PROGRAM GUIDE

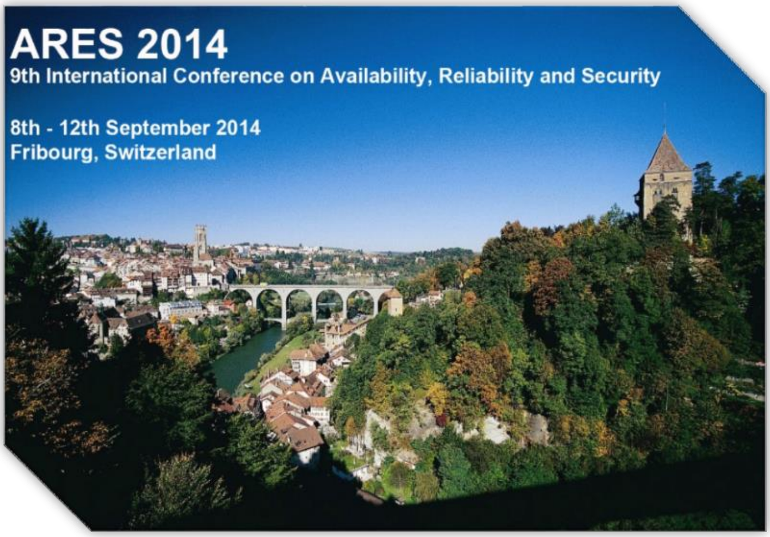
ARES Conference
International Conference on Availability, Reliability and Security

9th International Conference on Availability, Reliability and Security (ARES 2014)

ifip

International Cross-Domain Conference and Workshop (CD-ARES 2014)

IFIP WG 8.4, 8.9, TC5 supported


ARES 2014
9th International Conference on Availability, Reliability and Security
8th - 12th September 2014
Fribourg, Switzerland

08 – 12 September 2014
University of Fribourg, Switzerland

Organized by…

iimt & secure sba-research.org

Supported by…

TU WIEN Technische Universität Wien, Vienna University of Technology

ifip

Society for ICT Knowledge Transfer

Table of Contents

The 9th International Conference on Availability, Reliability and Security (ARES 2014)

The Ninth International Conference on Availability, Reliability and Security (ARES 2014) brings together researchers and practitioners in the field of dependability and information assurance. ARES 2014 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 2014 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 three well-known keynote speakers: Bart Preneel, Katholieke Universiteit Leuven, Belgium, Volkmar Lotz, SAP Research, Germany and Allison Mankin, Verisign Labs, United States.

From the many submissions we have selected the **13** 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 **16%**. 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.

A different country hosts the conference every year. The 2014 edition takes place in Fribourg, Switzerland, at the University of Fribourg.

We wish all participants an enjoyable conference and interesting discussions.

The ARES 2014 Program Committee Co-Chairs
Collin Mulliner, *Northeastern University, United States*
Edgar Weippl, *Vienna University of Technology & SBA Research, Austria*

The ARES 2014 General Chair
Stephanie Teufel, *University of Fribourg, Switzerland*

Organizing Committee ARES 2014

ARES 2014 Program Committee Co-Chairs

Collin Mulliner, *Northeastern University, United States*
Edgar Weippl, *SBA Research, Austria*

ARES 2014 General Chair

Stephanie Teufel, *University of Fribourg, Switzerland*

ARES 2014 Publication Chair

Christine Strauss, *University of Vienna, Austria*

ARES 2014 Program Committee

- Jon A. Solworth, *University of Illinois at Chicago, US*
- Rafael Accorsi, *University of Freiburg, Germany*
- Isaac Agudo, *University of Malaga, Spain*
- Amin Anjomshoaa, *Vienna University of Technology, Austria*
- Alessandro Armando, *Università di Genova, Italy and Fondazione Bruno Kessler (FBK), Italy*
- Aslan Askarov, *Harvard University, US*
- Carlos Blanco Bueno, *University of Cantabria, Spain*
- Ravishankar Borgaonkar, *Technische Universität Berlin, Germany*
- Stephane Bressan, *National University of Singapore, Singapore*
- Luanne Burns Goldrich, *The Johns Hopkins University Applied Physics Laboratory, US*
- Lasaro Camargos, *Federal University of Uberlândia, Brazil*
- Jordi Castellà-Roca, *Rovira i Virgili University of Tarragona, Spain*
- Lorenzo Cavallaro, *Royal Holloway, University of London, UK*
- David Chadwick, *University of Kent, UK*
- Stephen Checkoway, *Johns Hopkins University, US*
- Soon Ae Chun, *City University of New York, US*
- Nathan Clarke, *University of Plymouth, UK*
- Marijke Coetzee, *University of Johannesburg, South Africa*
- Vincenzo De Florio, *PATS / Universiteit Antwerpen and PATS / iMinds, Belgium*
- Steven Demurjian, *University of Connecticut, US*
- Mark Dillon, *International Criminal Court, Netherlands*
- Jochen Dinger, *Karlsruhe Institute of Technology (KIT), Germany*
- Stelios Dritsas, *Athens University of Economic and Business, Greece*
- Pavlos Efraimidis, *Democritus University of Thrace, Greece*
- Manuel Egele, *Carnegie Mellon University, US*
- Christian Engelmann, *Oak Ridge National Laboratory, US*
- Aristide Fattori, *Università degli Studi di Milano, Italy*
- Hannes Federrath, *University of Hamburg, Germany*
- Christophe Feltus, *Centre de Recherche Public Henri Tudor, Luxembourg*
- Simone Fischer-Huebner, *Karlstad University, Sweden*
- Francesco Flammini, *Ansaldo STS, Italy*
- Steven Furnell, *Plymouth University, UK*
- Ralf Gitzel, *ABB Corporate Research, Germany*
- Karl Goeschka, *Vienna University of Technology, Austria*
- Nico Golde, *Qualcomm Research Germany*
- Marcin Gorawski, *Wroclaw University of Technology and Silesian University of Technology, Poland*
- Dimitris Gritzalis, *Athens University of Economics and Business, Greece*
- Stephan Groß, *Technische Universität Dresden, Germany*
- Daniel Grosu, *Wayne State University, US*
- Bogdan Groza, *Politehnica University of Timisoara, Romania*
- Dominik Herrmann, *University Hamburg, Germany*
- Michael Huth, *Imperial College London, UK*

- Michael Hutter, *Graz University of Technology, Austria*
- Martin Gilje Jaatun, *SINTEF, Norway*
- Hai Jin, *Huazhong University of Science and Technology, China*
- Jan Jürjens, *TU Dortmund and Fraunhofer ISST, Germany*
- Sokratis K. Katsikas, *University of Piraeus, Greece*
- Vasilis Katos, *University of Thrace, Greece*
- Stefan Katzenbeisser, *Technische Universität Darmstadt, Germany*
- Peter Kieseberg, *SBA Research, Austria*
- Ezzat Kirmani, *St. Cloud State University, US*
- Thomas Korak, *TU Graz, Austria*
- Thorsten Kramp, *IBM Research Zurich, Switzerland*
- Ralf Kuesters, *University of Trier, Germany*
- Costas Lambrinoudakis, *University of Piraeus, Greece*
- Andrea Lanzi, *Eurecom, Germany*
- Yih-Jiun Lee, *Chinese Culture University, Taiwan*
- Corrado Leita, *Symantec Research Labs, France*
- Shujun Li, *University of Surrey, UK*
- Giovanni Livraga, *Universita' degli Studi di Milano, Italy*
- Javier Lopez, *University of Malaga, Spain*
- Kostas Markantonakis, *Royal Holloway and Bedford New College, UK*
- Ioannis Mavridis, *University of Macedonia, Greece*
- Todd McDonald, *University of South Alabama, US*
- André Miede, *University of Applied Sciences Saarbrücken, Germany*
- Daniel Migault, *Francetelecom / Paris 6, France*
- Katerina Mitrokotsa, *Chalmers University of Technology, Sweden*
- Mattia Monga, *Universita` degli Studi di Milano, Italy*
- Haris Mouratidis, *University of Brighton, UK*
- Thomas Moyer, *MIT Lincoln Laboratory*
- Matthias Neugschwandtner, *Vienna University of Technology, Austria*
- Rolf Oppliger, *eSecurity Technologies, Switzerland*
- Jaehong Park, *University of Texas at San Antonio, US*
- Günther Pernul, *University of Regensburg, Germany*
- Todd R. Andel, *University of South Alabama, US*
- Konrad Rieck, *University of Göttingen, Germany*
- Stefanie Rinderle-Ma, *University of Vienna, Austria*
- Domenico Rosaci, *University "Mediterranea" of Reggio Calabria, Italy*
- Christian Rossow, *Vrije Universiteit Amsterdam, Netherlands*
- Volker Roth, *Freie Universität Berlin, Germany*
- Giovanni Russello, *University of Auckland, New Zealand*
- Luis Enrique Sánchez Crespo, *University of Armed Forced (Ecuador), University of Castilla-la Mancha (Spain)*
- Mark Scanlon, *University College Dublin, Ireland*
- Sebastian Schinzel, *Münster University of Applied Sciences, Germany*
- Jörn-Marc Schmidt, *secunet, Germany*
- Max Schuchard, *University of Minnesota, US*
- Stefan Schulte, *Vienna University of Technology, Austria*
- Jean-Pierre Seifert, *Technische Universität Berlin, Germany*
- Haya Shulman, *TU Darmstadt, Germany*
- Dimitris Simos, *SBA Research, Austria*
- Patrick Stewin, *Technische Universität Berlin, Germany*
- Mark Strembeck, *Vienna University of Economics and Business, Austria*
- Tomasz Truderung, *University of Trier, Germany*
- Aggeliki Tsohou, *Brunel Business School, UK*
- Umberto Villano, *Universita' del Sannio, Italy*
- Lucas Vincenzo Davi, *TU Darmstadt, Germany*
- Cong Wang, *City University of Hong Kong, Hong Kong*
- Jinpeng Wei, *Florida International University, US*
- Christos Xenakis, *University of Piraeus, Greece*
- Alec Yasinsac, *University of South Alabama, US*
- Xiaoyong Zhou, *Indiana University*, US

Cross-Domain Conference and Workshop (CD-ARES 2014)

The Cross-Domain Conference and Workshop CD-ARES is focused on the holistic and scientific view for 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.

CD-ARES 2014 provides a good mix of topics ranging from knowledge management and software security to mobile and social computing.

The collocation with the SeCIHD'14 Workshop is another possibility to discuss most essential application factors. Due to its great success and echo in the scientific community this special track will be held this year for the fourth time.

The main goal of SeCIHD 2014 is to collect and discuss new ideas and solutions for homeland defense. To handle the complex research challenges of homeland defense, it is necessary to adopt "Multi-Disciplinary" approach, which is the core spirit of CD-ARES 2014. This year, SeCIHD 2014 is composed of 14 papers, which introduce the latest technologies of homeland defense including Security Issues and Protocols for Internet Services, Anomaly Detection, Cryptographic Models, Security and Privacy in Ambient Intelligence and so forth.

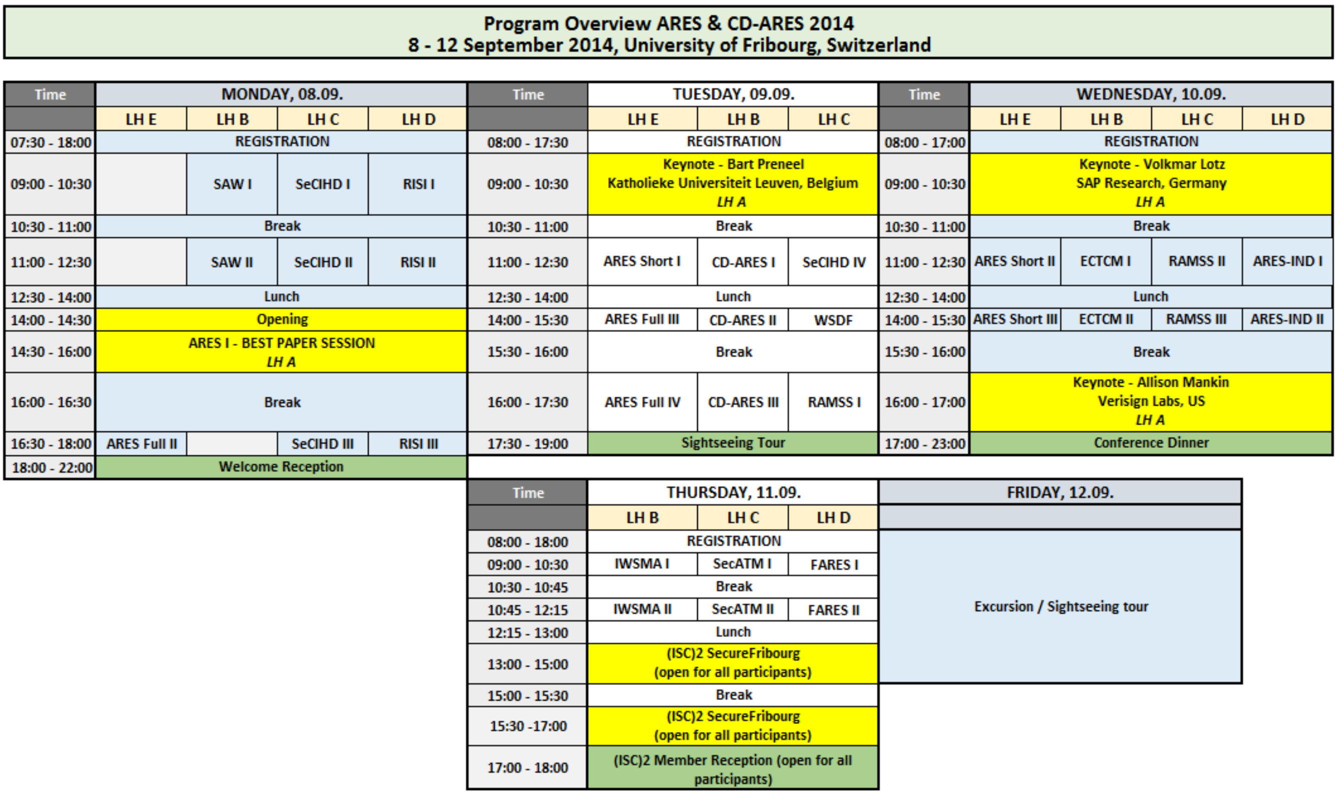
The papers presented at this conference were selected after extensive reviews by the Program Committee with the essential help of associated reviewers.

We would like to thank all PC members and the reviewers who made great effort contributing their time, knowledge and expertise and foremost the authors for their contributions.

The CD-ARES 2014 Editors

Stephanie Teufel, *University of Fribourg, Switzerland*
A Min Tjoa, *Vienna University of Technology, Austria*
Ilsun You, *Korean Bible University, South Korea*
Edgar Weippl, *SBA Research, Austria*

Program Overview



Program Overview ARES & CD-ARES 2014
8 - 12 September 2014, University of Fribourg, Switzerland

Time	MONDAY, 08.09.			
	LH E	LH B	LH C	LH D
07:30 - 18:00	REGISTRATION			
09:00 - 10:30		SAW I	SeCIHD I	RISI I
10:30 - 11:00	Break			
11:00 - 12:30		SAW II	SeCIHD II	RISI II
12:30 - 14:00	Lunch			
14:00 - 14:30	Opening			
14:30 - 16:00	ARES I - BEST PAPER SESSION *LH A*			
16:00 - 16:30	Break			
16:30 - 18:00	ARES Full II		SeCIHD III	RISI III
18:00 - 22:00	Welcome Reception			

Time	TUESDAY, 09.09.		
	LH E	LH B	LH C
08:00 - 17:30	REGISTRATION		
09:00 - 10:30	Keynote - Bart Preneel Katholieke Universiteit Leuven, Belgium *LH A*		
10:30 - 11:00	Break		
11:00 - 12:30	ARES Short I	CD-ARES I	SeCIHD IV
12:30 - 14:00	Lunch		
14:00 - 15:30	ARES Full III	CD-ARES II	WSDF
15:30 - 16:00	Break		
16:00 - 17:30	ARES Full IV	CD-ARES III	RAMSS I
17:30 - 19:00	Sightseeing Tour		

Time	WEDNESDAY, 10.09.			
	LH E	LH B	LH C	LH D
08:00 - 17:00	REGISTRATION			
09:00 - 10:30	Keynote - Volkmar Lotz SAP Research, Germany *LH A*			
10:30 - 11:00	Break			
11:00 - 12:30	ARES Short II	ECTCM I	RAMSS II	ARES-IND I
12:30 - 14:00	Lunch			
14:00 - 15:30	ARES Short III	ECTCM II	RAMSS III	ARES-IND II
15:30 - 16:00	Break			
16:00 - 17:00	Keynote - Allison Mankin Verisign Labs, US *LH A*			
17:00 - 23:00	Conference Dinner			

Time	THURSDAY, 11.09.		
	LH B	LH C	LH D
08:00 - 18:00	REGISTRATION		
09:00 - 10:30	IWSMA I	SecATM I	FARES I
10:30 - 10:45	Break		
10:45 - 12:15	IWSMA II	SecATM II	FARES II
12:15 - 13:00	Lunch		
13:00 - 15:00	(ISC)2 SecureFribourg (open for all participants)		
15:00 - 15:30	Break		
15:30 -17:00	(ISC)2 SecureFribourg (open for all participants)		
17:00 - 18:00	(ISC)2 Member Reception (open for all participants)		

FRIDAY, 12.09.
Excursion / Sightseeing tour

Monday, 08 September 2014

07:30 – 18:00 Registration for all events

09:00 – 10:30 Parallel Sessions

SAW I – Secure Software Architectures – 1st International Software Assurance Workshop

Session Chair: Simon Tjoa, St. Pölten University of Applied Sciences, Austria
Location: Lecture Hall B
Time: 09:00 – 10:30

1. Vulnerability-Based Security Pattern Categorization in Search of Missing Patterns
   Priya Anand, Jungwoo Ryoo (Pennsylvania State University, United States), Rick Kazman (Mellon University Pittsburgh, United States)

   Abstract: A Security Pattern encapsulates security design expertise that addresses recurring information security problems in the form of a credentialed solution. It also presents potential problems and trade-offs in its application. This paper proposes a novel classification model for security patterns. Based on our review of more than one hundred security patterns, we categorize security patterns according to the type of vulnerability they address and also identify similar or identical patterns with different names. Our literature review indicates that there exists very little research on the categorization of security patterns based on vulnerabilities. Any attackers need to exploit existing vulnerabilities to break the security of an information system. To solve security problems effectively, we have to fix their root causes, which are vulnerabilities. The primary contribution of this paper is twofold: (1) to propose a novel security pattern classification model that helps software designers choose an appropriate security pattern once they know the type of a vulnerability they would like to remove and (2) to identify missing security patterns, which naturally emerge as a result of classifying security patterns according to the vulnerabilities they address. The identification of missing patterns could be useful in soliciting help to develop more patterns from the security community to tackle the vulnerabilities currently not handled by the existing patterns.

2. Building Sustainable Software by Preemptive Architectural Design Using Tactic-Equipped Patterns
   Dae-Kyoo Kim (Oakland University, United States), Jungwoo Ryoo (Penn State Altoona, United States), Suntae Kim (Chonbuk National University, Korea)

   Abstract: Sustainability of software architectures has gained increasing attention to cope with factors causing architectural changes such as requirements changes, technological changes, and changes in business strategies and goals. However, there has not been much work on architectural sustainability. In this paper, we present a novel approach for addressing architectural sustainability with respect to non-functional requirements changes through preemptive architectural designs built upon the combined use of architectural patterns and architectural tactics. The approach presented in this paper provides a strategic solution for practitioners to building a quality attribute into a chosen architectural pattern to proactively deal with the requirements changes of quality attribute, which may arise after the construction phase.

3. Using Assurance Cases to Develop Iteratively Security Features Using Scrum
   Lotfi ben Othmane (Fraunhofer SIT, Germany), Pelin Angin, Bharat Bhargava (Purdue University, United States)

   Abstract: A security feature is a customer-valued capability of software for mitigating a set of security threats. Incremental development of security features, using the Scrum method, often leads to developing ineffective features in addressing the threats they target due to factors such as incomplete security tests. This paper proposes the use of security assurance cases to maintain a global view of the security claims as the feature is being developed iteratively and a process that enables the incremental development of security features while ensuring the security requirements of the feature are fulfilled.

SeCIHD I – 4th IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense

Session Chair: Fang-Yie Leu, Tunghai University, Taiwan
Location: Lecture Hall C
Time: 09:00 – 10:30

1. Invited Talk – Trust Extension Protocol for Authentication in Networks Oriented to Management (TEPANOM)
Antonio J. Jara (University of Applied Sciences Western Switzerland, Switzerland)

Abstract: Future Internet of Things is being deployed massively, since it is being already concerned deployments with thousands of nodes, which present a new dimension of capacities for monitoring solutions such as smart cities, home automation, and continuous healthcare. This new dimension is also presenting new challenges, in issues related with scalability, security and management, which require to be addressed in order to make feasible the Internet of Things- based solutions. This work presents a Trust Extension Protocol for Authentication in Networks Oriented to Management (TEPANOM). This protocol allows, on the one hand, the identity verification and authentication in the system, and on the other hand the bootstrapping, configuration and trust extension of the deployment and management domains to the new device. Thereby, TEPANOM defines a scalable network management solution for the Internet of Things, which addresses the security requirements, and allows an easy, and transparent support for the management, which are highly desirable and necessary features for the successful of the solutions based on the Internet of things. The proposed protocol has been instanced for the use case of a fire alarm management system, and successfully evaluated with the tools from the Automated Validation of Internet Security Protocols and Applications (AVISPA) framework.

