ARES Conference
International Conference on Availability, Reliability and Security

ARES 2016

11th International Conference on Availability, Reliability and Security

31 August – 02 September, 2016
Salzburg, Austria

ARES 2016
11th International Conference on Availability, Reliability and Security
August 31 - September 2, 2016
Salzburg, Austria
©shutterstock.com

Organized by….

SBA Research

fhs Fachhochschule Salzburg University of Applied Sciences

Supported by....

Society for ICT Knowledge Transfer

TU Wien Technische Universität Wien Vienna University of Technology

WKS Unternehmensberatung · Buchhaltung · IT

Table of Content

Welcome to ARES 2016

It is our great pleasure to welcome you to the Eleventh International Conference on Availability, Reliability and Security (ARES 2016) in Salzburg, Austria.

This event brings together researchers and practitioners in the fields of IT security, dependability and information assurance. ARES 2016 highlights the interdisciplinary nature of the fields and also picks up new trends. Following the tradition of previous ARES conferences, a special focus is given to the crucial linkage between availability, reliability, security and privacy.

ARES 2016 aims at strengthening the exchange of the various disciplines and furthering discussion in the community. We are very happy to have three distinguished keynote speakers at the main conference in 2016: Bernhard Schölkopf (Max-Planck-Campus Tübingen, Germany) will talk about machine learning, Negar Kiyavash (University of Illinois at Urbana-Champaign, US) will address the topic of (the lack of) privacy in anonymized networks and Koen Hermanns (EUROJUST, The European Union's Judicial Cooperation Unit) will talk about international judicial cooperation in the fight against cybercrime.

From the many submissions we have selected the 21 best for presentation as full paper. The quality of submissions has steadily improved over the last few years and the conference officers faced a difficult decision when selecting which papers should be accepted. This year's acceptance rate for full papers was only 24.42%. In addition, several workshops and short papers are included in the program to show intermediate results of ongoing research projects and offer interesting starting points for discussion. The ARES EU Projects Symposium is held for the second time in conjunction with the ARES Conference. The goal is to disseminate the results of EU research projects, meet potential project partners and exchange ideas within the scientific community.

The organization of ARES 2016 was a great team effort. We first thank the authors for providing the content of the program. We are grateful to the program committee, who worked very hard in reviewing papers and providing feedback for authors. Finally, we thank all workshop chairs for their efforts in organizing interesting workshop sessions. Special thanks are due to Yvonne Poul and Bettina Bauer from SBA research for the smooth organization.

ARES is hosted in a different country each year. After Fribourg in 2014, and Toulouse in 2015, this year's ARES takes place in Salzburg, Austria. We would like to thank the Salzburg University of Applied Sciences for hosting the conference.

We hope that you will thoroughly enjoy the conference program, participate in interesting discussions during the conference and get new motivation from the talks and the exchange.

Have a great time at ARES 2016 and in Salzburg!

Dominik Engel
ARES 2016 General Chair & Program Committee Chair
Salzburg University of Applied Sciences
Austria

Stephen B. Wicker
ARES 2016 Program Committee Chair
Cornell University
USA

Welcome to CD-ARES 2016

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.

To guarantee a high-quality event, we assembled a program for CD-ARES 2016 consisting of 12 selected papers. CD-ARES 2016 provides a good mix of topics ranging from knowledge management and software security to mobile and social computing.

Machine learning is the fastest growing field in computer science, and health informatics is among the greatest challenges, where privacy, data protection, safety, information security and fair use of data is of utmost importance. Experts of work area 1 (data science), 2 (machine learning) and 7 (privacy) of the international expert network HCI-KDD have carefully selected five papers for the PAML (Privacy Aware Machine Learning) session.

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 efforts contributing their time, knowledge, expertise and foremost the authors for their contributions.

Have a great time at ARES 2016 and in Salzburg!

Francesco Buccafurri, Andreas Holzinger, Peter Kieseberg, A Min Tjoa, Edgar Weippl
CD-ARES 2016 Chairpersons

Welcome to the ARES EU Projects Symposium 2016

The ARES EU Projects Symposium is held for the second time in conjunction with the ARES Conference.

The goal is to disseminate the results of EU research projects, meet potential project partners and exchange ideas within the scientific community.

