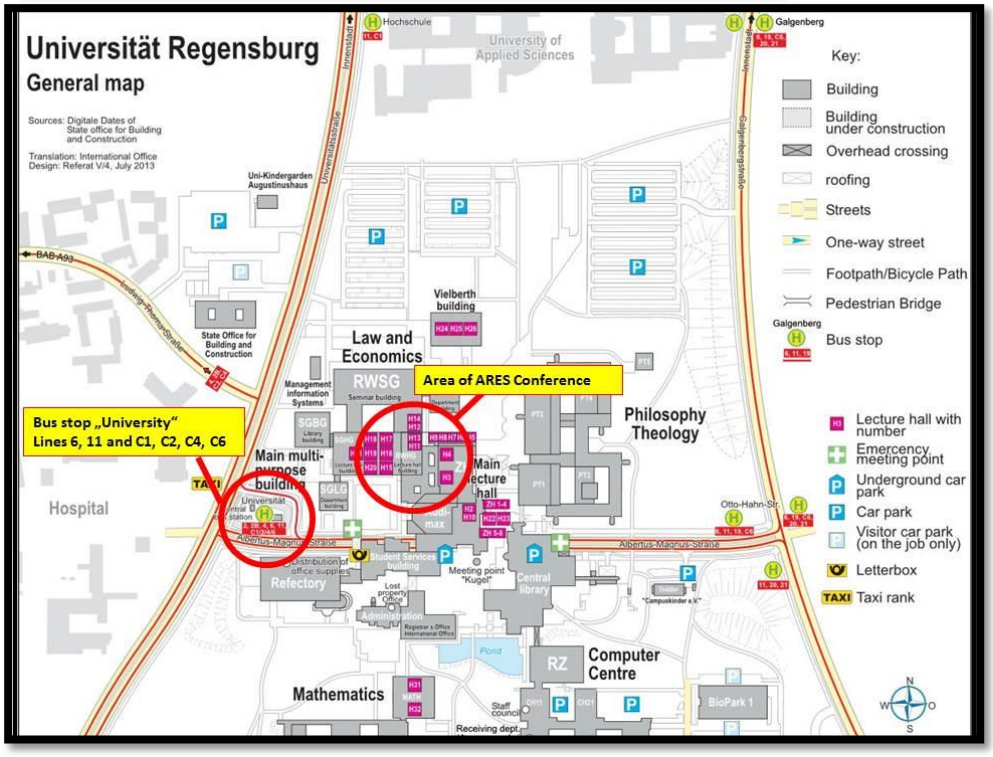
To get from the main station to the University of Regensburg by foot, cross the railroad tracks via “Galgenbergbrücke” and head south until you reach the University.

If you want to take the bus to the University, the lines 6 (direction "Klinikum") and 11 (direction "Burgweinting") and all Campus-lines (C1, C2, C4, C6) will get you there. Both lines also stop at the main station. The bus stop in front of the University of Regensburg is called “Universität”. If you arrive by taxi, tell the driver to stop at "Universität Regensburg, Busbahnhof".



Address of ARES 2013

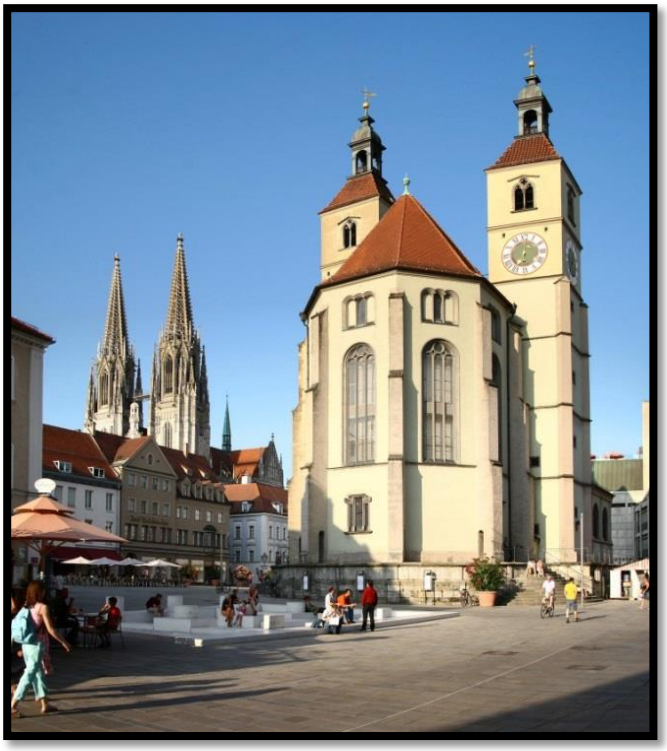
Universität Regensburg
Universitätsstraße 31
93053 Regensburg
Germany



About Regensburg

The first settlements in Regensburg date to the Stone Age. The Celtic name Radasbona was the oldest name given to a settlement near the present city. Around AD 90, the Romans built a fort there.
Anyone thinking a medieval town with a 2,000-year-old history might be slightly on the quiet side is greatly mistaken: Regensburg is anything but dull. World heritage comes to life in the individual historical buildings and squares but, above all, in the town that they form. What's more, this is a town for fun-lovers with the highest concentration of bars in Germany.
The people of Regensburg only found true appreciation for their town's old quarter at a relatively late stage. As recently as the 1960s there were plans to tear down the historical buildings and replace them with new ones. Nowadays, everyone is delighted that this didn't happen and, since the 1970s, locals have been carefully restoring and preserving their heritage in the old quarter. Few other towns in central Europe can offer legacies of more than 2,000 years of history whichever way you look.