2. Feature Grouping for Intrusion Detection System based on Hierarchical Clustering
Jingping Song, Zhiliang Zhu (Northeastern University, China), Chris Price (Aberystwyth University, UK)

Abstract: Intrusion detection is very important to solve an increasing number of security threats. With new types of attack appearing continually, traditional approaches for detecting hazardous contents are facing a severe challenge. In this work, a new feature grouping method is proposed to select features for intrusion detection. The method is based on agglomerative hierarchical clustering method and is tested against KDD CUP 99 dataset. Agglomerative hierarchical clustering method is used to construct a hierarchical tree and it is combined with mutual information theory. Groups are created from the hierarchical tree by a given number. The largest mutual information between each feature and a class label within a certain group is then selected. The performance evaluation results show that better classification performance can be attained from such selected features.

RISI I – Information and Participation for Response and Recovery – 4th International Workshop on Resilience and IT-Risk in Social Infrastructures

Session Chair: Sven Wohlgemuth, TU Darmstadt/CASED, Germany
Location: Lecture Hall D
Time: 09:00 – 10:30

1. Invited Talk: Organizing On-Site Volunteers: An App-Based Approach
Stefan Sackmann, Marlen Hofmann, Hans J. Betke (Martin Luther University Halle-Wittenberg, Germany)

Abstract: Mobile ICT provides promising new options for coordinating on-site volunteers in disaster response. A novel app-based IT system called Hands2Help is presented in this contribution supporting incident commanders and control centers in the coordination of volunteers.

2. Visualization of Recovery Situation in Disaster Area by Using Web Reservation Data
Yu Ichifuji (Research Organization of Information and Systems, Japan), Noboru Sonehara (National Institute of Informatics, Japan)

Abstract: Public policy should be decided quickly on the basis of scientific data. However, in urgent situations, e.g., disaster recovery, it takes too long to administer a social survey and collect the results. We have therefore developed a social data collection technique that utilizes the Web reservation data of hotels and bullet trains and propose using this technique to support policymaking in real time. One challenge with using Web data is the difficulty of grasping the real situation due to problems with duplication, so we came up with a method of integrating Web reservation data. We built a social data collection infrastructure using Web data and then compared the integrated data with social survey data of Kyoto and Sendai. Results showed that the integrated data fit the social survey data within 10%. Using these data can show the resilience of hotels and shinkansen. By performing analysis on the basis of this collected data, we can support more timely policymaking. This infrastructure is effective both normal situation and disaster situation.

10:30 – 11:00 Coffee Break

11:00 – 12:30 Parallel Sessions

SAW II – Software Security Analysis – 1st International Software Assurance Workshop

Session Chair: Jungwoo Ryoo, Pennsylvania State University, United States
Location: Lecture Hall B
Time: 11:00 – 12:30

1. LiSTT: An Investigation into Unsound-Incomplete Yet Practical Result Yielding Static Taintflow Analysis
Sanjay Rawat (International Institute of Information Technology, India), Laurent Mounier, Marie-Laure Potet (University of Grenoble, France)

Abstract: Vulnerability analysis is an important component of software assurance practices. One of its most challenging issues is to find software flaws that could be exploited by malicious users. A necessary condition is the existence of some tainted information flow between tainted input sources and vulnerable functions. Finding the existence of such a taint flow dynamically is an expensive and nondeterministic process. On the other hand, though static analysis may explore (theoretically) all the tainted paths, scalability is an issue, especially in the view of complete- and soundness. In this paper, we explore the possibilities of making static analysis scalable, by compromising its complete- and soundness properties and yet making it effective in detecting taint flows that lead to vulnerability exploitation. This technique is based on a combination of call graph slicing and data-flow analysis. A prototype tool has been developed, and we give experimental results showing that this approach is effective on large applications.

2. Visualization of Security Metrics for Cyber Situation Awareness
Igor Kotenko, Evgenia Novikova (St. Petersburg Institute for Information and Automation of the Russian Academy of Sciences, Russia)

Abstract: One of the important direction of research in situational awareness is implementation of visual analytics techniques which can be efficiently applied when working with big security data in critical operational domains. The paper considers a visual analytics technique for displaying a set of security metrics used to assess overall network security status and evaluate the efficiency of protection mechanisms. The technique can assist in solving such security tasks which are important for security information and event management (SIEM) systems. The approach suggested is suitable for displaying security metrics of large networks and support historical analysis of the data. To demonstrate and evaluate the usefulness of the proposed technique we implemented a use case corresponding to the Olympic Games scenario.

SeCIHD II – 4th IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense

Session Chair: Fang-Yie Leu, Tunghai University, Taiwan
Location: Lecture Hall C
Time: 11:00 – 12:30

1. One-time biometrics for Online Banking and Electronic Payment Authentication
Aude Plateaux, Patrick Lacharme (ENSICAEN, France), Audun Jøsang (University of Oslo, Norway), Christophe Rosenberger (ENSICAEN, France)

Abstract: Online banking and electronic payment systems on the Inter- net are becoming increasingly advanced. On the machine level, transactions take place between client and server hosts through a secure channel protected with SSL/TLS. User authentication is typically based on two or more factors. Nevertheless, the development of various malwares and social engineering attacks transform the user’s PC in an untrusted device and thereby making user authentication vulnerable. This paper investigates how user authentication with biometrics can be made more robust in the online banking context by using a specific device called OffPAD. This context requires that authentication is realized by the bank and not only by the user (or by the personal device) contrary to standard banking systems. More precisely, a new protocol for the generation of one-time passwords from biometric data is presented, ensuring the security and privacy of the entire transaction. Experimental results show an excellent performance considering with regard to false positives. The security analysis of our protocol also illustrates the benefits in terms of strengthened security.

2. PrivacyFrost2: A Efficient Data Anonymization Tool Based on Scoring Functions

Shinsaku Kiyomoto, Yutaka Miyake (KDDI R & D Laboratories Inc., Japan)

Abstract: In this paper, we propose an anonymization scheme for generating a k-anonymous and l-diverse (or t-close) table, which uses three scoring functions, and we show the evaluation results for two different data sets. Our scheme is based on both top-down and bottom-up approaches for full-domain and partial-domain generalization, and the three different scoring functions automatically incorporate the requirements into the generated table. The generated table meets users' requirements and can be employed in services provided by users without any modification or evaluation.

3. Crypto-biometric Models for Information Secrecy

Marek R. Ogiela, Lidia Ogiela, Urszula Ogiela (AGH University of Science and Technology, Poland)

Abstract: In this paper will be presented some advances in crypto-biometric procedures used for encryption and division of secret data, as well as modern approaches for strategic management of divided information. Computer techniques for secret information sharing aim to secure information against disclosure to unauthorized persons. The paper will present algorithms dedicated for information division and sharing on the basis of biometric or personal features. Computer techniques for classified information sharing should also be useful in the process of shared information generation and distribution. For this purpose there will be presented a new approach for information management based on cognitive systems.

4. Building an Initialization Cipher Block with Two- Dimensional Operation and Random Parameters

Yi-Li Huang, Fang-Yie Leu (TungHai University, Taiwan), Ilsun You (Korean Bible University, South Korea), Jing-Hao Yang (TungHai University, Taiwan)

Abstract: In recent years, parallel computing capabilities have been more powerful than before. Consequently some block cipher standards, such as DES used to protect important electronic messages, have been cracked in the past years. Also due to the rapid development of hardware processing speeds, 3DES and AES may someday be solved by brute-force attacks. Basically, the common characteristics of these block cipher standards are that each time, when a standard is invoked, the same parent key is used to generate subkeys. The subkeys are then utilized in the standard's encryption rounds to encrypt data. In fact, the variability of the key values is quite limited. Generally, producing random parameters to encrypt data is an effective method to improve the security of ciphertext. But how to ensure the security level of using and delivering these random parameters and how to avoid information leakage have been a challenge. So in this paper, we propose a novel random parameter protection approach, called the Initialization Cipher Block Method(ICBM for short), which protects random parameters by using a two-dimensional operation and employs random parameters to change the value of a fixed parent key for block ciphering, thus lowering the security risk of a block cipher algorithm. Security analysis demonstrates that the ICBM effectively improve the security level of a protected system. Of course, this also safely protect our homeland, particularly when it is applied to our governmental document delivery systems.

RISI II – k-Anonymization for Information Sharing – 4th International Workshop on Resilience and IT-Risk in Social Infrastructures

Session Chair: Isao Echizen, National Institute of Informatics, Japan
Location: Lecture Hall D
Time: 11:00 – 12:30

1. A k-anonymity method based on search engine query statistics for disaster impact statements

Hidenobu Oguri (NIFTY Corporation, Japan), Noboru Sonehara (National Institute of Informatics, Japan)

Abstract: Privacy is a major concern in the management of big data, especially for datasets that contain sensitive personal information. Personal information is frequently used in marketing analyses, and we can also use it to evaluate the damage situation at the time of a disaster. One model that is widely used to protect privacy is k-anonymity, which can be generally defined as a clustering method in which any record in a dataset is indistinguishable from at least (k-1) other records in the same dataset. Most approaches to k-anonymity suffer from huge information loss due to the abstraction of continuous numerical and categorical attributes that have a hierarchical structure. It is difficult to use conventional k-anonymity with actual Internet services because of the computational complexity and value loss stemming from the loss of information. In this paper, we propose an anonymous algorithm that can respond to both the marketing and disaster analyzing. In ordinary times, we can analyze personal data with this algorithm using SEM price, and in times of disaster, we ensure information anonymity according to the number of times a searched word appears and distribute only the necessary information. This approach makes it possible to calculate only the necessary data and to maintain a sufficient k-anonym zed level. Application of this method to actual data showed that using an index number of the occurrences of the search term makes it is possible to anonymize the information with preferentially partitioning disaster locations.

2. A System for Anonymizing Temporal Phrases of Message Posted in Online Social Networks and for Detecting Disclosure

Hoang-Quoc Nguyen-Son (The Graduate University for Advanced Studies, Japan), Minh-Triet Tran (University of Science, Vietnam), Hiroshi Yoshiura (University of Electro-Communications, Japan), Sonehara Noboru, Isao Echizen (National Institute of Informatics, Japan)

Abstract: Time-related information in message posted on-line is one type of sensitive information targeted by attackers, one reason that sharing information online can be risky. Therefore, time information should be anonym zed before it is posted in online social networks (OSNs). One approach to reducing the risk is to anon Mize the personal information by removing temporal phrases, but this makes the anonymous message loses too much information. We have proposed a system for creating anonymous fingerprints about temporal phrases to cover most of potential cases of OSN disclosure. The fingerprints not only anon Mize time-related information but also can be used to identify a person who has disclosed information about the user. In experiment with 16,647 different temporal phrases extracted from about 16 million tweets, the average number of fingerprints created for an OSN message is 526.05 fingerprints. This is significantly better than the 409.58 fingerprints of the state-of-the-art previous detection temporal phrases algorithm. Fingerprints are quantified using a modified normalized certainty penalty metric to ensure that an appropriate level of information anonymity is used for each user's friend. The algorithm works well not only for temporal phrases in message posted on social networks but also for other types of phrases (such as location and objective ones) or other areas (religion, politics, military, etc.).

3. Effects of External Information on Anonymity and Role of Transparency with Example of Social Network De-anonymisation

Haruno Kataoka, Yohei Ogawa (University of Electro-Communications, Japan), Isao Echizen (National Institute of Informatics, Japan), Tetsuji Kuboyama (Gakushuin University, Japan), Hiroshi Yoshiura (University of Electro-Communications, Japan)

Abstract: Personal data to be used for sophisticated data-centric services is typically anonym zed to ensure the privacy of the underlying individuals. However, the degree of protection against de-anonymization is uncertain because de-anonymization has not been explicitly modelled for scientific analysis and because the information that attackers might use is not well defined given that they can use a wide variety of external information sources such as public ally accessible information on the web. We have developed a system that de-anonymizes anonymous posts on social networks with a considerably high precision rate. We analysed this system and its behaviour and, on the basis of our findings, we clarified a de-anonymization model and used it to clarify the effects of external information on anonymity. We also identified the limitation of anonymization under conditions of external information being available and clarified the role of transparency can play in controlling the use of personal data.

12:30 – 14:00 Lunch

14:00 – 16:00 Plenary Sessions

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

Location: Lecture Hall A
Time: 14:00 – 14:30

14:30 – 16:00 ARES Full I – ARES BEST PAPER Session – 9th International Conference on Availability, Reliability and Security

Session Chair: Collin Mulliner, Northeastern University, United States & Edgar Weippl, SBA Research, Austria
Location: Lecture Hall A
Time: 14:30 – 16:00

1. A New Access Control Scheme for Facebook-Style Social Networks
   Jun Pang, Yang Zhang (University of Luxembourg, Luxembourg)

   Abstract: The popularity of online social networks (OSNs) makes the protection of users' private information an important but scientifically challenging problem. In the literature, relationship-based access control schemes have been proposed to address this problem. However, with the dynamic developments of OSNs, we identify new access control requirements which cannot be fully captured by the current schemes. In this paper, we focus on public information in OSNs and treat it as a new dimension which users can use to regulate access to their resources. We define a new OSN model containing users and their relationships as well as public information. Based on this model, we introduce a variant of hybrid logic for formulating access control policies. A type of category relations among public information are exploited to further improve our logic for its usage in practice. In addition, we propose a few solutions to address the problem of information reliability in OSNs.

2. No Smurfs: Revealing Fraud Chains in Mobile Money Transfers
   Maria Zhdanova, Jürgen Repp, Roland Rieke (Fraunhofer Institute SIT, Germany), Chrystel Gaber (Orange, France), Baptiste Hemery (Normandie Université, France)

   Abstract: Mobile Money Transfer (MMT) services provided by mobile network operators enable funds transfers made on mobile devices of end-users, using digital equivalent of cash (electronic money) without any bank accounts involved. MMT simplifies banking relationships and facilitates financial inclusion, and, therefore, is rapidly expanding all around the world, especially in developing countries. MMT systems are subject to the same controls as those required for financial institutions, including the detection of Money Laundering (ML) - a source of concern for MMT service providers. In this paper we focus on an often practiced ML technique known as micro-structuring of funds or smurfing and introduce a new method for detection of fraud chains in MMT systems. Whereas classical detection methods are based on machine learning and data mining, this work builds on Predictive Security Analysis at Runtime (PSA@R), a model-based approach for event-driven process analysis. We provide an extension to PSA@R which allows us to identify fraudsters in an MMT service monitoring network behavior of its end-users. We evaluate our method on simulated transaction logs, containing approximately 460,000 transactions for 10,000 end-users, and compare it with classical fraud detection approaches. With 99.81% precision and 90.18% recall, we achieve better recognition performance in comparison with the state of the art.

3. BitTorrent Sync: Network Investigation Methodology
   Mark Scanlon, Jason Farina, M-Tahar Kechadi (University College Dublin, Irreland)

   Abstract: The volume of personal information and data most Internet users find themselves amassing is ever increasing, and the fast pace of the modern world results in most people requiring instant access to their files. Millions of these users turn to cloudbased file synchronisation services, such as Dropbox, Microsoft SkyDrive, Apple iCloud and Google Drive, to enable “alwayson” access to their most up-to-date data from any computer or mobile device with an Internet connection. The prevalence of recent articles regarding invasion of privacy issues and data protection breaches in the media has caused many to review their online personal data security practices. To provide an alternative to cloud-based file backup and synchronisation, BitTorrent Inc. released an alternative cloudless file backup and synchronisation service, named BitTorrent Sync in April 2013. BitTorrent Sync’s popularity rose dramatically throughout 2013, reaching over two million active users by the end of the year. This paper outlines a number of scenarios where the network investigation of the service may prove invaluable as part of a digital forensic investigation. An investigation methodology is proposed outlining the required steps involved in retrieving digital evidence from the network and the results from a proof of concept investigation are presented.

16:00 – 16:30 Coffee Break

16:30 – 18:00 Parallel Sessions

ARES Full II – Mobile Security and Attack Prevention – 9th International Conference on Availability, Reliability and Security

Session Chair: Collin Mulliner, Northeastern University, United States
Location: Lecture Hall E
Time: 16:30 – 18:00

1. Divide-and-Conquer: Why Android Malware Cannot Be Stopped

Dominik Maier, Tilo Müller, Mykola Protsenko (Friedrich-Alexander-Universität, Germany)

Abstract: In this paper, we demonstrate that Android malware can bypass all automated analysis systems, including AV solutions, mobile sandboxes, and the Google Bouncer. We propose a tool called Sand-Finger for the fingerprinting of Android-based analysis systems. By analyzing the fingerprints of ten unique analysis environments from different vendors, we were able to find characteristics in which all tested environments differ from actual hardware. Depending on the availability of an analysis system, malware can either behave benignly or load malicious code at runtime. We classify this group of malware as Divide-and-Conquer attacks that are efficiently obfuscated by a combination of fingerprinting and dynamic code loading. In this group, we aggregate attacks that work against dynamic as well as static analysis. To demonstrate our approach, we create proof-of-concept malware that surpasses up-to-date malware scanners for Android. We also prove that known malware samples can enter the Google Play Store by modifying them only slightly. Due to Android's lack of an API for malware scanning at runtime, it is impossible for AV solutions to secure Android devices against these attacks.

2. DroidForce: Enforcing Complex, Data-centric, System-wide Policies in Android

Siegfried Rasthofer, Steven Arzt (Technische Universität Darmstadt, Germany), Enrico Lovat (Technische Universität München, Germany), Eric Bodden (Technische Universität Darmstadt, Germany)

Abstract: Smartphones are nowadays used to store and process many kinds of privacy-sensitive data such as contacts, photos, and e-mails. Sensors provide access to the phone's physical location, and can record audio and video. While this is convenient for many applications, it also makes smartphones a worthwhile target for attackers providing malicious applications. Current approaches to runtime enforcement try to mitigate unauthorized leaks of confidential data. However, they are often capable of enforcing only a very limited set of policies, like preventing data leaks only within single components or monitoring access only to specific sensitive system resources. In this work, we present Droid Force, an approach for enforcing complex, data-centric, system-wide policies on Android applications. Droid Force allows users to specify fine-grained constraints on how and when which data may be processed on their phones, regardless of whether the malicious behavior is distributed over different colluding components or even applications. Policies can be dynamically exchanged at runtime and no modifications to the operating system nor root access to the phone are required. Droid Force works purely on the application level. It provides a centralized policy decision point as a dedicated Android application and it instruments a decentralized policy enforcement point into every target application. Analyzing and instrumenting an application takes in total less than a minute and secured applications exhibit no noticeable slowdown in practice.

3. Lobotomy: An Architecture for JIT Spraying Mitigation

Martin Jauernig, Matthias Neugschwandtner, Christian Platzer (Vienna University of Technology, Austria), Paolo Milani Comparetti (Lastline Inc., United States)

Abstract: JIT spraying has an assured spot in an attacker's toolkit for Web browser exploitation: With JIT spraying an attacker is able to circumvent even the most sophisticated defense strategies against code injection, including address space layout randomization (ASLR), data execution prevention (DEP) and stack canaries. In this paper, we present Lobotomy, an architecture for building injection-safe JIT engines. Lobotomy is secure by design: it separates compiler and executor of a JIT engine in different processes that share the memory regions containing the compiled code. This allows us to use least-privilege access rights for both processes, preventing memory regions to be mapped with write- and execute-rights at the same time. Our proof-of-concept implementation that modifies the well-known Fire fox JIT engine Trace monkey shows both the effectiveness and real-world feasibility of our architecture. Additionally, we provide a thorough evaluation of our version compared to an unmodified baseline and competing approaches.

SeCIHD III – 4th IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense

Session Chair: Antonio J. Jara, University of Applied Sciences Western Switzerland, Switzerland
Location: Lecture Hall C
Time: 16:30 – 18:00

1. Expert Knowledge based Design and Verification of Secure Systems with Embedded Devices

Vasily Desnitsky, Igor Kotenko (St. Petersburg Institute for Informatics and Automation, Russia)

Abstract: The sweeping growth of the amount of embedded devices together with their extensive spread pose extensively new design challenges for protection of embedded systems against a wide set of security threats. The embedded device specificity implies combined protection mechanisms require effective resource consumption of their software/hardware modules. At that the design complexity of modern embedded devices, characterized by the proper security level and acceptable resource consumption, is determined by a low structuring and formalization of security knowledge. The paper proposes an approach to elicit security knowledge for subsequent use in automated design and verification tools for secure systems with embedded devices.