This year, eight workshops will be held within the ARES EU Project Symposium:

- 1st Workshop on Future Access Control, Identity Management and Privacy Preserving Solutions in Internet Services (FASES 2016)
- 1st Workshop on Security, Privacy, and Identity Management in the Cloud (SECPID 2016)
- 1st Workshop on Multi User Interaction in Social Media: Secure information flow for disaster emergencies (MUININ 2016)
- 1st International Workshop on Social collaboration in trusted, user-driven software development (SOCOTUD 2016)
- 1st Workshop on Measuring the Economic Impact of Cyber Crime and Devising Solutions (E-CRIME 2016)
- 1st Workshop on Risk Assessment for Socio-Technical Systems (RESIT 2016)
- 1st Workshop on Secure and Efficient Outsourcing of Storage and Computation of Data in the Cloud (SECODIC 2016)
- 1st Workshop on Strengthening Cooperation of European Network Centres of Excellence in Cybercrime (SENCEC 2016)

We would like to thank the workshop organizers for their great efforts and hard work in proposing the workshop, selecting the papers, the interesting programs and for the arrangements of the workshops during the conference days.

We hope you enjoy the ARES EU Projects Symposium!

This year the following projects will be represented:

tredisec

witdom

TYPES

ReCRED

prisma cloud

CREDENTIAL

CLOUD TEAMS

SLÁNDÁIL

senter

predict
prioritise
prevent
TREsPASS

ecrime
The Economic Impacts of Cyber Crime

SECODIC 2016 - Workshop on Secure and Efficient Outsourcing of Storage and Computation of Data in the Cloud

Workshop Chairs:

- Melek Önen (EURECOM, France)
- Ghassan Karame (NEC, Germany)
- Matthias Neugschwandtner (IBM Research, Switzerland)
- Elsa Prieto (Atos, Spain)
- Eduarda Freire (IBM Research, Switzerland)

Abstract: Cloud computing services are increasingly being adopted by individuals and companies owing to their various advantages such as high storage and computation capacities, reliability, and low maintenance costs. The advent of cloud storage and computation services, however, comes at the expense of data security and privacy. For example, when users upload data to the cloud, they tend to lose control over their data and have little means to verify, for example, how data is processed or stored. Therefore, customers nowadays call for end-to-end security whereby only the data owner and authorized parties can have access to the data. End-to-end security has gained even more importance after the outbreak of data breaches and massive surveillance programs around the globe last year.

At the same time, end-to-end security poses a number of new challenges to cloud providers. How can they keep their costs low by making efficient use of their resources when users upload encrypted data? How can they offer computational services over encrypted user data? How can cloud providers perform computation over user data under the requirement that they do not know the specifics of the computational algorithm?

Addressing these questions, this workshop aims at discussing the recent advances in managing security and performance in the cloud as well as protection of data at rest and in transit. This research is not only motivated by users' satisfaction, but also by the enforcement of European Data Protection Regulations as well as institution's internal regulations. Since the majority of institutions lack resources and computing power to deal with large amount of data, and therefore outsourcing data to the cloud is strictly necessary, not complying with those regulations means not advancing in research.

These challenges drive a number of EU projects to devise effective solutions that meet the growing need for data protection in a number of security-critical scenarios (e.g. Financial Services and ehealth). Two of these projects are TREDISEC and WITDOM:

TREDISEC aims to design novel security primitives that ensure data protection and user privacy while maintaining the cost effectiveness of cloud systems. By doing so, TREDISEC aims to conciliate functional requirements in the cloud (such as multitenancy and data deduplication) with various security and privacy requirements to meet EU data protection regulations. This will provide considerable incentives for cloud providers to offer security services to their clients (since these services do not come at odds with resource sharing) and will increase the adoption of the cloud paradigm by companies and individuals (since end-to-end security is ensured at all times).

WITDOM aims at developing an end-to-end secure by design framework for data storage and processing in non-trusted environments. This framework will be instantiated with two critical scenarios: a health scenario, based on genetic data outsourcing for large research or individual clinical data analyses, and a financial services scenario, based on customer's data outsourcing for provision of secure and efficient financial services to the clients. The technologies used in WITDOM include privacy-enhancing techniques, homomorphic encryption, and cryptographic techniques for integrity and verifiability of outsourced processes.

During the workshop we will discuss hot topics related to end-to-end security, privacy, and data protection in the cloud and advances in the field. We therefore expect the workshop to give extensive insights into the state-of-the-art in cloud technologies and novel perspectives for ensuring security and privacy in the cloud. The workshop will be an excellent venue for security experts and cloud providers who want to keep up with new research advances in the area of cloud security.