Regensburg has 1,500 listed buildings; 984 of them make up the UNESCO World Heritage 'Old Town with Stadtamhof' ensemble. The old stone bridge over the Danube, the cathedral and Krauterermarkt square with the Collegiate Church of St. John, the Cathedral Treasury Museum, the castle-like patrician town house 'Heuport' and the historic Adler Pharmacy count among Regensburg's most significant architectural monuments, but represent just a few of the vast number of outstanding sights. Further up the river, next to the old Amberger Stadel warehouse, is Fischmarkt square with its Roland fountain. Beyond that is a museum dedicated to the astronomer Johannes Kepler. Other fascinating places to visit are St. Ulrich's Church and Diocesan Museum, the former Cathedral deanery, the squares Dachauplatz, Neupfarrplatz, Alter Kornmarkt, Kohlenmarkt, Zieroldsplatz, Rathausplatz and Haidplatz, Porta Praetoria and the patrician towers – including the 28m Golden Tower, the highest medieval residential tower north of the Alps.



Regensburg's cultural scene is just as diverse as the treasures of its old quarter, combining traditional and modern elements with influences from around the globe. It includes countless theatre and dance shows, concerts, festivals, exhibitions and other cultural attractions. There is sure to be something for everyone, whether you prefer sophisticated or traditional entertainment, classical or eminently German. The choice of venues is endless too, ranging from hip and modern locations to historical settings or even outdoors on the town's squares.

Regensburger Dult (23.08.2013 – 08.09.2013)

The Regensburger Dult is fun fair with a long standing tradition dating back to the 10th century. If you want visit the Dult you can either walk, take a taxi or the public transportation. The Bus stop is called “Dultplatz” and the RVV line 17 (which also stops at the main station) will take you there. In addition there’s a free bus called the “Dult-Bus”. It goes every 20 minutes starting at 5 pm every Monday, Tuesday, Thursday, Friday, Sunday and from 1 pm every Wednesday and Saturday. The last bus back to the main station goes at 00.15 am.

Where to eat in your free time (insider tips from local people)

Fine-Dining:
http://www.historisches-eck.de/
http://www.heuport.de/
http://www.lessing-regensburg.de/
http://www.scholz-regensburg.de/

Bavarian Cuisine:
http://www.weltenburger-am-dom.de/
http://www.kneitingerkeller.de/lokal.htm
http://www.spitalgarten.de/
http://www.regensburger-weissbrauhaus.de/

International Cuisine:
http://www.osteriasiciliana.de
http://www.jalapenos-regensburg.de/
http://www.dergrieche-regensburg.de/
http://www.taormina-regensburg.de/

Social Events

Mayor's Reception at the old City Hall on September 2nd

The Mayor's Reception will take place on Monday, 2nd of September 2013, at the old city hall and will start at 19.30h. We will meet directly there.

Address:
Altes Rathaus
Rathausplatz 1
93047 Regensburg

How to get there:

Take the bus line 6 towards *Wernerwerkstraße* and get out at *Regensburg, HBF/Albertstraße*. There you can take the bus line A towards *Arnulfsplatz.* Get out at the bus stop *Altes Rathaus*.

Conference Dinner at "Fürstliches Brauhaus" on September 3rd

The Conference Dinner will take place on Tuesday, 3rd of September 2013, at "Fürstliches Brauhaus".

After the last session at 17.30 a bus will pick you up at the University and take you to the Conference Dinner location. Departure time is 17.45. The "Fürstliches Brauhaus" is located right in the city center of Regensburg.

Sightseeing Tour through the old city of Regensburg on September 4th

We are pleased to invite you to join us for a guided city tour through the large medieval centre of the city, which is also a UNESCO World Heritage Site. The tour will take place on Wednesday, 04th of September. We will meet at about 18.00 in the city and the walking tour will take about 1,5 hours (details will be announced during the conference).

Participants have to sign up for the walking tour until Monday, 2nd of September! If you want to join the tour please come to the registration desk or drop us an email.

Classic Walking Tour

Patricians and bishops, demons and saints, citizens and craftsmen have left their mark on Regensburg's colourful history. Discover the major landmarks and monuments of one of the most important towns during the Middle Ages and listen to vivid stories and legends of the people of Regensburg.

We are looking forward to meeting you there!

Conference Office

If you have any questions or need assistance during the conference do not hesitate to contact:

ARES / CD-ARES Conference Office

Email: office@ares-conference.eu

Yvonne Poul

Tel: +43 699 100 41 066

ypoul@sba-research.org