2. Towards analysis of sophisticated attacks, with conditional probability, genetic algorithm and a crime function

Wolfgang Boehmer (Technische Universität Darmstadt, Germany)

Abstract: In this short article, a proposal to simulate a sophisticated attack on a technical infrastructure is discussed. Attacks on (critical) infrastructures can be modeled with attack trees, but regular (normal) attack trees have some limitation in the case of a sophisticated attack like an advanced persistent (sophisticated) attack. Furthermore, attacks can also be simulated to understand the type of attack, and in order to subsequently develop targeted countermeasures. In this case, a normal, and also a sophisticated attack, is typically carried out in three phases. In the first phase (I) extensive information is gathered about the target object. In the second phase (II), the existing information is verified with a target object scan. In the third phase (III), the actual attack takes place. A normal attack tree is not able to explain this kind of attack behavior. So, we advanced a normal attack tree, which uses conditional probability according to Bayes to go through a certain path - step by step - from the leaf to the root. The learning ability, which typically precedes an attack (phase II), is simulated using a genetic algorithm. To determine the attack, we used threat trees and threat actors. Threat actors are weighted by a function that is called criminal energy. In a first step, it proposes three types of threat actors. The vulnerabilities have been identified as examples for a laboratory network.

3. Detection of Malicious Web Pages using System Calls Sequences

Gerardo Canfora (University of Sannio, Italy), Eric Medvet (University of Trieste, Italy), Francesco Mercaldo, Corrado Aaron Visaggio (University of Sannio, Italy)

Abstract: Web sites are often used for diffusing malware; an increasingly number of attacks are performed by delivering malicious code in web pages: drive-by download, malvertisement, rogueware, phishing are just the most common examples. In this scenario, JavaScript plays an important role, as it allows to insert code into the web page that will be executed on the client machine, letting the attacker to perform a plethora of actions which are necessary to successfully accomplish an attack. Existing techniques for detecting malicious JavaScript suffer from some limitations like: the capability of recognizing only known attacks, being tailored only to specific attacks, or being ineffective when appropriate evasion techniques are implemented by attackers. In this paper we propose to use system calls to detect malicious JavaScript. The main advantage is that capturing the system calls allows a description of the attack at a very high level of abstraction. On the one hand, this limits the evasion techniques which could succeed, and, on the other hand, produces a very high detection accuracy (96%), as experimentation demonstrated.

4. Risk Reduction Overview: A visualization method for risk management

Hellen Havinga (Rijkswaterstaat, The Netherlands), Olivier Sessink (Ministry of Defense, The Netherlands)

Abstract: The Risk Reduction Overview (RRO) method presents a comprehensible overview of the coherence of risks, measures and residual risks. The method is designed to support communication between different stakeholders in complex risk management. Seven reasons are addressed why risk management in IT security has many uncertainties and fast changing factors, four for IT security in general and three for large organizations specifically. The RRO visualization has been proven valuable to discuss, optimize, evaluate, and audit a design or a change in a complex environment. The method has been used, evaluated, and improved over the last six years in large government and military organizations. Seven areas in design and decision making are identified in which a RRO is found to be beneficial. Despite the widely accepted need for risk management

we believe this is the first practical method that delivers a comprehensive overview that improves communication between different stakeholders.

RISI III – Resilient Networks – 4th International Workshop on Resilience and IT-Risk in Social Infrastructures

Session Chair: Stefan Sackmann, Martin-Luther University of Halle-Wittenberg, Germany
Location: Lecture Hall D
Time: 16:30 – 18:00

1. Keynote: Risk-Aware Design and Management of Resilient Networks
   Piotr Cholda (AGH University of Science and Technology, Poland)

   Abstract: A current view on the design of networks resilient to non-malicious failures supported by risk engineering is presented in this keynote. The aspect of risk response is emphasized.

18:00 – 22:00 Welcome Reception

The Welcome Reception will take place shortly after the last session in the bar / restaurant "Le Quai" next to the University.

Address:

Le Quai
Route de la Fonderie 6
1700 Fribourg
Switzerland

Tuesday, 09 September 2014

08:00 – 17:30 Registration for all events

09:00 – 10:30 Plenary Session

Keynote

Location: Lecture Hall A
Time: 09:00 – 10:30

Mass surveillance and cryptology

Bart Preneel (Katholieke Universiteit Leuven, Belgium)

Abstract: The implications of the Snowden revelations have brought to the light interesting research challenges in the area of information security and cryptology. It has become clear that nation states do not limit themselves to large scale passive eavesdropping, but have moved towards sophisticated traffic analysis techniques and active attacks on networks and end systems. Moreover, in the next years one can expect a deployment of ever more sophisticated techniques by a growing number of actors. The awareness of these threats has resulted in an increased interest in the implementation of cryptographic mechanisms; a key question is whether the current cryptographic mechanisms are adequate to protect against these advanced opponents. We will also discuss which areas pose the largest challenges and which defenses have the best chances to be effective.

10:30 – 11:00 Coffee Break

11:00 – 12:30 Parallel Sessions

ARES Short I – Ontologies and Integrated Devices – 9th International Conference on Availability, Reliability and Security

Session Chair: Peter Kieseberg, SBA Research, Austria
Location: Lecture Hall E
Time: 11:00 – 12:30

1. EM Leakage of RFID Devices—Comparison of Two Measurement Approaches
   Thomas Korak (Graz University of Technology, Austria), Thomas Plos (NXP Semiconductors Austria, Austria)

   Abstract: Security-relevant applications applying contactless communication technologies based on radio-frequency identification (RFID) need to be robust against side-channel analysis (SCA) attacks. This work compares two measurement approaches for evaluating the robustness of RFID devices against SCA attacks: Analogue demodulation and resolution optimization of the oscilloscope. Several distances for measuring the side-channel information have been evaluated showing that above a specific distance the resolution optimization outperforms the analogue pre-processing. By applying a pre-processing step, the results can further be improved. With an appropriate measurement setup the effort for a security evaluation can be decreased, further leading to faster time-to-market and reduced development costs.

2. Supporting Security Automation for Multi-chassis Link Aggregation Groups via the Interconnected-Asset Ontology
   Henk Birkholz, Ingo Sieverdingbeck (Fraunhofer Institute for Secure Information Technology, Germany)

   Abstract: Multi-chassis (MC) endpoints and link aggregation groups (LAG) are common configurations in production networks today. Security automation processes that rely on correct topological data require a machine-process able representation of corresponding network topologies. Unfortunately, MC-LAG setups can be interpreted in more than one way regarding the topological layout, which complicates the process significantly. In this paper we present an extension to the Interconnected-asset topology (IO) that provides detailed data about topologies in process-specific views to better support security automation processes.

3. Concurrent Queries in Location Based Services
Emad Elabd (Menoufia University, Egypt), Mohand-Said Hacid (University Claude Bernard Lyon, France)

Abstract: The location-based services (LBS) are gaining a great importance due to the tremendous development in telecommunications and geographic information systems. In addition, the spread of laptops and mobile devices that can use these services at anytime and anywhere helps the diffusion of this type of application. Nevertheless, there are significant challenges that could impede the use of this type of services. User's Privacy is considered as one of these important challenges that limit the usage of these services because this type of services is user location based. Thereby, different techniques are developed to preserve the user location privacy while s/he uses the LBS. Most of these techniques depend on the Kanonymity [11] of user's location by querying about a spatial region that contains k-1 users. Thus, the adversary cannot detect the user who asked for the service from these k users. However, if the adversary is in possession of some information about the users such as users' profiles and historical queries1, s/he can discover in a high percentage the query issuer from the k users in the spatial region. In addition, if several users in a specified spatial area send at the same time their requests, the potential attacks targeting the privacy in the LBS could increase. In this paper, we investigate the impact of users' profiles and previously issued queries by the users in case of concurrent queries on the privacy. We propose an algorithm for predicating the issuer of each query and her/his underlying location in case of concurrent queries based on the users' profiles, historical queries, and the spatial area geographical characteristics. The experiments show that the concurrent queries affect negatively the privacy level in the location based services.

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 I – Knowledge Management – International Cross Domain Conference and Workshop

Location: Lecture Hall B
Time: 11:00 – 12:30

1. Argumentation-based group decision support for collectivist communities
Marijke Coetzee (University of Johannesburg, South Africa)

Abstract: In collectivist communities, decisions are taken by groups of people who prefer to consider the opinions of their in-group. For them it is important to reach group consensus by focusing on the group's preferences and goals. Such decision processes can be supported by multi-criteria decision analysis that identifies sets of objectives, representing subjective values used in decision making, to better generate recommendations. Recently, several attempts have been made to ex-plain and suggest alternatives in decision-making problems by using arguments. Argumentation theory is the process of bringing together arguments so that conclusions can be justified and explained. Each potential decision usually has arguments for or against it, of various strengths. For collectivist communities, the non-monotonicity of argumentation theory is useful as it supports an adaptive decision-making style. The fact that the opinions of group members can be evaluated and replaced, if they are found lacking via a group opinion strategy, fits well with collectivist decision-making. This paper proposes a framework that allows a group of users, belonging to a collectivist and mostly rural community, to share their opinions when making decisions such as buying goods in bulk in order by incorporating their cultural beliefs in the system design.

3. A Knowledge Integration approach for Safety-Critical Software Development and Operation based on the Method Architecture
Shuichiro Yamamoto (Nagoya University, Japan)

Abstract: It is necessary to integrate practical software development and operation body of knowledge to deploy development and operation methods for assuring safety. In this paper, an approach based on the method architecture is proposed to develop a Knowledge integration method for describing various software related bodies of knowledge and the safety case for assuring software life cycle and operation processes.

4. Metrics-based incremental determinization of finite automata

Sergiu Balan, Gianfranco Lamperti (Università degli Studi di Brescia, Italy), Michele Scandale (Politecnico di Milano, Italy)

Abstract: Some application domains, including monitoring of active systems in artificial intelligence and model-based mutation testing in software engineering, require determinization of finite automata to be performed incrementally. To this end, an algorithm called Incremental Subset Construction (ISC) was proposed a few years ago. However, this algorithm was recently discovered to be incorrect is some instance problems. The incorrect behavior of ISC originates when the redirection of a transition causes a portion of the automaton to be disconnected from the initial state. This misbehavior is disturbing in two ways: portions of the resulting automaton are disconnected and, as such, useless; moreover, a considerable amount of computation is possibly wasted for processing these disconnected parts. To make ISC sound, a metrics-based technique is proposed in this paper, where the distance between states is exploited in order to guarantee the connection of the automaton, thereby allowing ISC to achieve soundness. Experimental results show that, besides being effective, the proposed technique is efficient too.

SeCIHD IV – 4th IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense

Session Chair: Antonio J. Jara, University of Applied Sciences Western Switzerland, Switzerland
Location: Lecture Hall C
Time: 11:00 – 12:30

1. Towards a Key Consuming Detection in QKD-VoIP Systems

Guohong Zhao, Wanrong Yu, Baokang Zhao, Chunqing Wu (National University of Defense Technology, China)

Abstract: Quantum Key Distribution (QKD) technology, based on laws of quantum physics, can generate unconditional security keys between two communication parties. QKD is nearly a commercial technology and can make it available to the public. In existing QKD networks and commercial QKD systems, classical network is an essential part of the implementation of QKD protocols. With security keys and encryption scheme (one-time pad), we can protect the security of various network applications. But the public classical channel in QKD network may suffers potential key consuming attacks. In this paper, we focus on how to detecting the potential attacks during the security applications in the QKD network. Especially, we propose a Dynamic Key Consuming Detection scheme (DKode) in QKD-VoIP systems which encrypting VoIP streams with security keys from QKD systems.

5. A Structure P2P based Web Services Registry With Access and Control

Qian He, Baokang Zhao (National University of Defense Technology, China), Yunjian Long (Guilin University of Electronic Technology, China), Jinshu Su (National University of Defense Technology, China), Ilsun You (Korean Bible University, South Korea)

Abstract: In the cloud computing, there are massive functions and resources are encapsulated into Web services. The traditional web service registry systems normally using the central architecture can't meet the requirements of cloud computing. A web service registry system based on structured P2P system with secure access and control is implemented. Multiple Universal Description, Discovery and Integration (UDDI) nodes are organized by the P2P based schedule and communication mechanism. The registration and discovery of Web services is redesigned to the new system that provides services like one single UDDI server. The experiment results show that the capacity can be ex- tended dynamically and support large scalable access.

6. A High-Speed Network Content Filtering System

Guohong Zhao, Shuhui Chen, Baokang Zhao (National University of Defense Technology, China), Ilsun You (Korean Bible University, South Korea), Jinshu Su, Wanrong Yu (National University of Defense Technology, China)

Abstract: Current software based Content Filtering Systems are too computing intensive in large scale packets payload detection and cannot meet the performance requirements of modern networks. Thus, hardware architectures are de- sired to speed up the detection process. In this paper, hardware based Conjoint Network Content Filtering System (CNCFS) is proposed to solve the problem. In CNCFS, a TCAM based algorithm named Linking Shared Multi-Match (LSMM) is implemented, which can speed up large scale Multi-Pattern Multi-Matching greatly. Also, this system can also be used in high speed mobile networks which need to deal with the security of fast handover of mobile users. The results of performance evaluation show that our solution can provide 5 Gbps wire speed processing capability.

7. Amplification DDoS Attacks: Emerging Threats and Defense Strategies

Antonio Colella (Italian Army and Italian Atlantic Committee, Italy), Clara Maria Colombini (University of Milan, Italy)

Abstract: There are too many servers on the Internet that have already been used, or that are vulnerable and can potentially be used to launch DDoS attacks. Even though awareness increases and organizations begin to lock down those systems, there are plenty of other protocols that can be exploited to be used instead of them. One example is the Simple Network Management Protocol (SNMP), which is a common UDP protocol used for network management. Several types of network devices actually come with SNMP "on" by default. A request sent to an SNMP server returns a response that is larger than the query that came in. The main aim of this paper is to investigate on the increasing prevalence and destructive power of amplification-based distributed denial of service (DDoS) attacks in order to present a solution based on a profiling methodology. The paper encompass three aspects: amplification DDoS attacks and main port used, the profiling methodology as a mean of identifying the threat and shape it. Finally, a proposal solution is given by considering both strategic and technical aspects.

12:30 - 14:00 Lunch

14:00 – 15:30 Parallel Sessions

ARES Full III – Secure Protocols – 9th International Conference on Availability, Reliability and Security

Session Chair: Edgar Weippl, SBA Research, Austria
Location: Lecture Hall E
Time: 14:00 – 15:30

1. A Formal Model and Analysis of the MQ Telemetry Transport Protocol

Benjamin Aziz (University of Portsmouth, UK)

Abstract: We present a formal model of the MQ Telemetry Transport version 3.1 protocol based on a timed message-passing process algebra. We explain the modeling choices that we made, including pointing out ambiguities in the original protocol specification, and we carry out a static analysis of the formal protocol model, which is based on an approximation of a name-substitution semantics for algebra. The analysis reveals that the protocol behaves correctly as specified against the first two quality of service modes of operation providing at most once and at least once delivery semantics to the subscribers. However, we find that the third and highest quality of service semantics is prone to error and at best ambiguous in certain aspects of its specification. Finally, we suggest an enhancement of this level of QoS for the protocol.

2. Practical Attack on Bilinear Pairings to Disclose the Secrets of Embedded Devices

Thomas Unterluggauer, Erich Wenger (Graz University of Technology, Austria)

Abstract: Identity-based encryption constitutes a promising alternative to traditional cryptography that works without symmetric keys or public key infrastructures. Such schemes generally depend on the computation of bilinear pairings. The latest developments in efficient pairing algorithms made identity-based encryption available to embedded devices as well. However, those devices are inherently exposed to side-channel attacks. In this paper, we present a correlation power analysis attack to extract the private key in the popular identity-based encryption scheme by Boneh and Boyen. On an ARM Cortex-M0 we exploit the leakage of a finite field multiplication within the highly practical optimal-Ate pairing defined over the elliptic curves by Barreto and Naehrig. As a secondary contribution, we practically verified the feasibility of our attack on an FPGA, an ASIC, and using power simulations. For future work our research intends to raise awareness of the importance of the randomization countermeasure in pairing computations.

3. Run-Time Risk Management in Adaptive ICT Systems

Ricardo Neisse, Igor Nai Fovino, Gianmarco Baldin (European Commission Joint Research Centre, Italy), Vera Stavroulaki, Panagiotis Vlacheas (University of Piraeus, Greece), Raffaele Giaffreda (CREATE-NET, Italy)

Abstract: The control and protection of user data is a very important aspect in the design and deployment of the Internet of Things (IoT). The heterogeneity of the IoT technologies, the number of the participating devices and systems, and the different types of users and roles create important challenges in the IoT context. In particular, requirements of scalability, interoperability and privacy are difficult to address even with the considerable amount of existing work both in the research

and standardization community. In this paper we propose a Model-based Security Toolkit, which is integrated in a management framework for IoT devices, and supports specification and efficient evaluation of security policies to enable the protection of user data. Our framework is applied to a Smart City scenario in order to demonstrate its feasibility and performance.

CD-ARES II – Software Security – International Cross Domain Conference and Workshop

Location: Lecture Hall B
Time: 14:00 – 15:30

1. Towards Developing Secure Software using Problem-oriented Security Patterns

Azadeh Alebrahim, Maritta Heisel (University of Duisburg-Essen, Germany)

Abstract: Security as one essential quality requirement has to be addressed during the software development process. Quality requirements such as security drive the architecture of a software, while design decisions such as security patterns on the architecture level in turn might constrain the achievement of quality requirements significantly. Thus, to obtain sound architectures and correct requirements, knowledge which is gained in the solution space, for example from security patterns, should be reflected in the requirements engineering. In this paper, we propose an iterative method that takes into account the concurrent development of requirements and architecture descriptions systematically. It reuses security patterns for refining and restructuring the requirement models by applying problem-oriented security patterns. Problem-oriented security patterns adapt existing security patterns in a way that they can be used in the problem-oriented requirements engineering. The proposed method bridges the gap between security problems and security architectural solutions.

2. Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services

Igor Kotenko, Evgenia Novikova (St. Petersburg Institute for Informatics and Automation, Russia)

Abstract: Mobile money transfer services (MMTS) are currently being deployed in many markets across the world and are widely used for domestic and international remittances. However, they can be used for money laundering and other illegal financial operations. The paper considers an interactive multi-view approach that allows describing metaphorically the behavior of MMTS subscribers according to their transaction activities. The suggested visual representation of the MMTS users' behavior based on the RadViz visualization technique helps to identify groups with similar behavior and outliers. We describe several case studies corresponding to the money laundering and behavioral fraud. They are used to assess the efficiency of the proposed approach as well as present and discuss the results of experiments.

3. A review of Security Requirements Engineering methods with respect to Risk Analysis and Model-Driven Engineering

Denisse Munante, Vanea Chiprianov, Laurent Gallon, Philippe Aniorte (University of Pau, France)

Abstract: One of the most important aspects that help improve the quality and cost of secure information systems in their early stages of the development lifecycle is Security Requirements Engineering (SRE). However, obtaining such requirements is non-trivial. One domain dealing also with eliciting security requirements is Risk Analysis (RA). Therefore, we perform a review of SRE methods in order to analyse which ones are compatible with RA processes. Moreover, the transition from these early security requirements to security policies at later stages in the lifecycle is generally non-automatic, informal and incomplete. To deal with such issues, model-driven engineering (MDE) uses formal models and automatic model transformations. Therefore, we also review which SRE methods are compatible with MDE approaches. Consequently, our review is based on criteria derived partially from existing survey works, further enriched and specialized in order to evaluate the compatibility of SRE methods with the disciplines of RA and MDE. It summarizes the evidence regarding this issue so as to improve understanding and facilitate evaluating and selecting SRE methods.

4. Adaptive User-Centered Security

Sven Wohlgemuth (Center for Advanced Security Research Darmstadt, Germany)

Abstract: One future challenge in informatics is the integration of humans in an infrastructure of data-centric IT services. A critical activity of this infrastructure is trustworthy information exchange to reduce threats due to misuse of (personal) information. Privacy by Design as the present methodology for developing privacy-preserving and secure IT systems aims to reduce security vulnerabilities already in the early requirement analysis phase of software development. Incident reports show, however, that not only an implementation of a model bears vulnerabilities but also the gap between rigorous view of threat and security model on the world and the real view of a run-time environment with its dependencies. Dependencies threaten reliability of information, and in case of personal information, privacy as well. With the aim of improving security

and privacy, this work proposes to implement Privacy by Design by adapting an IT system to security vulnerabilities and their users' views on an information exchange and its IT support with eventually opposite security interests.

WSDF – 7th International Workshop on Digital Forensics

Session Chair: Richard Overill, King's College London, UK & Martin Mulazzani, SBA Research, Austria
Location: Lecture Hall C
Time: 14:00 – 15:30

1. Real-Time Screen Watermarking Using Overlaying Layer

Maciej Piec, Andreas Rauber (SBA Research, Austria)

Abstract: Protection of intellectual property is a well researched area of computer science. There are many methods that allow securing information that should not be available to unauthorized parties. Many of these techniques provide protection on a relatively low level such as file encryption or filtering of network traffic. However, many of the mechanisms fail as soon as someone attempts to save the content of the screen that is displaying the sensitive data. Such a malicious insider can cause serious harm to an organization's reputation and finances. It is important in case of such incidents to be able to track the source of the leak. In this paper a method for watermarking the screen image, that can be used in forensic investigations, is presented. The imperceptible digital watermark is placed on the overlay layer over the whole computer screen. Our method leverages the Human Visual System (HVS) properties and allows to generate dynamically adaptable watermarks that respond to the currently displayed content by using the FAST feature detection algorithm. We use QR Codes that provide spatial non-uniformity and error correction capabilities. The evaluation shows that our scheme works well in the selected use-case scenarios. We show that the watermark is robust against modifications typical for office processing, such as cropping and quality preserving JPEG compression.