FASES 2016 - Workshop on Future Access Control, Identity Management and Privacy Preserving Solutions in Internet Services

Workshop Chairs:

- Christos Xenakis (University of Piraeus, Greece)
- Nikos Passas (University of Athens, Greece)
- Francesco Bonchi (ISI Foundation, Italy, and Eurecat, Spain)

Abstract: With e-commerce and online advertising now exceeding 1 trillion USD per annum, the sharing economy on the rise, and the emergence of the Internet of Things, the design and implementation of novel solutions for privacy preservation, integrated identity management and reliable and user-friendly authentication and authorization mechanisms is more pressing than ever. Current online services are opaque with respect to data gathering and processing and rely on the password-based concept (developed in the 60's) do not meet the requirements and expectations of users and do not leverage the potential of existing technologies. Although some important steps have been made in resolving fundamental challenges in these areas, new paradigms for transparency, privacy, authentication, authorization and access control are needed. The next generation online services need to facilitate robust access control, safe e-commerce and sharing transactions. At the same time such services should provide an adequate level of transparency on the utilization of user data as well as guarantee a privacy-preserving data processing, sharing and storage. In this workshop we encourage the submission of original works describing more sophisticated solutions in the areas of data transparency, privacy, authentication, authorization and access control, aiming to define the common basis for the development of next generation of online services

Online advertising generated in 2013 $42B worth of revenue and more than 3.4 million direct and indirect jobs in Europe in 2012 alone. It supports some of the most important Internet services such as search, social media and user generated content sites. However, the lack of transparency regarding tracking techniques and the type of information companies collect about users is creating increasing concerns in society. Software tools for implementing total mitigation (e.g., ad blocker or cookies blocker) have been released to block any transfer of information from end users towards the online advertising ecosystem. A massive adoption of these tools by end users may cause disruptions in the digital economy by affecting the online advertising sector and leading to consequences such as losing of a large number of employments. TYPES aims to cope with this challenge by defining, implementing, and validating in pre-market status a holistic framework of technologies and tools that guarantees both transparency and privacy preservation, gives the end user control upon the amount of information he/she is willing to share, and defines privacy-by-design solutions. In particular, these tools should enable the end user: i) to configure the privacy settings so that only the information allowed by the end-user is collected by online advertising platforms; ii) to understand the flow of their information within the online advertising ecosystem and how it is being used; iii) to detect episodes of information collection occurring without consent and identify the offender; iv) to know the value of their data. TYPES will demonstrate solutions that protect user's privacy while empowering them to control how their data is used by service providers for advertising purposes. At the same time, TYPES will make it easier to verify whether users' online rights are respected and if personal data is exchanged for a reasonable value-added to users.

ReCRED's ultimate goal is to promote the user's personal mobile device to the role of a unified authentication and authorization proxy towards the digital world. ReCRED adopts an incrementally deployable strategy in two complementary directions: extensibility in the type and nature of supported stakeholders and services (from local access control to online service access), as well as flexibility and extensibility in the set of supported authentication and access control techniques; from widely established and traditional ones to emerging authentication and authorization protocols as well as cryptographically advanced attribute-based access control approaches. Simplicity, usability, and users privacy is accomplished by: i) hiding inside the device all the complexity involved in the aggregation and management of multiple digital identifiers and access control attribute credentials, as well as the relevant interaction with the network infrastructure and with identity consolidation services; ii) integrating in the device support for widespread identity management standards and their necessary extensions; and iii) controlling the exposure of user credentials to third party service providers. ReCRED addresses key security and privacy issues such as resilience to device loss, theft and impersonation, via a combination of: i) local user-to-device and remote device-to-service secure authentication mechanisms; ii) multi-factor authentication mechanisms based on behavioral and physiological user signatures not bound to the device; iii) usable identity management and privacy awareness tools; iv) usable tools that offer the ability for complex reasoning of authorization policies through advanced learning techniques. ReCRED's viability will be assessed via four large-scale realistic pilots in real-world operational environments. The pilots will demonstrate the integration of the developed components and their suitability for end users, so as to show their TRL7 readiness.

SECPID 2016 - Workshop on Security, Privacy, and Identity Management in the Cloud

Workshop Chairs:

- Stephan Krenn (AIT Austrian Institute of Technology GmbH, Austria)
- Thomas Lorünser (AIT Austrian Institute of Technology GmbH, Austria)
- Daniel Slamanig (Graz University of Technology, Austria)
- Bernd Zwattendorfer (Stiftung Secure Information and Communication Technologies, Austria)

Abstract: Over the last years, the computing paradigm has experienced a massive shift from local to cloud-based applications. As a result, users and organizations do no longer have full control over their data and services, but they rely on third-party cloud providers. This development poses various challenges concerning the integrity and confidentiality of data as well as the privacy of users of such systems. Currently, no satisfactory solutions to these challenges exist, which is a roadblock for the large-scale deployment of cloud-based applications handling sensitive data such as electronic health records.

The aim of this symposium is to provide a platform to discuss innovative ideas related to the following questions: How can cloud services be made more trustworthy? How can we build distributed systems without single point of failure or trust? How to design end-to-end secure services in an untrusted environment? Which methodologies and technologies are required to integrate security and privacy by design? Is it possible to give back users full control over their data, i.e., let them decide when and to whom they are revealed? Next to the regular session with peer-reviewed research papers, an invited talk will be given by a representative of the H2020 project SAFECLOUD.

The ambition of PRISMACLOUD is to develop and show-case cryptographic tools that protect the security and privacy of user data during its lifecycle in the cloud. In particular, the project focuses on the development of (information theoretically) secure storage solutions as well as efficient, privacy preserving yet verifiable computing on authenticated data.

CREDENTIAL aims at developing privacy friendly means for storing and sharing personal data in the cloud, and at realizing an “identity and access management as a service” system supporting publicly certified identity data.

SOCOTUD 2016 - The 1st International Workshop on “Social collaboration in trusted, user-driven software development”

Workshop Chairs:

- Sabine Kolvenbach (Fraunhofer Institute for Applied Information Technology, Germany)
- Sebastian Franken (Fraunhofer Institute for Applied Information Technology, Germany)
- Dr. S. Koussouris (National Technical University of Athens, Greece)

Abstract: It can be taken for granted that until today, the requirements’ elicitation process for the majority of both commercial and open source software solutions, as well as their evaluation, takes place within the narrow boundaries of isolated software development teams. Thus the most important stakeholder, the consumer or end-user with their needs are not properly considered. This often results in products and services that are mainly inadequate for the activities their respective product managers have envisioned. In this context, the concept of engaging potential users from the target audience in the software development process is constantly gaining momentum. It is important to build a close relationship with them for receiving early feedback on the product being developed. Apparently, this concept calls for the incorporation of better collaboration support during software development projects and social networking features between software developers and prospective end users within existing software development environments. However, approaches on how to engage potential customers throughout the software development lifecycle are largely unexplored, whereas research on how privacy issues and aspects of trust are shaped in such a user-driven development process is limited. This workshop aims at presenting and discussing concepts and solutions for ensuring customer-developer interaction along the software development process in a trustful and privacy respectful way.

The workshop is organized by the CloudTeams project (Collaborative Software Development Framework based on Trusted, Secure Cloud-based Pool of Users is a research project).

CloudTeams will be a cloud-based platform transforming software development for cloud services into a much easier, faster, and targeted process, by engaging communities of users who will participate in the product lifecycle to help software teams develop better solutions for customers’ problems. CloudTeams is in the intersection of three important fields: crowdsourcing platforms, collaborative software development tools, and trusted cloud service delivery. This innovative combination of different tools and practices under a unique concept will be enhanced with a rewarding system to enable end-users to jump into the platform and support solutions they are interested in. In addition, a testing and trust framework will validate the whole process based on proper analytics and qualitative feedback by the prospective customers. The final, cloud-based software solutions will be validated based on the CloudTeams methodology and thus trusted by the customers, and help developers finding the proper market fit in a quick and efficient way.

MUININ 2016 - Workshop on Multi User Interaction in Social Media: Secure information flow for disaster emergencies

Workshop Chair:
Khurshid Ahmad (Trinity College Dublin, Ireland)

Abstract: The Muinín workshop is being organised to bring together civil protection, including police and intelligence, ethics scholars, legal experts, and technologists involved in introducing and maintaining social information networks for preventing and mitigating the impact of disasters. Muinín is the Irish word for having trust and confidence in oneself and others. The lessons learnt and systems developed during the execution the three year FP7-sponsored security project Slandail (Project No. # 607691, 2014-2017) will form the basis of the workshop. Slandail (Irish for security) and is an acronym for Security System for language and image analysis. The prime objective of the Slandail Project is to evaluate the impact of social media in emergencies.

SLÁNDÁIL presentations will include:

End User Perspective

- Police and civil protection requirements for the use of social media in disaster emergencies
- Inter-operability during an emergency: Multi-cultural and multi-lingual challenges
- Resilience and Business Continuity leveraged through social media interactions and social cohesion
- Building and communicating trust between security agencies and the public

Technical Challenges

- Automatic analysis of texts, images and gestures in social media for identifying unusual events
- Emotion and sentiment analytics for emergency communications.