2. An Efficient Intrinsic Authorship Verification Scheme Based on Ensemble Learning

Oren Halvani, Martin Steinebach (Fraunhofer Institute for Secure Information Technology, Germany)

Abstract: Authorship Verification is an important sub discipline of digital text forensics. Its goal is to decide, if two texts are written by the same author or not. We present an efficient Authorship Verification scheme based on an ensemble of K-Nearest Neighbor classifiers, where each classifier generates a decision regarding a feature category. Our scheme provides many benefits such as, for instance, the independence of linguistic resources like thesauruses or language models. Furthermore, it can handle different Indo-European languages as for instance English, German, Spanish, Greek, Dutch, Swedish or French. Another benefit is the low runtime, due to the fact that deep linguistic processing (tagging, chunking, parsing, etc.) is not taken into account. Moreover, our scheme can easily be modified for example by replacing the involved distance function, the acceptance criterion or the used features including their parameters. The proposed scheme is evaluated against the publicly available PAN-2013 Author Identification (AI) test corpus, where it was ranked as the second-best in the top ten list, as well as against five other test corpora, compiled by our own. We show in our experiments that it is possible to achieve promising results, even when using a fixed setting of parameters and features across seven different languages.

3. Efficient Cropping-Resistant Robust Image Hashing

Martin Steinebach (Fraunhofer SIT, Germany), Huajian Liu (Chinese Academy of Sciences, China), York Yannikos (Fraunhofer SIT, Germany)

Abstract: A digital forensics examiner often has to deal with large amounts of multimedia content during an investigation. One important part of such an investigation is to identify illegal material like pictures containing child pornography. Robust image hashing is an effective technique to help identifying known illegal images even after the original images were modified by applying various image processing operations. However, some specific operations lead to increased false negative rates when using robust image hashing. One of the most challenging operations today is image cropping. In this work we introduce an approach to counter cropping operations on images by combining image segmentation and efficient block mean image hashing. We show that we are able to achieve high detection rates for images where cropping operations where applied on the original known source. This further improves the robustness of our image hashing approach.

15:30 – 16:00 Coffee Break

16:00 – 17:30 Parallel Sessions

ARES Full IV – Trust and Availability – 9th International Conference on Availability, Reliability and Security

Session Chair: Martin Mulazzani, SBA Research, Austria
Location: Lecture Hall E
Time: 16:00 – 17:30

1. Rethread: A Low-Cost Transient Fault Recovery Scheme for Multithreaded Processors
Jian Fu, Qiang Yang, Raphael Poss, Chris R. Jesshope (University of Amsterdam, The Netherlands), Chunyuan Zhang (National University of Defense Technology, China)

Abstract: Transient fault recovery is important in processor availability. However, significant silicon or performance overheads are characteristics of existing techniques. We uncover an opportunity to reduce the overheads dramatically in modern processors that appears as a side-effect of introducing hardware multithreading to improve performance. We observe that threads are usually short code sequences with no branches and few memory side-effects, which means that the number of checkpoints is small and constant. In addition, the state structures of a thread already presented in hardware can be reused to provide check pointing. In this paper, we demonstrate this principle of using a hardware/software co-design called Rethread, which features compiler-generated code annotations and automatic recovery in hardware by restarting threads. This approach provides the ability to recover from transient faults without dedicated hardware. Moreover, results show performance degradation under both fault-free condition (<5%) and as a function of fault rate.

2. Visualizing Transaction Context in Trust and Reputation Systems
Johannes Sänger, Günther Pernul (University of Regensburg, Germany)

Abstract: Transaction context is an important aspect that should be taken into account for reputation-based trust assessment, because referrals are bound to the situation-specific context in which they were created. The non-consideration of transaction context may cause several threats such as the value imbalance problem. Exploiting this weakness, a seller can build high reputation by selling cheap products while cheating on the expensive ones. In the recent years, multiple approaches have been introduced that address this challenge. All of them chose metrics leading to numerical reputation values. These values, however, are non-transparent and quite hard to understand for the end-user. In this work, in contrast, we combine reputation assessment and visual analytics to provide an interactive visualization of multivariate reputation data. We thereby allow the user to analyze the data sets and draw conclusions by himself. In this way, we enhance transparency, involve the user in the evaluation process and as a consequence increase the users' trust in the reputation system.

3. Enhanced Configuration Generation Approach for Highly Available COTS Based Systems
Parsa Pourali, Ferhat Khendek (Concordia University, Canada), Maria Toeroe (Ericsson, Canada)

Abstract: The design of configurations for high availability management is a complex and error prone task. Automation of the process is a first step towards improving the quality of such configurations and for exploring the different potential solutions for a given set of requirements. An automated approach for configuration generation for applications deployed on top of the Service Availability Forum (SAForum) middleware has been proposed in the literature. This approach, however, may generate several configurations among which some may not meet the required level of service availability. Therefore, these configurations need to be analyzed to select one for the deployment. This is a complex process as many configurations may be generated and considered throughout the process. In this paper, we propose to enhance this configuration generation approach with a method to eliminate early in the generation process some configurations that cannot meet the service availability requirement. The method estimates the service availability for the different possible combinations of software components, which can provide the requested services, taking into account the properties of these components and the behaviour of the SAForum middleware.

4. Phishdentity: Leverage Website Favicon to Offset Polymorphic Phishing Website
Jeffrey Choo Soon Fatt, Chiew Kang Leng, Sze San Nah (Universiti Malaysia Sarawak, Malaysia)

Abstract: Phishing attacks involve the use of fuzzy techniques to create polymorphic phishing web pages to give the impression of legitimate websites. Many websites are subject to the threat of phishing, including financial, social networks, tourism, e-commerce etc. For example, phishers are particularly fond of travel-related services by imitating as trip consultant, airline reservation, hotel booking etc. However, the targeted legitimate websites still maintain the webpage appearance visually similar to the original. In this paper, we propose an approach which is based on the website favicon to find the identity of a website and use it to evaluate the genuineness of a website. This approach utilizes Google search-by-image API to return the search results pages. Then, we perform latent semantic analysis based on the search results pages. We collected 1,000 webpages to verify the effectiveness of this approach. The results show that our proposed method achieved 97.2% true positive with only 5.4% false positive.

CD-ARES III – Mobile and Social Computing – International Cross Domain Conference and Workshop

Location: Lecture Hall B
Time: 16:00 – 17:30

1. Mobile Computing is not Always Advantageous: Lessons Learned from a Real-World Case Study in a Hospital

Andreas Holzinger, Bettina Sommerauer (Medical University Graz, Austria), Peter Spitzer (Graz University Hospital, Austria), Simon Juric, Borut Zalik, Matjaz Debevc (University of Maribor, Slovenia), Chantal Lidynia, André Calero Valdez (RWTH Aachen University, Germany), Carsten Röcker (Medical University Graz, Austria), Martina Ziefle (RWTH Aachen University, Germany)

Abstract: The use of mobile computing is expanding dramatically in recent years and trends indicate that “the future is mobile”. Nowadays, mobile computing plays an increasingly important role in the biomedical domain, and particularly in hospitals. The benefits of using mobile devices in hospitals are no longer disputed and many applications for medical care are already available. Many studies have proven that mobile technologies can bring various benefits for enhancing information management in the hospital. But is mobility a solution for every problem? In this paper, we will demonstrate that mobility is not always an advantage. On the basis of a field study at the pediatric surgery of a large University Hospital, we have learned within a two-year long mobile computing project, that mobile devices have indeed many disadvantages, particularly in stressful and hectic situations and we conclude that mobile computing is not always advantageous.

2. Semantic-aware Mashups for Personal Resources in SemanticLIFE and SocialLIFE

Sao-Khue Vo, Amin Anjomshoaa, A Min Tjoa (Vienna University of Technology, Austria)

Abstract: SemanticLIFE is a Semantic Desktop system, which deals with the personal lifetime data. However, SemanticLIFE is limited to local storage, which is an isolated data repository. In the recent years, people have the tendency to share their resources, which are not only stored locally on their personal computers, but also hosted on social networking sites (SNSs). We propose and use the term ‘SocialLIFE’ to denote one’s lifetime information in SNSs, in which personal resources are his/her activities, interests, and related connections. In this paper, we also propose a mashup language and a semantic-based mashup framework. The final goal of this research is to provide a semantic- based way for bridging the gap between SemanticLIFE and SocialLIFE in order to integrate and reuse existing personal resources of existing applications such as information resources of Semantic Desktops and SNSs. The proposed mashup system also aims to supports non-expert users to create data mashups based on semantic-aware mashup dataflow.

3. Towards Interactive Visualization of Longitudinal Data to support Knowledge Discovery on Multi-Touch Tablet Computers

Andreas Holzinger, Michael Schwarz, Bernhard Ofner, Fleur Jeanquartier (Medical University Graz, Austria), Andre Calero-Valdez (RWTH Aachen University, Germany), Carsten Roecker (Medical University Graz, Austria), Martina Ziefle (RWTH Aachen University, Germany)

Abstract: A major challenge in modern data-centric medicine is the increasing amount of time-dependent data, which requires efficient user-friendly solutions for dealing with such data. To create an effective and efficient knowledge discovery process, it is important to support common data manipulation tasks by creating quick, responsive and intuitive interaction methods. In this paper we describe some methods for interactive longitudinal data visualization with focus on the usage of mobile multi-touch devices as interaction medium, based on our design and development experiences. We argue that when it comes to longitudinal data this device category offers remarkable additional interaction benefits compared to standard point-and-click desktop computer devices. An important advantage of multi-touch devices arises when interacting with particularly large longitudinal data sets: Complex, coupled interactions such as zooming into a region and scrolling around almost simultaneously is more easily achieved with the possibilities of a multi-touch device than compared to a regular mouse-based interaction device.

RAMSS I – 2nd 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 C
Time: 16:00 – 17:30

1. Practical Applications of Advanced Statistical Models in Reliability Data Analysis

Vasiliy Krivtsov (The Ford Motor Company, United States), Olexandr Yevkin (IHS, Canada)

Abstract: The purpose of this paper is to share some practical applications of advanced probabilistic models in reliability data analysis. In particular, we will focus on reliability models with fixed and time-dependent covariates. While these models are popular in biological and medical studies, their application in engineering reliability data analysis is still limited. As a special advanced topic, we also discuss a new approach to model/estimate MTTF using Pade approximation.

2. Stochastic Model for Medical Image Segmentation

Zeev Barzily (ORT Braude College, Israel), Mingyue Ding (Huazhong University of Science and Technology, China), Zeev Volkovich (ORT Braude College, Isreal)

Abstract: Stochastic modeling in image analysis aims to represent the images features in a small number of parameters so as to recognize the source producing the images. In this paper we address the image segmentation problem in the case of significantly differ segments' sizes. A probabilistic model dealing the distribution of gray level in the observed image is based on the Gaussian Mixture Model identifying each component a segment. According to the general segmentation methodology for multi-modal gray levels images we presume that every region-of-interest attaches to a distinct substantial mode of the empirical distribution of gray levels. So, the number of the components is evaluated via a new resampling procedure involving the Expectation-Maximization algorithm used in order to estimate the significant histograms picks. Stable states of our model are associated within of the proposed method with the "true" segments quantities specified by the appropriate components' quantities. Numerical experiments demonstrate the high ability of the proposed method.

3. Fast Monte Carlo Simulation Methods Adapted to Simple Petri Net Models

Stéphane Collas, Maïder Estecahandy (TOTAL S.A., France), Laurent Bordes, Christian Paroissin (Universit´e de Pau et des Pays de l'Adour, France)

Abstract: In oil and gas industry, the reliability analysis of High Integrity Protection Systems is an important issue. The standard modeling languages and the traditional methods employed for these studies are difficult to apply mainly because of the complexity of the operating context of these equipment. Thus, a powerful alternative is Petri nets associated with the Monte Carlo simulation (MC). However, obtaining accurate estimators on rare events (system failures) calls for very long computing times. To address this issue, the common methods are not well-suited to Petri Nets whereas the "Me thode de Conditionnement Temporel" (MCT) seems to be. Indeed, this method does not require to know the model distributions, however, it is only defined when the rare event is an absorbing state. To overcome this limitation, we first propose an extension of MCT (EMCT) to simple cases which represent repeated cycles where the failure event is either direct or in competition with other events. The first results show that EMCT gives better estimates than MC for a similar computing time. Second, we introduce a new computational technique, called Dissociation method, which is valid only if the components of the system are independent. We combine it with both MC and EMCT. Through different numerical examples, we observe a significant improvement of the obtained results.

4. Monte-Carlo Based Reliability Modelling of a Gas Network Using Graph Theory Approach

Pavel Praks, Vytis Kopustinskas (European Commission, Joint Research Centre, Italy)

Abstract: The aim of the study is to develop a European gas transmission system probabilistic model to analyse in a single computer model, the reliability and capacity constraints of a gas transmission network. We describe our approach to modelling the reliability and capacity constraints of networks elements, for example gas storages and compressor stations by a multi-state system. The paper presents our experience with the computer implementation of a gas transmission network probabilistic prototype model based on generalization of the maximum flow problem for a stochastic-flow network in which elements can randomly fail with known failure probabilities. The paper includes a test-case benchmark study, which is based on a real gas transmission network. Monte-Carlo simulations are used for estimating the probability that less than the demanded volume of the commodity (for example, gas) is available in the selected network nodes. Simulated results are presented and analysed in depth by statistical methods.

17:30 – 19:00 Sightseeing Tour

Meeting point: University of Fribourg, in front of the building, 17.30 (shortly after the last session)

Departure train: 17.45

Wednesday, 10 September 2014

08:00 – 17:00 Registration for all events

09:00 – 10:30 Plenary Session

Keynote

Location: Lecture Hall A
Time: 09:00 – 10:30

Monitoring Threats and Vulnerabilities in Complex IT Landscapes

Volkmar Lotz (SAP Research, Germany)

Abstract: Even when applying current best practices and technologies to secure software and IT landscapes, it would be inappropriate to assume that there are no remaining vulnerabilities and that there will be no attempts to exploit them. Hence, complementing security technology and management with means to detect and monitor vulnerabilities and attacks is an essential element in a comprehensive security strategy. In this talk, we investigate into two major challenges that monitoring solutions need to address in industrial-scale business application environments: the large amount of data that need to be processed to be able to, for instance, detect complex attacks spanning a number of components and layers, and the small amount of time that is available to react to, for instance, the discovery of zero-day exploits. We sketch a solution that exploits advanced in-memory database technology and an event stream processer to enable threat detection in real time over billions of events.

We present a second solution that addresses the prolongation of the time window to react to the publication of vulnerabilities in third party components used by an application. It has turned out that potential vulnerabilities are announced and discussed much earlier in social media than in the official channels like ver=ndor sites or vulnerability registries. Monitoring and analysing such media leads to a significant gain in response time.

10:30 – 11:00 Coffee Break

11:00 – 12:30 Parallel Sessions

ARES Short II – Security and Privacy – 9th International Conference on Availability, Reliability and Security

Session Chair: Matthias Neugschwandtner, Vienna University of Technology, Austria
Location: Lecture Hall E
Time: 11:00 – 12:30

1. What Does the Fox Say? On the Security Architecture of Firefox OS

   Marta Piekarska, Bhargava Shastry, Ravishankar Borgaonkar (Technische Universität Berlin, Germany)

   Abstract: We are witnessing a shift in the design of mobile operating systems from custom architectures to web-based platforms. This paper attempts to understand the security implications of bringing the smartphone to the web. We base our work on Firefox OS as the open nature of the project offers an insight into its design, and allows for the introduction of extensions to its security architecture. This paper has the following contributions: (1) Systematizing our knowledge about the security architecture of Firefox OS, (2) Pointing out shortcomings of Firefox OS's security architecture, (3) Formulating a threat model that web-based OSes face, and (4) Outlining directions for future research in the field

2. Palpable Privacy through Declarative Information Flows Tracking for Smart Buildings

   François Lesueur, Sabina Surdu (INSA-Lyon, France), Romuald Thion (Université Lyon, France), Yann Gripay, Meriam Ben Ghorbel-Talbi (INSA-Lyon, France)

Abstract: Smart buildings are more and more common due to recent technological advances. They promise to improve users' lives, but they are packed with sensors that gather user related data, fueling ever increasing privacy infringement suspicions. Captured data usually takes the form of dynamic streams, hence such buildings can naturally be programmed using Data Stream Management Systems (DSMSs) that execute long-running queries on data flowing from sensors. In this paper we address the problem of the dissemination control of private data, encountered in smart buildings. We introduce Tuple-Based Access Control (TBAC), a novel access control model that tracks sensor information flows in a DSMS. We provide users with the ability to enforce easy-to-understand, intuitive security policies on sensor-produced data. When such data are combined by queries in the system, so are their security policies, hence data access control is disseminated throughout the system. We argue that such a model is mandatory to ease the acceptance of smart buildings. Nevertheless, TBAC can also be relevant to other scenarios involving dissemination of aggregable private data.

3. Healthcare Services in the Cloud—Obstacles to Adoption, and a Way Forward
   Karin Bernsmed, Daniela Soares Cruzes, Martin Gilje Jaatun, Børge Haugset, Erlend Andreas Gjære (SINTEF ICT, Norway)

   Abstract: Cloud computing has been receiving a great deal of attention during the past few years. A major feature of public cloud services is that data are processed remotely in unknown systems that the users do not own or operate. This context creates a number of challenges related to data privacy and security and may hinder the adoption of cloud technology in, for example, the healthcare domain. This paper presents results from a stakeholder elicitation activity, in which the participants identified a number of obstacles to the adoption of cloud computing for the processing of healthcare data. We compare our results with previous studies and outline accountability as a possible way forward to increase the adoption of cloud services in the healthcare domain.

4. Privacy Dashboards: Reconciling Data-Driven Business Models and Privacy
   Christian Zimmermann, Rafael Accorsi, Günter Müller (University of Freiburg, Germany)

   Abstract: We argue for the use of Privacy Dashboards as enablers for privacy-enabled data-driven business models. Specifically, while dashboards are succesful instruments in business intelligence tools, their use in privacy protection is far less well-understood. Addressing this problem at the technical level, this paper provides a classification scheme for Privacy Dashboards and elaborates on the current state of the art to draw a research agenda for designing Privacy Dashboards that cater to users' desire of control and businesses' need for data collection and usage.

ECTCM I – 2nd International Workshop on Emerging Cyberthreats and Countermeasures

Session Chair: Markus Zeilinger, University of Applied Sciences Upper Austria, Austria
Location: Lecture Hall B
Time: 11:00 – 12:30

1. The SMM Rootkit Revisited: Fun with USB
   Joshua Schiffman, David Kaplan (Advanced Micro Devices, United States)

   Abstract: System Management Mode (SMM) in x86 has enabled a new class of malware with incredible power to control physical hardware that is virtually impossible to detect by the host operating system. Previous SMM root kits have only scratched the surface by modifying kernel data structures and trapping on I/O registers to implement PS/2 key loggers. In this paper, we present new SMM-based malware that hijacks Universal Serial Bus (USB) host controllers to intercept USB events. This enables SMM root kits to control USB devices directly without ever permitting the OS kernel to receive USB-related hardware interrupts. Using this approach, we created a proof-of-concept USB key logger that is also more difficult to detect than prior SMM-based key loggers that are triggered on OS actions like port I/O. We also propose additional extensions to this technique and methods to prevent and mitigate such attacks.

2. Towards a Hardware Trojan Detection Cycle
   Adrian Dabrowski, Heidelinde Hobel, Johanna Ullrich, Katharina Krombholz, Edgar Weippl (SBA Research, Austria)

   Abstract: Intentionally inserted malfunctions in integrated circuits, referred to as Hardware Trojans, have become an emerging threat. Recently, the scientific community started to propose technical approaches to mitigate the threat of unspecified and potentially malicious functionality. However, these detection and prevention mechanisms are still hardly integrated in the industry's Hardware development life cycles. We therefore propose in this work a secure hardware development life cycle that assembles methods from trustworthy software engineering. In addition to full traceability from specification to implementation, and down to each gate, we introduce a feedback detection cycle that systematically escorts every single step of the development process. To do so, we integrate different detection methods for each development phase that are derived from a common knowledge base.

3. PhiGARo: Automatic Phishing Detection and Incident Response Framework

Martin Husák, Jakub Cegan (Masaryk University)

Abstract: We present a comprehensive framework for automatic phishing incident processing and work in progress concerning automatic phishing detection and reporting. Our work is based upon the automatic phishing incident processing tool PhiGARo which locates users responding to phishing attack attempts and prevents access to phishing sites from the protected network. Although PhiGARo processes the phishing incidents automatically, it depends on reports of phishing incidents from users. We propose a framework which introduces honey pots into the process in order to eliminate the reliance on user input. The honey pots are used to capture e-mails, automatically detect messages containing phishing and immediately transfer them to PhiGARo. There is a need to propagate e-mail addresses of a honey pot to attract phishers. We discuss approaches to the honey pot e-mail propagation and propose a further enhancement to using honey pots in response to phishing incidents. We propose providing phishers with false credentials, accounts and documents that will grant them access to other honey pot services. Tracing these honey tokens may lead us to the originators of the phishing attacks and help investigations into phishing incidents.

RAMSS II – 2nd International Workshop on Statistical Methods in Reliability Assessment of Complex Industrial Multi-state Systems

Session Chair: Alex Karagrigoriou, University of the Aegean, Greece
Location: Lecture Hall C
Time: 11:00 – 12:30

1. Performance Determination for MSS Manufacturing System by Lz-Transform and Stochastic Processes Approach

Ilia Frenkel, Svetlana Daichman, Lev Khvatskin, Neta Avraham, Oshrit Zihry (SCE - Shamoon College of Engineering, Israel), Anatoly Lisnianski (The Israel Electric Corporation Ltd., Israel)

Abstract: We analyzed performance of industrial animal food additives manufacturer. Our primary focus is on production of food supplement for growing chickens. In order to determine the performance of manufacturing production system we constructed a mathematical model that based on Markov chains and represents the different states of each element and sub-systems in the system and the various production levels. The system can be represented as Markov model with 48 different states expressing the different performance levels of the entire process and created as system with 48 differential equations, solution of which is complicated problem. To overcome this obstacle we propose an application of the Lz-transform method for performance assessment of aging multi-state system (MSS) and its manufacturing capability. We demonstrated that the suggested method can be implemented in engineering decision making and construction of various MSS aging systems related to requirements, availability and production.

2. On Availability Comparison of Reservation Modes for Multi-state Air Conditioning Systems Using Markov Approach

Lev Khvatskin, Ilia Frenkel (SCE - Shamoon College of Engineering, Israel)

Abstract: In this paper we compare different reservation modes of Air conditioning systems for apartments, offices or cooling rooms that have a specific regime of temperature/humidity conditions. In the first reservation mode the required temperature and humidity conditions are provided by two cooling chillers (conditioners) with reserved chiller staying in cold reserve. In the second mode the reserved chiller orders from rented firm. Markov Models are built for comparison analysis of possible operation modes. The model takes into consideration the important factors such as cooling generators output, failure and repair rate, availability, time of supply of rented chiller. A numerical example is presented to illustrate the described approach.

3. Semi-Markov Modelling for Multi-state Systems

Vlad Stefan Barbu (University of Rouen, France), Alex Karagrigoriou (University of the Aegean, Greece), Andreas Makrides (University of Cyprus, Cyprus)

Abstract: Markov processes are widely used in reliability engineering. In this work we focus on multi state systems (MSS) and apply the Semi-Markov methodology for parameter estimation. For this purpose the sojourn times are assumed to be independent not identically distributed (inid) random variables that follow a general class of distributions that includes several popular reliability distributions like the exponential, Weibull, and Pareto.

4. Optimizing the Availability and the Operational Cost of a Periodically Inspected Multi-state Deteriorating System with Condition Based Maintenance Policies
Sonia Malefaki (University of Patras, Greece), Vasilis Koutras, Agapios Platis (University of the Aegean, Greece)

Abstract: In this paper a multi-state deterioration system which experiences several states of performance degradation until it fails is studied extensively and condition-based preventive maintenance policies are examined. The optimal maintenance policy aims at maximizing system's asymptotic availability and at minimizing its total operational cost, with respect to the two different inspection intervals. For the simultaneous optimization of the aforementioned measures, multi-objective optimization methods are employed. In the current work, the inspection times are assumed to be constant, thus the system's evolution in time is modeled by a semi-Markov process. Finally, the proposed system is compared with the corresponding Markov one which is the most commonly used approximation of the original system in practice.

ARES-IND I – ARES Industrial Track

Session Chairs: Kari Jussila, Aalto University, Finland & Juhani Anttila, IAQ, Finland
Location: Lecture Hall D
Time: 11:00 – 12:30

1. Keynote: Cloud Security Issues for SMEs
Gerald Quirchmayr (University of Vienna, Austria)

Abstract: Cloud computing is a very cost effective technology that already has a great impact on business applications, especially for small and medium size enterprises. While the technology itself comes at a very low cost for users and frees them from having to bother with the maintenance of infrastructures and software, the security aspects lead to considerable challenges. Given the requirements imposed by privacy and other legislation, many small and medium size enterprises consequently wonder whether cloud technology is really the best solution for them. This talk therefore aims at giving an overview of the most relevant technical, organizational and legal issues and points to some selected solutions for small and medium size enterprises.

2. Fighting Botnets with Cyber-Security Analytics: Dealing with Heterogeneous Cyber-Security Information in New Generation SIEMs
Beatriz Gallego-Nicasio Crespo (Atos Research & Innvoation, Spain), Alan Garwood (LSEC, Belgium)

Abstract: One of the cyber-threats with the highest impact nowadays, in terms of number of compromised systems and the impact they can have on the Internet at large, is commonly known as the botnet. In the ACDC (Advanced Cyber Defence Centre) project, partners from 14 European countries, including public administrations, private sector organizations and academia, are trying to achieve a sustainable victory over botnets. This paper presents how a new generation SIEM is being used in the ACDC project to leverage its scalability and enhanced analytic capabilities and produce advance cyber-intelligence from the heterogeneous and massive streams of data continuously produced in the cyber-security context, in combination with traditional security events and system logs. The paper describes a case study where this approach is being tested. In the case study, the SIEM has been adapted to cope, not only with traditional security events and system logs, but also with pre-analyzed information about cyber-threats and incidents reported by the tools of some of the ACDC partner organizations. The case study also tests the adoption of the standard XML-based format called STIX, developed by the Mitre Corporation in the USA, and its suitability as a common specification for exchanging cybersecurity information between a subset of ACDC tools, the Atos SL SIEM and the ACDC's centralized data clearing house (CCH).

3. Network Security Analysis Using Behavior History Graph
Mirko Sailio, Matti Mantere, Sami Noponen (VTT Technical Research Centre of Finland, Finland)

Abstract: Industrial control system networks are responsible for the operation of critically important functions of modern societies. In this paper we describe a highly distributable technique with low hardware requirements for mapping the typical network behavior of such stable networks. We propose that this technique is able to detect multiple wide ranging attack scenarios threatening these networks. We then proceed to test the techniques' hypothesized advantages using a industrial control system network of a real world experimental pilot factory. The results for this technique are promising, with the achievement of predicted 100% detection rate for both real and simulated behavior changes in the testing material.

12:30 – 14:00 Lunch

14:00 – 15:30 Parallel Sessions

ARES Short III – Software Security and Authentication / ARES Closing Session – 9th International Conference on Availability, Reliability and Security

Session Chair: Collin Mulliner, Northeastern University, United States & Edgar Weippl, SBA Research, Austria
Location: Lecture Hall E
Time: 14:00 – 15:30

1. Continuous and Non-intrusive Reauthentication of Web Sessions Based on Mouse Dynamics
Eric Medvet, Alberto Bartoli, Francesca Boem, Fabiano Tarlao (University of Trieste, Italy)

Abstract: We propose a system for continuous reauthentication of web users based on the observed mouse dynamics. Key feature of our proposal is that no specific software needs to be installed on client machines, which allows to easily integrate continuous reauthentication capabilities into the existing infrastructure of large organizations. We assess our proposal with real data from 24 users, collected during normal working activity for several working days. We obtain accuracy in the order of 97%, which is aligned with earlier proposals requiring instrumentation of client workstations for intercepting all mouse activity-quite a strong requirement for large organizations. Our proposal may constitute an effective layer for a defense-in-depth strategy in several key scenarios: web applications hosted in the cloud, where users authenticate with standard mechanisms, organizations which allow local users to access external web applications, and enterprise applications hosted in local servers or private cloud facilities.

2. Verifying Implementation of Security Design Patterns Using a Test Template
Masatoshi Yoshizawa, Takanori Kobashi, Hironori Washizaki, Yoshiaki Fukazawa (Waseda University, Japan), Takao Okubo (Institute of Information Security, Japan), Haruhiko Kaiya Kanagawa University, Japan), Nobukazu Yoshioka (National Institute of Informatics, Japan)

Abstract: Although security patterns contain security expert knowledge to support software developers, these patterns may be inappropriately applied because most developers are not security specialists, leading to threats and vulnerabilities. Here we propose a validation method for security design patterns in the implementation phase of software development. Our method creates a test template from a security design pattern, which consists of the "aspect test template" to observe the internal processing and the "test case template". Providing design information creates a test from the test template. Because a test template is recyclable, it can create easily a test, which can validate the security design patterns. As a case study, we applied our method to a web system. The result shows that our method can test repetition in the early stage of implementation, verify pattern applications, and assess whether vulnerabilities are resolved.

3. AES-SEC : Improving Software Obfuscation through Hardware-Assistance
Sebastian Schrittwieser (St. Pölten University of Applied Sciences, Austria), Stefan Katzenbeisser (TU Darmstadt, Germany), Georg Merzdovnik, Peter Kieseberg, Edgar Weippl (SBA Research, Austria)

Abstract: While the resilience of software-only code obfuscation remains unclear and ultimately depends only on available resources and patience of the attacker, hardware-based software protection approaches can provide a much higher level of protection against program analysis. Almost no systematic research has been done on the interplay between hardware and software based protection mechanism. In this paper, we propose modifications to Intel's AES-NI instruction set in order to make it suitable for application in software protection scenarios and demonstrate its integration into a control flow obfuscation scheme. Our novel approach provides strong hardware-software binding and restricts the attack context to pure dynamic analysis – two major limiting factors of reverse engineering – to delay a successful attack against a program.

ECTCM II – 2nd International Workshop on Emerging Cyberthreats and Countermeasures

Session Chair: Dieter Vymazal, University of Applied Sciences Upper Austria, Austria
Location: Lecture Hall B
Time: 14:00 – 15:30

1. Performance Measures of Behavior-Based Signatures: An Anti-malware Solution for Platforms with Limited Computing Resource
Kelly Hughes, Yanzhen Qu (Colorado Technical University, United States)

Abstract: The signature-based malware-detection method is the most popular one used in anti-malware software. However, given advanced malware capabilities, the database of traditional signature-based antimalware software is becoming bloated to support identification of every variant. The increase in signatures slows the detection process and, in some cases, exceeds the resource availability of the platforms that need it most. With the expansion of the smaller platforms with limited computing resources, such as some mobile devices and various types of sensor networks, including Internet-of-Things (IoT), anti-malware's capability needs to be refined to support these platforms. Behavior-based signatures might provide that much-needed reduction in the number of signatures found in a signature set while retaining the full spectrum of malware variants.

2. Network Security Monitoring in a Small-Scale Smart-Grid Laboratory

Matti Mantere, Sami Noponen, Pia Olli, Jarno Salonen (VTT Technical Research Centre of Finland, Finnland)

Abstract: Smart grids are the next generation of electrical grids, enabling the better management and leveling of power consumption by suppliers. Via the use of automatic meter reading, smart grid also provides better information to the end-users, making it possible to enhance their energy consumption and adapt it according to the current energy price, availability and other factors. As the grid becomes more and more reliant to ICT and communication networks, risks related to cybersecurity and privacy have to be taken into account. The link between automatic meters and the distribution operator has to be protected from security breaches that may lead to false billing and the transferred data has to be protected as it contains sensitive information about household and business behavior. In this article we present a limited state-of-the-art review as well as a network security monitoring setup for small-scale laboratory that is in essence a small scale smart grid environment. We discuss about the challenges and threats that are possible in the smart grid environment and the feasibility of using network security monitoring techniques that represent our work-in-progress research in this context.

3. Increasing the Resilience and Trustworthiness of OpenID Identity Providers for Future Networks and Services

Diego Kreutz (Universidade de Lisboa, Portugal), Eduardo Feitosa, Hugo Cunha (Universidade Federal do Amazonas, Brasil), Heiko Niedermayer, Holger Kinkelin (Technische Universität München, Germany)

Abstract: We introduce a set of tools and techniques for increasing the resilience and trustworthiness of identity providers (IdPs) based on OpenID. To this purpose we propose an architecture of specialized components capable of fulfilling the essential requirements for ensuring high availability, integrity and higher confidentiality guarantees for sensitive data and operations. Additionally, we also discuss how trusted components (e.g., TPMs, smart cards) can be used to provide remote attestation on the client and server side, i.e., how to measure the trustworthiness of the system. The proposed solution outperforms related work in different aspects, such as countermeasures for solving different security issues, throughput, and by tolerating arbitrary faults without compromising the system operations. We evaluate the system behavior under different circumstances, such as continuous faults and attacks. Furthermore, the first performance evaluations show that the system is capable of supporting environments with thousands of users.

RAMSS III – 2nd 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 C
Time: 14:00 – 15:30

1. Analysis of Algorithms for Computation of Direct Partial Logic Derivatives in Multiple-Valued Decision Diagrams

Jozef Kostolny, Miroslav Kvassay, Elena Zaitseva (University of Zilina, Slovakia)

Abstract: Reliability is a very important characteristic of many systems. However, there are some problems how to represent a complex system that contains a lot of different components. The problem of component variability can be solved by using Multi-State Systems (MSSs), which consists of components with different number of performance levels. The problem of large system dimension can be solved by using decision diagrams for system representation. However, new algorithms have to be developed for reliability analysis of MSSs represented by decision diagrams. A possible way is the extension of existing tools of reliability analysis on this representation of a MSS. Direct Partial Logic Derivatives (Direct Partial Logic Derivatives) are one of the tools that have been expanded on decision diagrams. Direct Partial Logic Derivatives can be used in reliability analysis to model the consequence of the component performance change on the system performance. Therefore, they can be used to find components that have the most influence on the system reliability. In some papers, there have been proposed algorithms that can be used to compute Direct Partial Logic Derivatives from decision diagrams. However, their computational

complexity has not been yet studied. In this paper, we summarize these algorithms and analyze their time complexity using some benchmarks that are often used to compare the complexity of algorithms designed for logic synthesis.

2. A Comparative Study of Control Charts for Zero-Inflated Binomial Processes
Athanasios C. Rakitzis (LUNAM University, France), Petros E. Maravelakis (University of Piraeus, Greece), Philippe C. Castagliola (LUNAM University, France)

Abstract: Zero-inflated probability models are recommended when there is an excessive number of zeros in count data. In the context of statistical process control, such cases arise in high-yield processes where the fraction of non-conforming units produced is very low. Other applications can be also found in the monitoring of health-related process, where it is of interest the monitoring of rare health-events like the number of congenital malformations or the rate of wound infections. In this work, we present one-sided and two-sided control charts that are suitable for the monitoring of changes in the parameters of a zero-inflated binomial process. We consider Shewhart-, EWMA- and CUSUM-type control charts, and we present aspects of their statistical design. Numerical comparisons between the different schemes are given as well.

3. Statistical Inference for Heavy-Tailed Distributions in Technical Systems
Alex Karagrigoriou (University of the Aegean, Greece), Ilia Vonta (National Technical University of Athens, Greece)

Abstract: In this work we explore the class of heavy-tailed distributions and discuss their significance in reliability engineering. At the same time we discuss measures of divergence which are extensively used in statistics in various fields. In this paper we rely on such measures to evaluate the residual and past lifetimes of events which are associated with the tail part of the distribution. More specifically, we propose a class of goodness of fit tests based on Csiszar's class of measures designed for heavy-tailed distributions.

4. On Sensitivity of Reliability Models to the Shape of Life and Repair Time Distributions
Vladimir Rykov (State University of Oil & Gas, Russia), Dmitry Efrosinin (Johannes Kepler University, Austria), Vladimir Vishnevsiy (Institute of Control Sciences, Russia)

Abstract: The sensitivity analysis of systems' characteristics to the shape of distributions is a very important task of reliability engineering of stochastic systems and networks. One of the earliest result concerning insensitivity of systems' characteristics to the shape of service time distribution was obtained in case of Erlang's formulas for loss queues with Poisson arrival stream, where steady-state distribution depends only on the mean service times. The paper deals with simple finite-source queueing models which completely fail if a source area becomes empty. The inter-arrival or service times are assumed to be generally distributed. It is shown that the steady-state probabilities of the systems with a buffer or with generally distributed inter-arrival times are sensitive to the shape of distributions but simultaneously the waiting time distributions have a weak sensitivity. It was observed that the sensitivity vanishes if the complete failure becomes a rare event. The results are compared with loss queues.

ARES-IND II – ARES Industrial Track

Session Chairs: Kari Jussila, Aalto University, Finland & Juhani Anttila, IAQ, Finland
Location: Lecture Hall D
Time: 14:00 – 15:30

Tutorial

Open Source Information Analysis

Gerhard Backfried (SAIL LABS Technology, Austria), Gerald Quirchmayr (University of Vienna, Austria)

Abstract: This tutorial will start with an overview of issues related to open source information analysis. It will then go deeper into the Sail Labs Media Mining System and the underlying technology. After discussing the architexture and functionality and giving some examples of current applications of the system, a case study on the use of the systems application in the context of the QuOIMA project will be presented.

15:30 – 16:00 Coffee Break

16:00 – 17:00 Plenary Session

Keynote

Location: Lecture Hall A
Time: 16:00 – 17:00

Change, Innovation, and Resilience in the DNS Ecosystem: a Verisign Labs Perspective

Allison Mankin (Verisign Labs, United States)

Abstract: Despite having marked the 30th anniversary in 2013, the Internet's Domain Name System (DNS) is in a period of great innovation, which applications are leveraging as the Internet evolves. In particular, with the emergence of DNS-enabled Authentication of Named Entities, or DANE, applications have new forms of access to global-scale security capabilities. This talk will analyze DNS innovation. One focus will be on modernized, specifically the extensible getdns application interface (getdnsapi.net) developed by Verisign Labs and Amsterdam-based NLNet Labs. Another focus will be on the emerging capabilities for privacy-enhanced access to DNS. In general, this keynote will present a long term view of the DNS Ecosystem, as seen from the research lab of Verisign.

17:00 – 23:00 Conference Dinner

Meeting point: University of Fribourg, in front of the building, 17.00 (shortly after the last session)
Departure busses: 17.15

Château de Gruyères

Thursday, 11 September 2014

08:00 – 18:00 Registration for all events

09:00 – 10:30 Parallel Sessions

IWSMA I – 2nd International Workshop on Security of Mobile Applications

Session Chair: Peter Kieseberg, SBA Research, Austria
Location: Lecture Hall B
Time: 09:00 – 10:30

1. A Trust Management Based Security Mechanism against Collusion Attacks in a MANET Environment
   Aida Ben Chehida Douss, Ryma Abassi, Sihem Guemara El Fatmi (University of Carthage, Tunisia)

   Abstract: MANETs (Mobile Ad hoc Networks) are self-organized networks with mobile and collaborating nodes without any pre-established infrastructure. Because of these characteristics, securing MANETs constitute a hard and challenging task. Consequently, new mechanisms may be of interest to secure such networks. To this end, we have found that trust management can be a support for MANET security. In fact, the reputation concept and the establishment of trustful relation between collaborating nodes can be meaningful to express security aspects in such environment. From there, we proposed in previous works a Mobility-based Clustering Algorithm (MCA) and a Trust management scheme for MCA (TMCA) to secure routing behaviors. MCA organizes nodes into clusters managed by a cluster-head (CH) and TMCA detects malicious routing behavior based on CHs direct observations and exchanged alerts. A delegation based process was also defined on TMCA and was called DTMCA. Although DTMCA meets security objectives, it may unfortunately be faced with various threats from malicious nodes: Several nodes can in fact collude in order to increase or decrease other reputation values to damage the QoS and even the MANET functioning. Our objective in this paper is then to secure DTMCA against collusion attacks. The mechanism proposed here is based on colluding nodes detection through cluster members behavior monitoring and by comparing this behavior with the received reputation value in the alert message. Detected colluder nodes are then discarded from further communication.

2. A Resource-Optimized Approach to Efficient Early Detection of Mobile Malware
   Jelena Milosevic, Andreas Dittrich, Alberto Ferrante, Miroslaw Malek (Università della Svizzera italiana, Switzerland)

   Abstract: With explosive growth in the number of mobile devices mobile malware is rapidly spreading, making security one of the key issues. Existing solutions, which are mainly based on binary signatures, are not very effective. The main contribution of this paper is a novel methodology to design and implement secure mobile devices by offering a resource-optimized method that combines efficient, light-weight malware detection on the mobile device with high precision detection methods on cloud servers. We focus on the early detection of behavioral patterns of malware families rather than the detection of malware binary signatures. Upon detection of an attack, an alarm is raised and the damage that can be caused by the detected malware type is estimated. Furthermore, the database with behavioral patterns is continuously updated, thus keeping a device resistant to new malware families.

3. An Improved Role-Based Access to Android Applications with JCHR
   Stefano Bistarelli (Università di Perugia, Italy), Gianpiero Costantino, Fabio Martinelli, Francesco Santini (Istituto di Informatica e Telematica, Italy)

   Abstract: In this paper we show how deductive and abductive reasoning in distributed authorisation can be efficiently ported to Android. Such logical-inference processes prove to be important tools due to the intrinsic autonomic-nature of these mobile devices. Both deduction and abduction are represented by using Constraint Handling Rules (CHR), a high-level declarative constraint programming-language, and implemented in JCHR (CHR embedded into Java). To represent credentials we elaborate on RTW, a weighted Role-based Trust-management family of languages: CHR programs are developed after such languages. In general, having weights associated with credentials leads to a more informative reasoning, for instance, access can be granted only if the total uncertainty is less than 20%.

SecATM I – International Workshop on Security in ATM and Other Critical Infrastructures

Session Chair: Martin Gilje Jaatun, SINTEF ICT, Norway
Location: Lecture Hall C
Time: 09:00 – 10:30

1. EMFASE—An Empirical Framework for Security Design and Economic Trade-off

Fabio Massacci, Federica Paci (University of Trento, Italy), Bjornar Solhaug (SINTEF, Norway), Alessandra Tedeschi (Deep Blue, Italy)

Abstract: Evaluation and validation methodologies are integral parts of Air Traffic Management (ATM). They are well understood for safety, environment and other Key Performance Areas, for which operational validation guidelines are well defined and widely used. In contrast, the effectiveness of risk assessment methods and practices for security, as well as their comparative evaluation is largely uncharted territory. There is limited information about the degree the practices and their corresponding activities provide security and whether or not they give return on investment. The "Empirical Framework for Security Design and Economics Trade-off" (EMFASE) project is investigating the above questions by applying different risk assessment methods on different application scenarios, such as the Remotely Operated Tower, and by evaluating them with respect to their performance, security impact, usability, and economy. In this paper we report the preliminary work carried out in EMFASE about the elicitation of a set of ATM relevant evaluation criteria for the comparison and assessment of the risk assessment methods under study and a brief description of the first set of experiments carried out.

2. The Social Acceptance of the Passivation of Misused Aircraft

Ana P.G. Martins (Deutsches Zentrum für Luft- und Raumfahrt e.V., Germany)

Abstract: One procedure under consideration to handle the threat posed by misused aircraft is passivation. In a passivated aircraft no more inputs from the cockpit are accepted and the aircraft safely lands in the nearest suitable airport without intervention from the pilots. Aircraft passivation is a procedure to be used in an emergency situation and would be handled as such by all stakeholders (air traffic control, airports, airlines, etc.). This paper attempts to address for the first time the social acceptability issues faced by passivation. It is assumed that the introduction of such a system in aircrafts will be a contentious issue expected to be met with strong resistance by pilots and the public in general. In this paper some of the technology under consideration is presented. This is followed by a discussion of the acceptance of similar technologies (unmanned aerial systems, driverless cars) before the social acceptance of passivation is discussed in more detail. Among the recommendations is the need to raise public awareness and familiarity with the technology. Pilots' acceptance is also seen as essential. Once society trusts the technology behind the system and the risks are deemed small enough, acceptance of passivation under some specific conditions should be possible.

3. Mathematical Modelling in Air Traffic Management Security

Denis Kolev (RNC Avionics Ltd, UK), Evgeniy Morozov (Wireless BT Ltd, UK)

Abstract: This paper addresses the potential of mathematical modelling in support of the classical security risk assessment and treatment approach. Classical security risk assessment and control selection is strongly based on expert judgment. Within the context of large scale system implementation in air traffic management, there is only a limited availability of resources during the system engineering phase. From that perspective an alternative approach based on system engineering artefacts is highly desirable. Furthermore, robust mathematical modelling can support in the verification of security risk mitigation decisions and provide a means to address trade-off decisions between a variety of different security controls. The research reported in this paper is based on game-theoretic concepts and graph theory. The security control selection problem is modelled as a multi-objective optimization problem. Two interwoven models are developed for addressing the security risk assessment problem of a system. The internal model describes the actual system and its parameters, while the external model is used to describe possible threat scenarios. These models and the modelling technique is instantiated for a simple airport context, and the essential building blocks of the method are discussed on this example. The work reported in this paper shows the general feasibility of a mathematically founded approach to security risk assessment in large-scale system engineering. The proposed modelling approach forms the basis for the development of a dynamic security risk management capability as part of a recently started European research project on global air traffic management security.

4. A Relative Cost-Benefit Approach for Evaluating Alternative Airport Security Policies

Woohyun Shim, Fabio Massacci (University of Trento, Italy), Alessandra Tedeschi, Alessandro Pollini (Deepblue S.r.l, Italy)

Abstract: While careful and prudent settings for airport security policies and strategies are more important than ever, most of them have been implemented as a direct result of terrorist activities rather than motivated by a proper assessment. Furthermore, even if many scholars have proposed ways to assess and evaluate alternative airport security policies particularly by using cost-benefit analysis, they have overlooked two important facets: parameter measurability and social

aspects of security policies. In this study, we develop a variant of cost-benefit analysis which we term "Relative Cost-Benefit Analysis" and illustrate how we can resolve these problems.

FARES I – 9th International Workshop on Frontiers in Availability, Reliability and Security

Session Chair: Edgar Weippl, SBA Research, Austria
Location: Lecture Hall D
Time: 09:00 – 10:30

1. A Usable Android Application Implementing Distributed Cryptography for Election Authorities

Stephan Neumann, Oksana Kulyk, Melanie Volkamer (Technische Universität Darmstadt, Germany)

Abstract: Although many electronic voting protocols have been proposed, their practical application faces various challenges. One of these challenges is, that these protocols require election authorities to perform complex tasks like generating keys in a distributed manner and decrypting votes in a distributed and verifiable manner. Although corresponding key generation and decryption protocols exist, they are not used in real-world elections for several reasons: The few existing implementations of these protocols and their corresponding interfaces are not designed for people with non technical background and thus not suitable for use by most election authorities. In addition, it is difficult to explain the security model of the protocols, but legal provisions generally require transparency. We implemented a smartphone application for election authorities featuring distributed key generation and verifiable distributed decryption of votes. In addition, we prepared education material throughout based on formulated metaphors for election authorities in order to explain the security of the application. We evaluated the usability of the application and understanding of the underlying security model, concluding that the application is usable for non-experts in computer science. While the participants were able to carry out the tasks, it became clear, that they did not have a clear understanding of the underlying security model, despite having viewed our educational material. We suggest improvements to this material as future work.

2. Complete SIP Message Obfuscation: PrivaSIP over Tor

Georgios Karopoulos (Joint Research Centre, Italy), Alexandros Fakis, Georgios Kambourakis (University of the Aegean, Greece)

Abstract: Anonymity on SIP signaling can be achieved either by the construction of a lower level tunnel (via the use of SSL or IPSec protocols) or by employing a custom-tailored solution. Unfortunately, the former category of solutions present significant impediments including the requirement for a PKI and the hop-by-hop fashioned protection, while the latter only concentrate on the application layer, thus neglecting sensitive information leaking from lower layers. To remediate this problem, in the context of this paper, we employ the well-known Tor anonymity system to achieve complete SIP traffic obfuscation from an attacker's standpoint. Specifically, we capitalize on Tor for preserving anonymity on network links that are considered mostly untrusted, i.e., those among SIP proxies and the one between the last proxy in the chain and the callee. We also, combine this Tor-powered solution with PrivaSIP to achieve an even greater level of protection. By employing PrivaSIP we assure that: (a) the first hop in the path (i.e., between the caller and the outbound proxy) affords anonymity, (b) the callee does not know the real identity of the caller, and (c) no real identities of both the caller and the callee are stored in log files. We also evaluate this scheme in terms of performance and show that even in the worst case, the latency introduced is not so high as it might be expected due to the use of Tor.

3. Privacy Preservation in Location-Based Mobile Applications: Research Directions

Asma Patel, Esther Palomar (Birmingham City University, UK)

Abstract: Proliferation of mobile devices equipped with position sensors has made Location-based Service (LBS) increasingly popular. These mobile devices send user's actual location information to the third party location servers, which compile and, in some cases, share with other service providers. As a result, users aware of the privacy implications feel continuously tracked. Effective and, even more important, socially-accepted privacy enhancing technologies for these services have recently received a lot of attention in academia and industry. This paper presents an overview of the privacy preserving techniques currently applied by LBS applications. It classifies these techniques into a classification model consisting of three layers. Thus, a brief description of all the protocols, mechanisms and interfaces covering from the application layer to the network layer are presented, also providing a comparative analysis of current privacy-aware location solutions. To guide future research, a new perspective of the literature findings is proposed and research questions, methods and implications are discussed. Novel to related work, our classification embraces a holistic picture of approaching privacy-aware mobile LBS.

4. Challenges of Composing XACML Policies

Bernard Stepien (University of Ottawa, Canada), Amy Felty (Dalhousie University, Canada), Stan Matwin (Polish Academy of Sciences, Poland)

Abstract: XACML (extensible Access Control Mark-up Language) is a declarative access control policy language that has unique language constructs for factoring out access control logic. These constructs make the specification of access control requirements more compact than decision trees, which can be considered the most natural way to specify access control logic. However, many publications report that performance of XACML policy decision point (PDP) engines is greatly affected by the structure of policy sets. In this paper we first explore the causes of potential inefficiencies of XACML policies, and then propose a procedure to re-structure policy sets vertically by modifying the distribution of access control logic among different configurations of structural elements, in order to remove much of this inefficiency. This is in contrast to horizontal re-ordering of constant structural elements. Our procedure can be applied regardless of the complexity and structure of the original policy set. We also compare the performance of policy sets that take advantage of the expressive power of XACML targets to decision trees.

10:30 – 10:45 Coffee Break

10:45 – 12:15 Parallel Sessions

IWSMA II – 2nd International Workshop on Security of Mobile Applications

Session Chair: Peter Kieseberg, SBA Research, Austria
Location: Lecture Hall B
Time: 10:45 – 12:15

1. Qualified Electronic Signature via SIM Card Using JavaCard 3 Connected Edition Platform
Jakub Breier (Nanyang Technological University, Singapore), Adam Pomothy (Slovak University of Technology, Slovakia)

Abstract: Digital signature is one of the most common ways of determining the origin of a document in a digital way. To ensure authenticity, integrity and non-repudiation when such signatures are used, many countries have their standards and regulations. In EU, a signature that complies with those regulations is called 'Qualified Electronic Signature' (QES). There are many QES solutions using dedicated smart cards or security tokens and few of them that use SIM cards as a signature creation device. These SIM-based solutions usually use a third party to perform a signature, such as mobile service operator and operate as a hybrid solutions. Hence, a cooperative connection between a mobile device and a SIM card is needed. In this paper we propose a solution based on the Java Card 3.0 Connected Edition platform that operate fulfills following conditions: it is a mobile service operator-independent and mobile phone operating system-independent. The first condition is achieved by performing all the operations directly on a SIM card and the second condition is satisfied by avoiding the application running on a mobile phone operating system. Instead, we propose a web based application to perform the necessary verification methods on the SIM card. So this proposed application can be accessed via mobile phone web browser. Of course, our solution satisfies the Common Criteria standard requirements for the EAL 4 level.

2. Panel Discussion: Future Topics in Mobile Security

SecATM II – International Workshop on Security in ATM and Other Critical Infrastructures

Session Chair: John Hird, EUROCONTROL, Belgium
Location: Lecture Hall C
Time: 10:45 – 12:15

1. Design-In Security for Air Traffic Control
Martin Hawley, Karol Gotz (Winsland Ltd, UK), John Hird (EUROCONTROL, Belgium), Chris Machin (Aztech BVBA, Belgium)

Abstract: Under the SESAR Programme, the European Air Traffic Management (ATM) industry has adopted an approach of 'design-in security' by applying security assessment from the beginning of the development lifecycle. This has necessitated a convergence of different approaches to security assessment from the different partners. A number of challenges have been apparent in developing both the method to be used and then executing it in a synchronised way with the rest of the programme. This paper highlights the issues raised in developing the methodology from the perspective of the security experts working within the programme.

2. Learn to SWIM
Matias Krempel (Deutsche Flugsicherung, Germany), Martin Gilje Jaatun (SINTEF ICT, Norway)

Abstract: This paper is meant to provide an overview over SWIM and its context from a security point of view. Rather than describing everything in detail it refers to the relevant SJU deliverables where possible and tries to provide the "glue" between the different pieces of information.

3. Security Situation Management: Towards Developing a Time-Critical Decision Making Capability for SESAR

Rainer Koelle (Lancaster University, UK)

Abstract: This paper addresses dynamic security management in air navigation as a distributed collaborative agent problem and identifies a modelling approach for the implementation of a situation management capability in ATM. The traditional focus of aviation security is on preventive security aircraft and airport measures. When it comes to air navigation, the concept and scope of security is evolving. This goes in hand with the understanding and the implementation of security requirements and capabilities in new system developments. Security incident management is a research gap in the on-going transformation programmes SESAR and NextGen. This paper proposes an engineering concept for the development of a dynamic security incident management capability for the future ATM system context (e.g. SESAR) based on the findings of previous research and the associated development of a situation management framework model. The results obtained demonstrate the general applicability of the situation management modelling approach to the design and validation of such a dynamic security management capability as part of the recently launched EU project on Global ATM Security Management (GAMMA). A set of principal research requirements for this project is derived addressing the emerging need for security incident management capabilities in general, e.g. self-protection / resilience, emergency response. The proposed modelling approach and the anticipated GAMMA deliverables offer an opportunity to address the research gap of SESAR and provide novel technological solutions to the envisaged European Security Operation Centre recently proposed under the umbrella of the centralised services for European ATM.

FARES II – 9th International Workshop on Frontiers in Availability, Reliability and Security

Session Chair: Edgar Weippl, SBA Research, Austria
Location: Lecture Hall D
Time: 10:45 – 12:15

1. EmailCloak: A Practical and Flexible Approach to Improve Email Privacy

Italo Dacosta, Andreas Put, Bart De Decker (KU Leuven, Belgium)

Abstract: Millions of users rely on email providers to manage and store their personal communications. This vast amount of private information, however, is often misused not only by adversaries, but also by the providers themselves. End-to-end email encryption is considered the most robust defense against this threat, however, its many requirements make this approach impractical for protecting everyday emails. In this paper, we present Email Cloak, an email alias service with public key encryption capabilities. Email Cloak relaxes email encryption requirements by relying on a privacy-respecting third-party. Emails sent and received by the user are automatically encrypted with her public key by Email Cloak before being forwarded to, and stored by her email provider. This approach, while seemingly straightforward, offers multiple benefits: simplified key management, selective and automatic encryption, advanced deployment options and transparency towards other parties. Moreover, our experimental evaluation shows that the overhead introduced by Email Cloak is adequate for email communications. We have also made our implementation publicly available. In doing so, we deliver a practical and flexible tool that provides privacy-concerned users with greater control over their stored emails.

2. Quality Matters: Systematizing Quality Deficiencies in the Documentation of Business Security Requirements

Christian Sillaber, Ruth Breu (University of Innsbruck, Austria)

Abstract: The ever increasing need for businesses to ensure compliance with various laws and regulations as well as internal and external policies increasingly requires businesses to manage a plethora of documentation on different business security requirements. However, business security requirement documentation often suffers from quality deficiencies and faults due to negligence, inconsistencies, conflicts or unclear responsibilities in globally distributed businesses. A key factor to successfully address these deficiencies and to support continuous quality improvement of business security requirements documentation is to know exactly what faults to look for in a structured manner. Based on a think-aloud study, we identify and categorize specific quality deficiencies that can be found in the documentation of business security requirements and classify the faults that might cause them. We conclude by proposing a taxonomy that covers the specification, interaction, and life-cycle faults that are at the root of observable failures in the documentation of business security requirements.

3. Evaluating the Effectiveness of ISO 27001: 2013 Based on Annex A
Bahareh Shojaie, Hannes Federrath (University of Hamburg, Germany), Iman Saberi (Germany)

Abstract: The part of the management system of an organization dealing with information security is called Information Security Management System (ISMS). The most adopted ISMS standard is ISO 27001:2005. The 2005 version of the standard has been updated in 2013 to provide more clarity and more freedom in implementation, based on practical experiences. This paper compares ISO 27001:2005 and the updated 2013 standard, based on Annex A controls. We classify the controls into five categories of data, hardware, software, people and network. All of the controls defined in Annex A, regardless of their objectives, can easily be allocated to at least one of these categories. Classifying the controls to known categories offers an integrated view of the updated standard and presents a suitable guide for evaluating the performance and efficiency of the updated standard.

4. A Proposal for a Unified Identity Card for Use in an Academic Federation Environment
Felipe Coral Sasso, Ricardo Alexandre Reinaldo de Moraes, Jean Everson Martina (Universidade Federal de Santa Catarina, Brasil)

Abstract: XACML (extensible Access Control Mark-up Language) is a declarative access control policy language that has unique language constructs for factoring out access control logic. These constructs make the specification of access control requirements more compact than decision trees, which can be considered the most natural way to specify access control logic. However, many publications report that performance of XACML policy decision point (PDP) engines is greatly affected by the structure of policy sets. In this paper we first explore the causes of potential inefficiencies of XACML policies, and then propose a procedure to re-structure policy sets vertically by modifying the distribution of access control logic among different configurations of structural elements, in order to remove much of this inefficiency. This is in contrast to horizontal re-ordering of constant structural elements. Our procedure can be applied regardless of the complexity and structure of the original policy set. We also compare the performance of policy sets that take advantage of the expressive power of XACML targets to decision trees.

12:15 – 13:00 Lunch

13:00 – 17:00 Plenary Session

(ISC)^2 SecureFribourg (open for all participants)

What do we really know about our Security Position?

Consumerisation, the cloud enabled and socially networked enterprise… with so much business occurring outside of the carefully planned IT strategy, it is time to take stock. How can we continue to make decisions that are informed, fast, and incisive?

The conference approaches a wide range of issues from the monitoring and control of free-flowing data that often is highly sensitive or subject to stringent regulation, to the new security threats, vulnerabilities and uncertainties that are occurring as new IT trends take hold.

You will gain the insight you need to get to grips with your current security stance and move forward with confidence in the ability to maintain a clean corporate reputation. Sessions offer analysis of both current and developing challenges: in data security; the threat landscape; growing concern over state sponsored attack; the changing enterprise and more, with a focus on delivering lessons learned from those who have experienced cyber-attack.

12.30 – 13.00
Registration & Welcome Coffee

13.00 – 13.05
Welcome Note
Edgar Weippl, Chairman, ARES

13.05 – 13.15
Chairman's Opening Remarks
Adrian Davis
Managing Director, (ISC)^2 EMEA

13.15 – 14.00
Keynote Address: Security in Electronic Voting
Prof. Dr. Ulrich Ultes-Nitsche
Department of Informatics, University of Fribourg

14.00 – 14.30
S1: CISO 2015-2020 : Expecting a new job?
Bruno Kerouanton
CISO - Republic and Canton of Jura

14.30 – 15.00
S2: Where's the elder lemon when you need him? *Gaps in the supply chain for security practitioners & professionals in the future labour market*
Richard Nealon
Member of the (ISC)^2 Board of Directors

15.00 – 15.30
Afternoon Refreshments

15.30 – 15.40
(ISC)^2 Chapter Switzerland / (ISC)^2 Austrian Chapter Update
tbc, (ISC)^2 Swiss Chapter
Gernot Goluch, President, (ISC)^2 Austrian Chapter

15.40 – 15.50
ISC)^2 Safe and Secure Online Programme - Introduction and Updates
Richard Lane
Foundation Committee Member, (ISC)^2
Head of Information Security, WIPO

15.50 – 16.20
S3: The Known Unknowns in Cyber Security & Outbidding Cyber Criminals
Stefan Frei

Lecturer for Networking Security, Dozent ETH

16.20 – 17.00
Panel: "Today's hot topics and burning questions"
Moderator: Adrian Davis
Speakers: Prof. Dr. Ulrich Ultes-Nitsche, Bruno Kerouanton, Richard Nealon and Stefan Frei

17:00 – 18:00 Evening Reception (open for all participants)

Friday, 12 September 2014

09:00 – 14:30 Excursion / Sightseeing Tour

On Friday, 12th of September 2014, we have organized two different excursions. The tour / guides / entrance fee and the transport is free of charge for you, lunch is not included. Please note that you can only attend one of the following two excursions:

Option 1:

Walking Tour – Bern

"UNESCO Stroll through the Old Town"

On this stroll through Bern's Old Town, you'll learn more about the city's 800-year history. You'll marvel at the late Gothic Cathedral (Münster) with its stunning portal and its depiction of the Last Judgment.

The Clock Tower (Zytglogge), our oldest city gate dating to the 13th century, awaits you and offers a fascinating show on the hour. And who knows, you might even meet up with a member of the Federal Council in front of the Parliament building. On rainy days, our arcades will provide shelter.

Come along and discover the Swiss capital and UNESCO World Heritage Site at its beautiful best.

Meeting point: University of Fribourg, in front of the building, 09.00 (please be punctual!)
Departure Fribourg: University of Fribourg, 09.15
Walking City Tour Bern: 10.00 – 12.00
Free time (e.g. for lunch): 12.00 – 13.30
Arrival Fribourg: 14.15 / 14.30

Please note: The costs for the city tour as well as the transport to and from Bern will be covered by the ARES Conference. Participants need to sign up for the tour. Lunch is not included, a restaurant will be recommended.

Option 2:

Hiking in Gantrisch, a natural preserve – Gäggersteg wood path

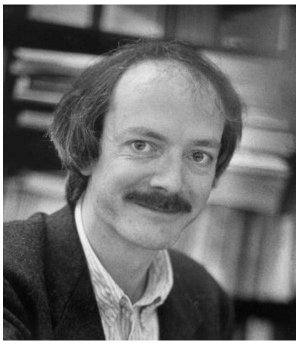
In 1999 the cyclone Lothar destroyed large areas of the forest between Schwarzenbühl and Ottenleue. High above the ground, on wooden footbridges, you can experience the forest's recreation. On our way to the alpine restaurant Selitaal you can enjoy the breathtaking view on the Gantrisch mountain chain.

The guided tour will take about 2,5 hours. After lunch at the panoramic restaurant Selitaal the bus will pick us up. Although you don't need a certain level of physical fitness or hiking skills to enjoy the tour, please make sure to wear appropriate shoes (trekking shoes or ones with good sole profile).

Meeting point: University of Fribourg, in front of the building, 08.45 (please be punctual!)
Departure Fribourg: University of Fribourg, 09.00
Hiking tour: 10.00 – 12.30
Lunch: 12.30 – 13.30
Arrival Fribourg: 14.30 / 14.45

Please note: The costs for the guided hiking tour as well as the transport to and from Gantrisch will be covered by the ARES Conference. Participants need to sign up for the tour. Lunch at the restaurant Selital is not included.

Keynotes



Bart Preneel
Katholieke Universiteit Leuven, Belgium

Keynote: Mass surveillance and cryptology

Tuesday, September 9, 2014 (09.00 – 10.30) Lecture Hall A

Abstract: *The implications of the Snowden revelations have brought to the light interesting research challenges in the area of information security and cryptology. It has become clear that nation states do not limit themselves to large scale passive eavesdropping, but have moved towards sophisticated traffic analysis techniques and active attacks on networks and end systems. Moreover, in the next years one can expect a deployment of ever more sophisticated techniques by a growing number of actors. The awareness of these threats has resulted in an increased interest in the implementation of cryptographic mechanisms; a key question is whether the current cryptographic mechanisms are adequate to protect against these advanced opponents. We will also discuss which areas pose the largest challenges and which defenses have the best chances to be effective.*

Prof. Bart Preneel is a full professor at the KU Leuven; he heads the COSIC research group, which is a member of the iMinds Security Department. He was visiting professor at five universities in Europe. He has authored more than 400 scientific publications and is inventor of 4 patents. His main research interests are cryptography, information security and privacy. Bart Preneel has coordinated the Network of Excellence ECRYPT, has served as panel member and chair for the European Research Council and has been president of the IACR (International Association for Cryptologic Research). He is a member of the Permanent Stakeholders group of ENISA (European Network and Information Security Agency) and of the Academia Europaea. He has been invited as speaker at more than 90 conferences in 40 countries. In 2014 he received the RSA Award for Excellence in the Field of Mathematics.

Volkmar Lotz
SAP Research, Germany

Keynote: Monitoring Threats and Vulnerabilities in Complex IT Landscapes

Wednesday, September 10, 2014 (09.00 – 10.30) Lecture Hall A

Abstract: *Even when applying current best practices and technologies to secure software and IT landscapes, it would be inappropriate to assume that there are no remaining vulnerabilities and that there will be no attempts to exploit them. Hence, complementing security technology and management with means to detect and monitor vulnerabilities and attacks is an essential element in a comprehensive security strategy. In this talk, we investigate into two major challenges that monitoring solutions need to address in industrial-scale business application environments: the large amount of data that need to be processed to be able to, for instance, detect complex attacks spanning a number of components and layers, and the small amount of time that is available to react to, for instance, the discovery of zero-day exploits. We sketch a solution that exploits advanced in-memory database technology and an event stream processer to enable threat detection in real time over billions of events.*

We present a second solution that addresses the prolongation of the time window to react to the publication of vulnerabilities in third party components used by an application. It has turned out that potential vulnerabilities are announced and discussed much earlier in social media than in the official channels like vendor sites or vulnerability registries. Monitoring and analyzing such media leads to a significant gain in response time.

Volkmar Lotz has more than 25 years experience in industrial research on Security and Software Engineering. He is heading SAP's Product Security Research, a group of 35+ researchers investigating into applied research and innovative security solutions for modern software platforms, networked enterprises and cloud-based applications, covering the whole development and product life cycle. The group defines and executes SAP's security research agenda in alignment with SAP's business strategy and global research trends. Volkmar's current research interests include Service Security, Data-centric Security, Security Engineering, Formal Methods and Compliance. Volkmar has published numerous scientific papers in his area of interest and is regularly serving on Programme Committees of internationally renowned conferences. He has been supervising various European projects, including large-scale integrated projects. Volkmar holds a diploma in Computer Science from the University of Kaiserslautern.

Allison Mankin
Verisign Labs, United States

Keynote: Change, Innovation, and Resilience in the DNS Ecosystem: a Verisign Labs Perspective

Wednesday, September 10, 2014 (16.00 – 17.00) Lecture Hall A

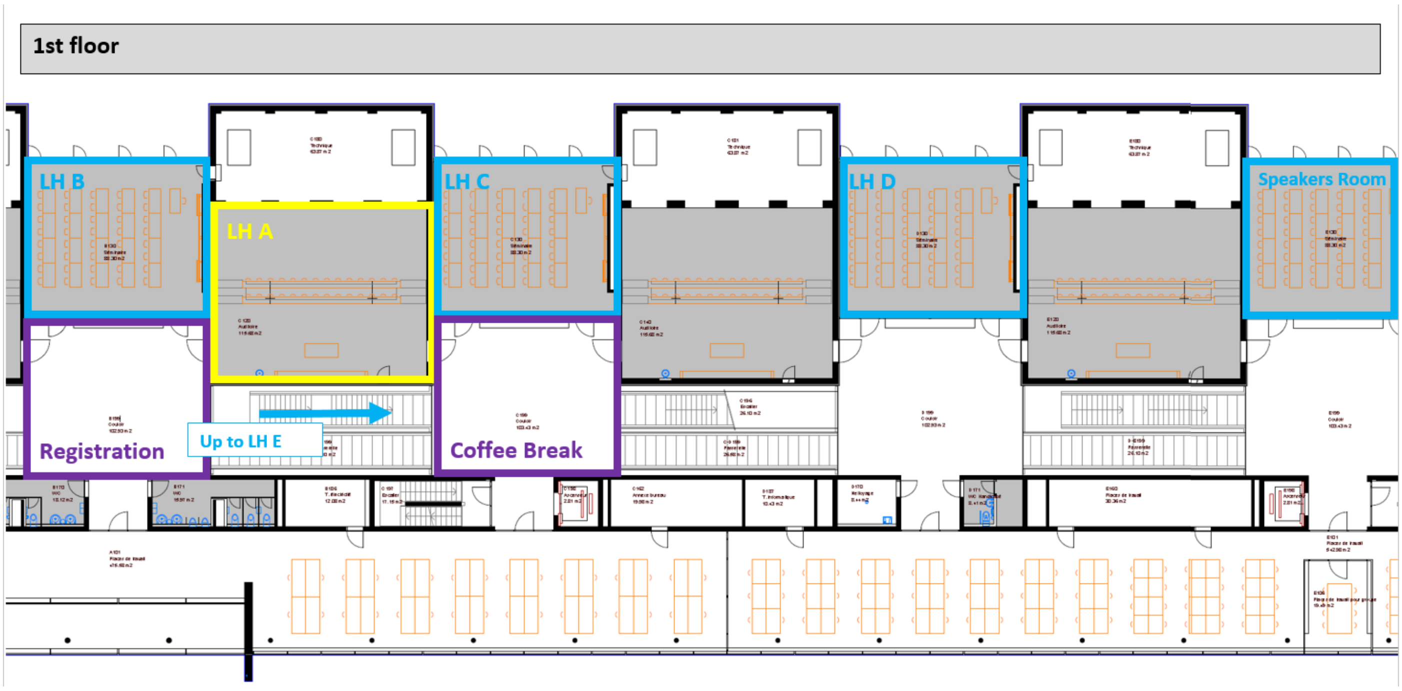
Abstract: *Despite having marked the 30th anniversary in 2013, the Internet's Domain Name System (DNS) is in a period of great innovation, which applications are leveraging as the Internet evolves. In particular, with the emergence of DNS-enabled Authentication of Named Entities, or DANE, applications have new forms of access to global-scale security capabilities. This talk will analyze DNS innovation. One focus will be on modernized, specifically the extensible getdns application interface (getdnsapi.net) developed by Verisign Labs and Amsterdam-based NLNet Labs. Another focus will be on the emerging capabilities for privacy-enhanced access to DNS. In general, this keynote will present a long term view of the DNS Ecosystem, as seen from the research lab of Verisign.*

Allison Mankin is the Director of Verisign Labs, a research organization focusing on medium- to long-term evolution, measurement and security of Internet infrastructure, especially DNS. She has been active in Internet research and engineering for over 25 years, including having served at the Internet Engineering Task Force as an area director for 10 of those years. She is best known for having co-led the IPng Selection Process at IETF (long ago). Her more recent work has been primarily in the areas of DNS, TCP, and their security.

Floor plans

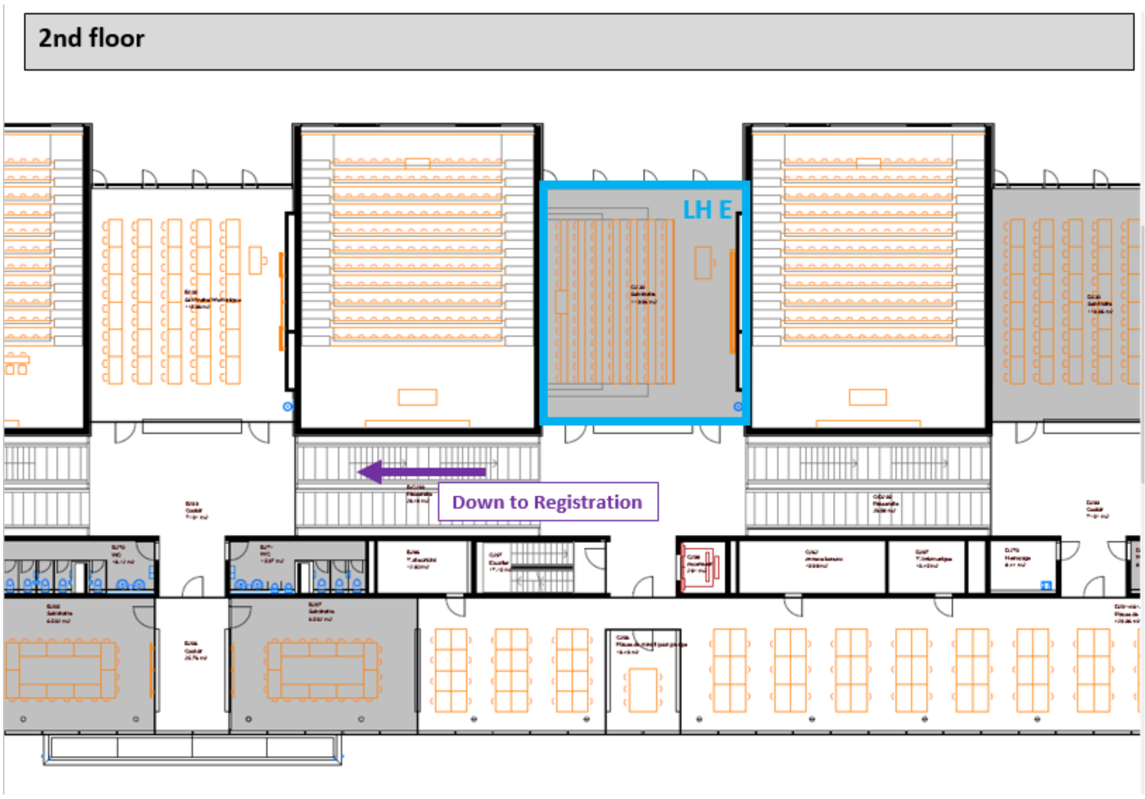
1st floor:

Registration, coffee break, speakers room and lecture halls A, B, C and D can be found on the 1st floor of the University building.



2nd floor:

Lecture Hall E can be found on the 2nd floor of the University building.



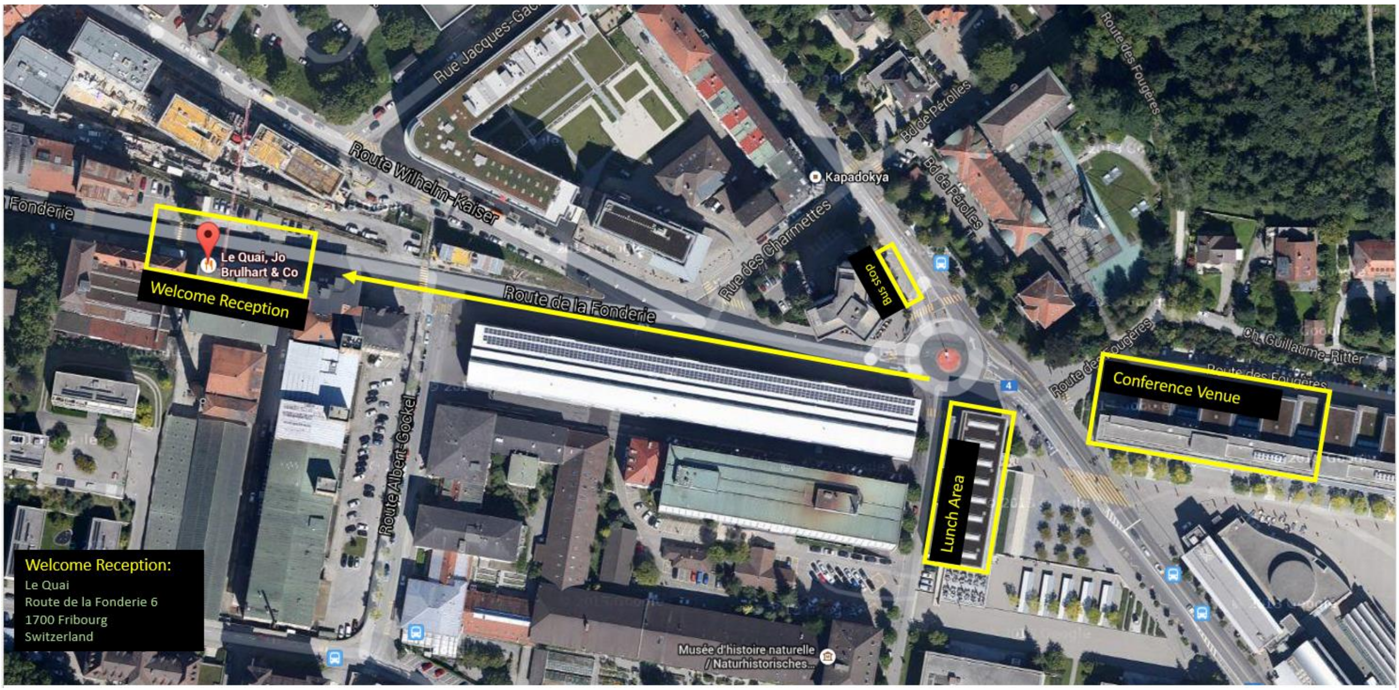
Social Events

Welcome Reception – Monday, 08th September 2014

The Welcome Reception will take place shortly after the last session in the bar / restaurant "Le Quai" next to the University. The former industry hall provides a special and charming atmosphere.

Address:

Le Quai
Route de la Fonderie 6
1700 Fribourg
Switzerland



Sightseeing Tour Fribourg – Tuesday, 09th September 2014

Explore Fribourg by Tiny Train

Spend an hour weaving your way through the picturesque spots of the town of Fribourg and immerse yourself in the medieval atmosphere of the Old Town with this guided tour.

Meeting point: University of Fribourg, in front of the building, 17.30 (shortly after the last session)
Departure: 17.45
Tour end: 18.45 / 19.00 at Grand-Places, Fribourg (city center)

Conference Dinner – Wednesday, 10th September 2014

The Conference Dinner will take place in Gruyères, which is located at the foot of the Pre-Alps, about half an hour from Fribourg. You will be enchanted by the charm and picturesque architecture of the medieval town of Gruyères. The town has given its name to the area and to its delicious cheese.

Meeting point: University of Fribourg, in front of the building, 17.00 (shortly after the last session)
Departure: Busses will depart at 17.15 from the University
Back in Fribourg: 23.00

Excursions – Friday, 12th September 2014

On Friday, 12th of September 2014, we have organized two different excursions. The tour / guides / entrance fee and the transport is free of charge for you, lunch is not included. Please note that you can only attend one of the following two excursions:

Option 1:

Walking Tour – Bern

“UNESCO Stroll through the Old Town”

On this stroll through Bern’s Old Town, you’ll learn more about the city‘s 800-year history. You’ll marvel at the late Gothic Cathedral (Münster) with its stunning portal and its depiction of the Last Judgment.

The Clock Tower (Zytglogge), our oldest city gate dating to the 13th century, awaits you and offers a fascinating show on the hour. And who knows, you might even meet up with a member of the Federal Council in front of the Parliament building. On rainy days, our arcades will provide shelter.

Come along and discover the Swiss capital and UNESCO World Heritage Site at its beautiful best.

Meeting point: University of Fribourg, in front of the building, 09.00 (please be punctual!)
Departure Fribourg: University of Fribourg, 09.15
Walking City Tour Bern: 10.00 – 12.00
Free time (e.g. for lunch): 12.00 – 13.30
Arrival Fribourg: 14.15 / 14.30

Please note: The costs for the city tour as well as the transport to and from Bern will be covered by the ARES Conference. Participants need to sign up for the tour. Lunch is not included, a restaurant will be recommended.

Option 2:

Hiking in Gantrisch, a natural preserve – Gäggersteg wood path

In 1999 the cyclone Lothar destroyed large areas of the forest between Schwarzenbühl and Ottenleue. High above the ground, on wooden footbridges, you can experience the forest's recreation. On our way to the alpine restaurant Selitaal you can enjoy the breathtaking view on the Gantrisch mountain chain.

The guided tour will take about 2,5 hours. After lunch at the panoramic restaurant Selitaal the bus will pick us up. Although you don't need a certain level of physical fitness or hiking skills to enjoy the tour, please make sure to wear appropriate shoes (trekking shoes or ones with good sole profile).

Meeting point: University of Fribourg, in front of the building, 08.45 (please be punctual!)
Departure Fribourg: University of Fribourg, 09.00
Hiking tour: 10.00 – 12.30
Lunch: 12.30 – 13.30
Arrival Fribourg: 14.30 / 14.45

Please note: The costs for the guided hiking tour as well as the transport to and from Gantrisch will be covered by the ARES Conference. Participants need to sign up for the tour. Lunch at the restaurant Selital is not included.

We are looking forward to meeting you there!

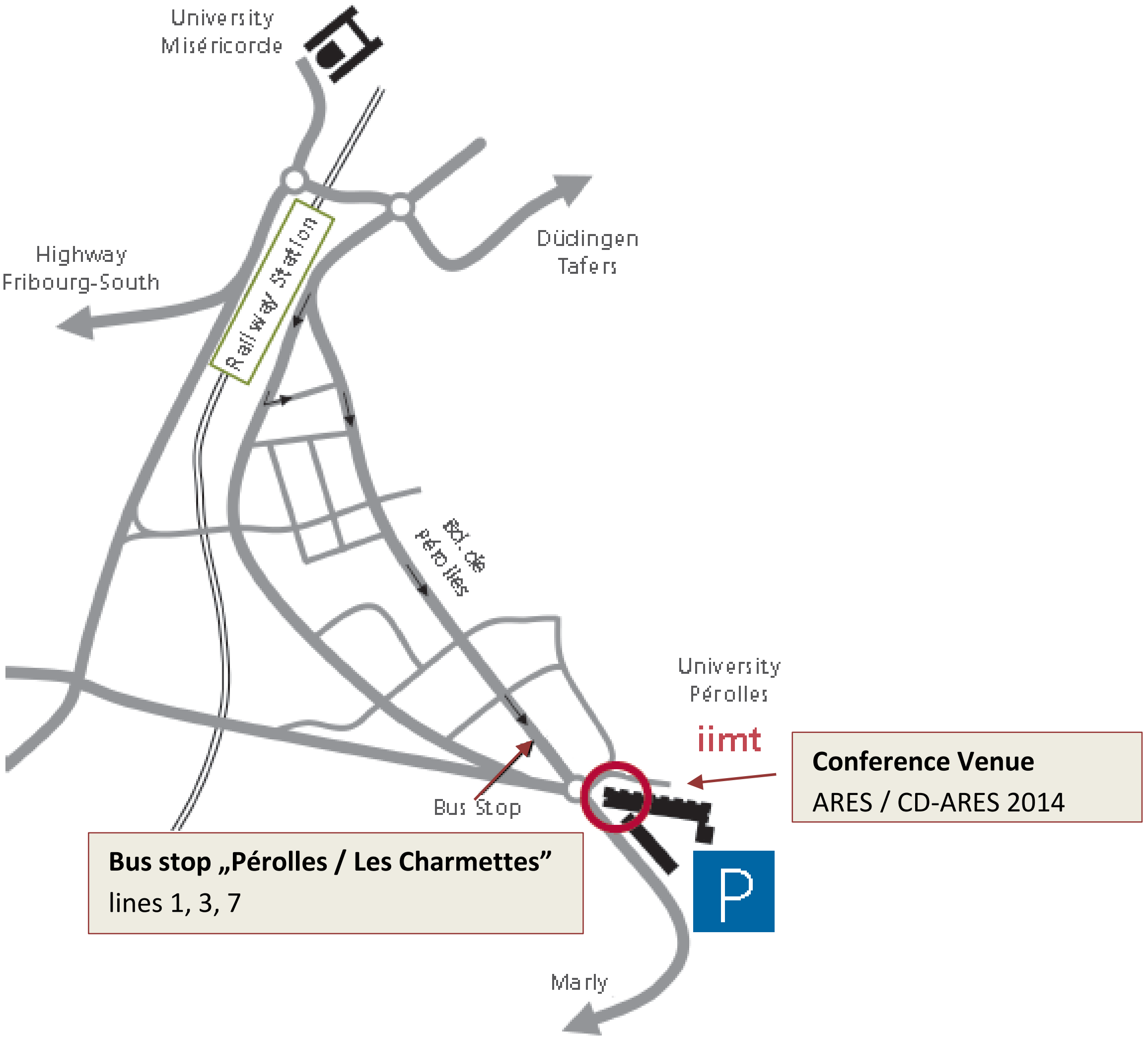
How to get to the Conference Venue (University of Fribourg)

Address of ARES 2014 Conference

University of Fribourg - University / Site Pérolles
Boulevard de Pérolles 90
1700 Fribourg
Switzerland

The University of Fribourg has more than one University buildings, so please make sure that you arrive at the right place, which is “Site Pérolles”.

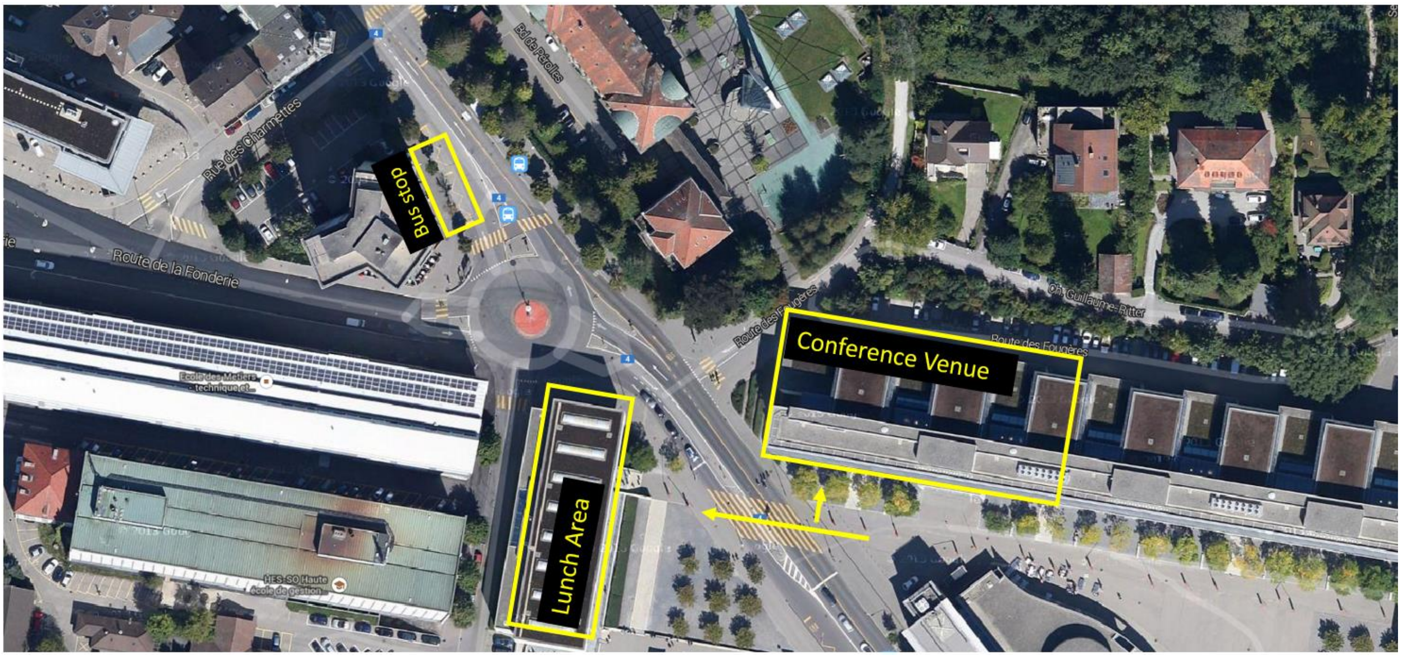
Take the bus to the University, the lines 1 (direction “Marly”) or 3 (direction "Pérolles") and 7 (direction "Cliniques") will get you there. All three lines stop at the main station. The bus stop in front of the University is called „Pérolles / Les Charmettes”.

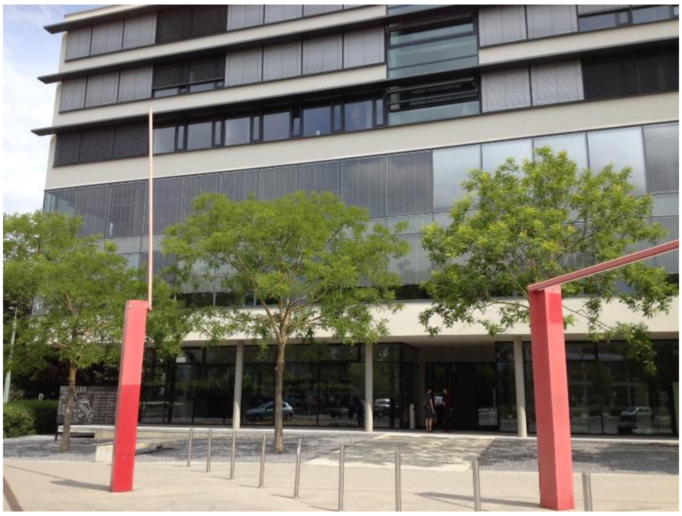


Conference Venue
ARES / CD-ARES 2014

Bus stop „Pérolles / Les Charmettes”
lines 1, 3, 7

Arriving at the University



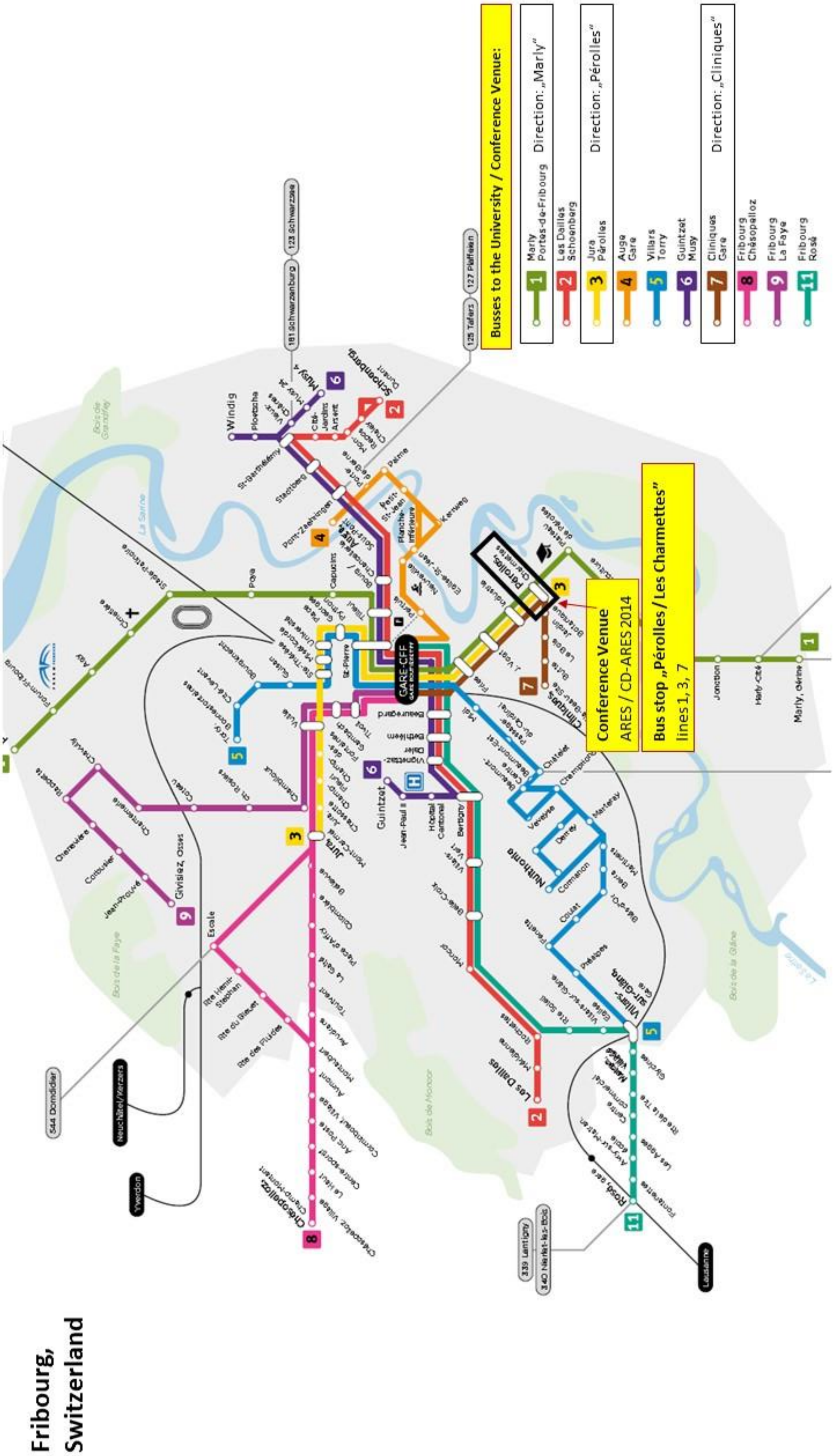


Take the first door of the University to enter the building.

The registration can be found on the 1st floor of the University building.

To get to the lunch area, cross the street.

Public Transport Fribourg



Busses to the University / Conference Venue:

1 Marly Portes-de-Fribourg Direction: „Marly“

2 Les Dailles Schoenberg

3 Jura Pérolles Direction: „Pérolles“

4 Auge Gare

5 Villars Torry

6 Guintzet Musy

7 Cliniques Gare Direction: „Cliniques“

8 Fribourg Chésopelloz

9 Fribourg La Faye

11 Fribourg Rosé

Conference Venue
ARES / CD-ARES 2014

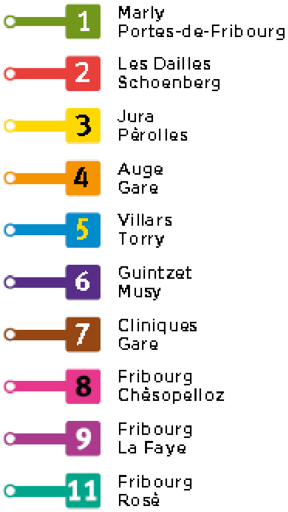
Bus stop „Pérolles/Les Charmettes“
lines 1, 3, 7

Fribourg,
Switzerland

Public Transport Tickets

The urban network in Fribourg

There are ten bus lines operating in Fribourg as well as a funicular railway, which links the lower part of the town to the city center.



Single Frimobil ticket

A single Frimobil ticket will allow you to travel freely in the zones you select. The period for which the ticket is valid and its price depend on the number of zones for which it is valid and are all shown on the ticket itself.

Ordinary single Frimobil tickets are available at full fare and reduced fares for journeys in second or first class. They can be bought from TPF ticket offices and ticket machines.

One-day Frimobil ticket

To make unlimited journeys in the zones you select, buy a one-day Frimobil ticket. It will allow unrestricted travel within those zones on the day of purchase until the end of services. The fare varies according to the number of zones you select and is shown on the ticket. With effect from three zones, a one day ticket costs the same as two single tickets for the same zones.

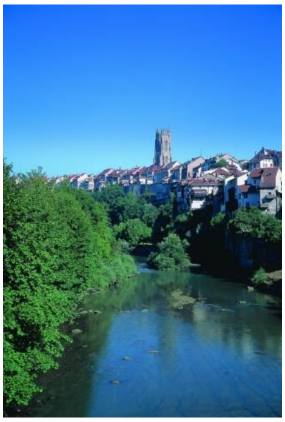
One-day Frimobil tickets are available at full fare and reduced fares for journeys in second or first class. They can be bought from TPF ticket offices and ticket machines.

Frimobil Travel card

A Frimobil Travel card will allow you travel without restriction for a week, a month or a year within the zones you choose.

About Fribourg

Fribourg is the capital of the Swiss canton of Fribourg and the district of Sarine. It is located on both sides of the river Saane/Sarine, on the Swiss plateau, and is an important economic, administrative and educational center on the cultural border between German and French Switzerland (Romandy). Its Old City, one of the best maintained in Switzerland, sits on a small rocky hill above the valley of the Sarine.



Fribourg was founded in 1157 by Berchtold IV von Zähringen. Its name is derived from German frei (free) and Burg (fort). Its most ancient part is conveniently located on a former peninsula of the River Sarine, protectealtd on three sides by steep cliffs. The easily defended city helped the Dukes of Zähringen to strengthen and extend their power in the Swiss plateau in the area between the Aar and the Saane/Sarine.

The Old City is located on a hill, only about 100 metres wide, which rises about 40 metres above the valley floor. Most quarters of the city are located on the High Plateau and its surrounding hills, which have an average elevation of 620 metres. The valley floor is only settled in the area immediately around the Old City.

As you discover the Old Town with its medieval streets and houses transposed into the present. Come to Fribourg and cross its bridges… bridges between two cultures, bridges linking the past and the future, the traditional and the modern. The pedestrian streets, the friendly terraces of its cafés. Savor the city, explore its treasures, museums and monuments. Discover the works of contemporary artists, such as Alfred Manessier, Jean Tinguely, Niki de Saint Phalle, Mario Botta and Jean Nouvel. Take a walk through history, leaving the ramparts to discover the medieval layout of the Old Town. Imagine shops and crafts of another era as the streets guide you past the Gothic facades.

Cross the bridges, sense the evolution between old and modern, and look past the ramparts to catch a glimpse of the future. Discover the magic of the Old Town, tread the cobbled streets, reach out and touch the stone of the bridges and feel the passing of time.

Enter the St. Nicholas Cathedral and be awed by the grandeur and grace of the Gothic architecture. Be inspired by the artistry of the builders, stone cutters and craftsmen who created it over the centuries. Climb the 365 steps of the spiral staircase to the top of the tower and you might hear the chimes of some of its thirteen bells, among the oldest in Switzerland.

The great chefs of Fribourg's many gourmet restaurants will whet your appetite with masterfully prepared seasonal menus that highlight regional products with authenticity, creativity and elegance – an incomparable and unforgettable experience. Try Fribourg's specialities, typical regional dishes such as cabbage, ham on the bone, the local botzi pears, meringues with the rich thick cream from Gruyère, anise seed bread or «bricelets», thin waffle biscuits… and don't forget to try the «cuchaule», a brioche-like sweet saffron bread to be eaten with the famous bénichon mustard, a delicious blend of sweet and spicy flavours.

Source: Fribourg Tourism

Travelling to Switzerland – useful information

Time zone

During the winter, Central European Time (CET) applies in Switzerland. From the end of March to the end of October, Summer Time applies (CET + 1 hour).

Important telephone numbers

Emergency Calls:

- 117 Police
- 118 Fire
- 144 Ambulance
- 1414 Swiss Rescue

Currency

Please note that Switzerland remains with the Swiss franc, usually indicated as CHF. While Switzerland is not part of the European Union and thus is not obliged to convert to the Euro, many prices are nonetheless indicated in euros so that visitors may compare prices.

Merchants may accept euros but are not obliged to do so. Change given back to the client will most likely be in Swiss francs.

Coins

5, 10, 20, 50 Cents and 1, 2, 5 Francs

Bank notes

10, 20, 50, 100, 200, 1000 Francs

Exchange rates*:

USD 1 = CHF 0,91

EUR 1 = CHF 1,21

GBP 1 = CHF 1,51

(* 25.08.2014)

Creditcards & money exchange

The cards most used are American Express, MasterCard and Visa.

Many banks in Switzerland have equipped their ATM machines with the CIRRUS or MAESTRO system. Many other Swiss banks offer ATM machines for cash advances with your credit card. It is recommended to have a small amount of cash on hand upon arrival in Switzerland for immediate expenses, i.e. taxies, city transportation etc.

You can change money at the following places:

- any Swiss bank
- airport
- main railway stations (western union)
- major hotels

Swiss banks offer the best exchange rates for your traveler's checks or cash for foreign currencies (only bank notes). Official exchange offices and hotels may charge a fee for their services.

Electricity

The voltage in Switzerland, as in most of Europe, is 230V/50 Hz.
Switzerland uses type C (2-pin) and Type J (3-pin) plugs. (Type C 2-pin plugs also fit J sockets.)

Drinking water

Swiss drinking water – a quality product from natural resources – of which 80 percent stems from natural springs and groundwater, and the rest from lakes. Strict regulations concerning water and the quality of it have led to such positive development that, in some places, you can drink straight out the lake without second thoughts! Swiss tap water also demonstrates a more balanced ecology as opposed to water purchased in bottles and mineral waters travelling from near and far.

Tipping

You never have to worry about tipping in Switzerland, as tips are included in the price. You can, however, add a smile to the face of someone who has provided good service by rounding up to the nearest franc or round figure.

Tax free shopping

The VAT you pay on purchased goods in Switzerland is 8%. You may ask at the shops for your Global Refund Cheque and reclaim the VAT. Your total purchases in a shop must amount to more than CHF 300 (including VAT). You must be a resident outside Switzerland and the goods must be exported within 30 days.
More informations: www.globalrefund.com

Business Hours

Banks

Banks are usually open Monday to Friday from 8:30 am to 4:30 pm. Once a week they extend their hours. They are closed Saturdays, Sundays and on public holidays. However, money can also be changed at major train stations. Look for the "Change/Cambio" signs.

Generally, offices are open 8 am to 12 noon and 2 pm to 5 pm on weekdays and closed on weekends. Many banks have automated teller machines (ATMs) that accept overseas bank cards. Please check with your local bank before leaving if your bank card is valid in Switzerland.

Post Offices

Post offices are usually open from 8 am to 12 noon and 2 pm to 5 pm on weekdays, whereas some branches that are located in shopping centers are usually open the same hours as the shopping centers, including the extended business times that are often offered once a week.

Shops

Shops in smaller towns and villages are generally open from 8.30 am - 12 noon and again from 2 - 6.30 pm. In larger cities they do not close for lunch.

Customs entry regulations

Duty and tax free imports per person:

Used personal effects

Used personal effects, such as clothing, underwear, toilet articles, sports gear, photo and film cameras, camcorders, portable computers, musical instruments, and other articles for general use.

Provision
Foodstuff and non-alcoholic beverages for the day of travelling.

Tobaccos and spirits
These limits apply only to persons older than 17 years:

- 200 cigarettes or 50 cigars or 250 grams of pipe tobacco
- 2 litres of alcohol (up to 15% vol.) and 1 litre of alcohol (over 15% vol.)

Cash
Importation and exportation of cash are not subjected to restrictions.

Other goods
For other private goods there is a total value limit of CHF 300.- per person.

Source: http://www.myswitzerland.com/

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

Notes

Notes

Program Overview ARES & CD-ARES 2014
8 - 12 September 2014, University of Fribourg, Switzerland

Time	MONDAY, 08.09.			
	LH E	LH B	LH C	LH D
07:30 - 18:00	REGISTRATION			
09:00 - 10:30		SAW I	SeCIHD I	RISI I
10:30 - 11:00	Break			
11:00 - 12:30		SAW II	SeCIHD II	RISI II
12:30 - 14:00	Lunch			
14:00 - 14:30	Opening			
14:30 - 16:00	ARES I - BEST PAPER SESSION *LH A*			
16:00 - 16:30	Break			
16:30 - 18:00	ARES Full II		SeCIHD III	RISI III
18:00 - 22:00	Welcome Reception			

Time	TUESDAY, 09.09.		
	LH E	LH B	LH C
08:00 - 17:30	REGISTRATION		
09:00 - 10:30	Keynote - Bart Preneel Katholieke Universiteit Leuven, Belgium *LH A*		
10:30 - 11:00	Break		
11:00 - 12:30	ARES Short I	CD-ARES I	SeCIHD IV
12:30 - 14:00	Lunch		
14:00 - 15:30	ARES Full III	CD-ARES II	WSDF
15:30 - 16:00	Break		
16:00 - 17:30	ARES Full IV	CD-ARES III	RAMSS I
17:30 - 19:00	Sightseeing Tour		

Time	WEDNESDAY, 10.09.			
	LH E	LH B	LH C	LH D
08:00 - 17:00	REGISTRATION			
09:00 - 10:30	Keynote - Volkmar Lotz SAP Research, Germany *LH A*			
10:30 - 11:00	Break			
11:00 - 12:30	ARES Short II	ECTCM I	RAMSS II	ARES-IND I
12:30 - 14:00	Lunch			
14:00 - 15:30	ARES Short III	ECTCM II	RAMSS III	ARES-IND II
15:30 - 16:00	Break			
16:00 - 17:00	Keynote - Allison Mankin Verisign Labs, US *LH A*			
17:00 - 23:00	Conference Dinner			

Time	THURSDAY, 11.09.		
	LH B	LH C	LH D
08:00 - 18:00	REGISTRATION		
09:00 - 10:30	IWSMA I	SecATM I	FARES I
10:30 - 10:45	Break		
10:45 - 12:15	IWSMA II	SecATM II	FARES II
12:15 - 13:00	Lunch		
13:00 - 15:00	(ISC)2 SecureFribourg (open for all participants)		
15:00 - 15:30	Break		
15:30 -17:00	(ISC)2 SecureFribourg (open for all participants)		
17:00 - 18:00	(ISC)2 Member Reception (open for all participants)		

FRIDAY, 12.09.
Excursion / Sightseeing tour