Ethical and Legal Framework for Data Harvesting and Storing from Social Media

- The essential tension between privacy and safety of citizens: A human rights perspective
- Copyright and data protection implications of harvesting social media data

SLÁNDÁIL is collaboration of emergency operatives, academics, ethics- and legal experts and SME's involved in emergency management, social media systems and public communication. Their common purpose is to make maximum ethical use of the information available in the social media to enhance the performance of emergency management systems. The Project has undertaken research in text and image analysis, in ethical and factual provenance of data, together with SMEs specialising in selling systems for social media analytics and for emergency monitoring. There are experts in human multi-lingual human communication working in the team. This is an Irish-led, Italian, German and British collaboration which will deliver next generation of emergency management systems for police and civil protection agencies.

SENCEC 2016 - Workshop on Strengthening Cooperation of European Network Centres of Excellence in Cybercrime

Workshop Chairs:

- Simas Grigonis (Mykolas Romeris University, Lithuania)
- Evaldas Bružė (Lithuanian Cybercrime Centre of Excellence for Training, Research and Education, Lithuania)
- Egidija Veršinskienė (Lithuanian Cybercrime Centre of Excellence for Training, Research and Education, Lithuania)

Abstract: Over the past few years we have witnessed the creation of several national CoE in the area of cybercrime all over. Today there exist more than 10 CoE operating all over Europe and despite some of the CoE great achievements most of them have been operating mainly in isolation of each other, they have different goals and may frequently result in duplication of effort. Organizations such as Directorate General on Migration and Home Affairs of the European Commission, FRONTEX, EUROPOL, European Cybercrime Training and Education Group (E.C.T.E.G.), INTERPOL, European Cybercrime Centre (EC3), Joint Research Centre (JRC), European Network of Law Enforcement Technology Services (ENLETS) and industry clusters would like to collaborate with the European Network and speed-up development by bridging the resources and using the European Network as a communications, distribution & dissemination channel. However, lack of visible agreement and commitment among the CoE and the current virtual nature of the European Network limits a lot the possibilities to go into any kind of mutual, long-term agreement. Considering the situation described and seeking to identify the means to increase cooperation, best national practices, problematic areas and possible solutions, the following key areas would be discussed in the workshop:

1. means aimed to create and increase international cooperation between national CoE (intended to implement and/or already implemented) and separate collaborating entities
2. best practices concerning CoE operation and management that all members of the European Network could follow
3. Training programs that could potentially be offered to law enforcement agencies with regard to functioning of the European Network of CoE.

The ambition of the SENTER project is to create a single point of reference for EU national cybercrime Centres of Excellence (hereinafter – CoE) and develop further the European Network of national CoE into well-defined and well-functioning community.

RESIST 2016 - Workshop on Risk Assessment for Socio-Technical Systems

Workshop Chair:
Christian W. Probst (Technical University of Denmark, DK)

Abstract: Attacks on organisations are no longer purely technical. Attacks like StuxNet involve technical and human factors, and they damage physical infrastructure. The recent attack on a German steel mill was a combination of both targeted phishing emails and social engineering attacks. The phishing helped the hackers extract information they used to gain access to the plant's office network and then its production systems. As a result, the technical infrastructure of the mill suffered severe damage. The attack on the German steel mill illustrates that we need to integrate the social and technical aspects of systems in assessing their security – and we need to do so today. Socio-technical systems pose new challenges by combining parts for which we often understand the security issues; the combined system is however much more complex due to interactions between these parts. This new class of attacks cleverly exploits multiple organisational vulnerabilities, involving physical security and human behaviour. Defenders need to make rapid decisions regarding which attacks to block, as both infrastructure and attacker knowledge change rapidly. Emerging security risks demand tool support to predict, prioritise, and prevent complex attacks systematically. This workshop will address recent advances in risk analysis for socio-technical systems. The research presented builds upon results from technical and social sciences, combining them for a better understanding of vulnerabilities of organisations as a whole, and supporting defenders in deciding where to invest resources for protection. During the workshop we will discuss topics relevant for risk assessment of socio-technical systems and advances in the field. The workshop will be highly interactive, providing ample opportunity for interaction with project members and discussions around the project results and tools.

The discussed challenges and presented findings are at the core of the TRESPASS project, which has developed the "attack navigator". The attack navigator identifies possible attack opportunities, ranks them by urgency, and suggests countermeasures. The project has also developed novel physical modelling tools to build maps for the navigator, and to identify relevant elements of an organization.

E-CRIME 2016 - Workshop on Measuring the Economic Impact of Cyber Crime and Devising Solutions

Workshop Chairs:

- Monica Lagazio (Trilateral Research & Consulting, UK)
- Bil Hallaq (University of Warwick, UK)
- Timothy Mitchener-Nissen (Trilateral Research & Consulting, UK)

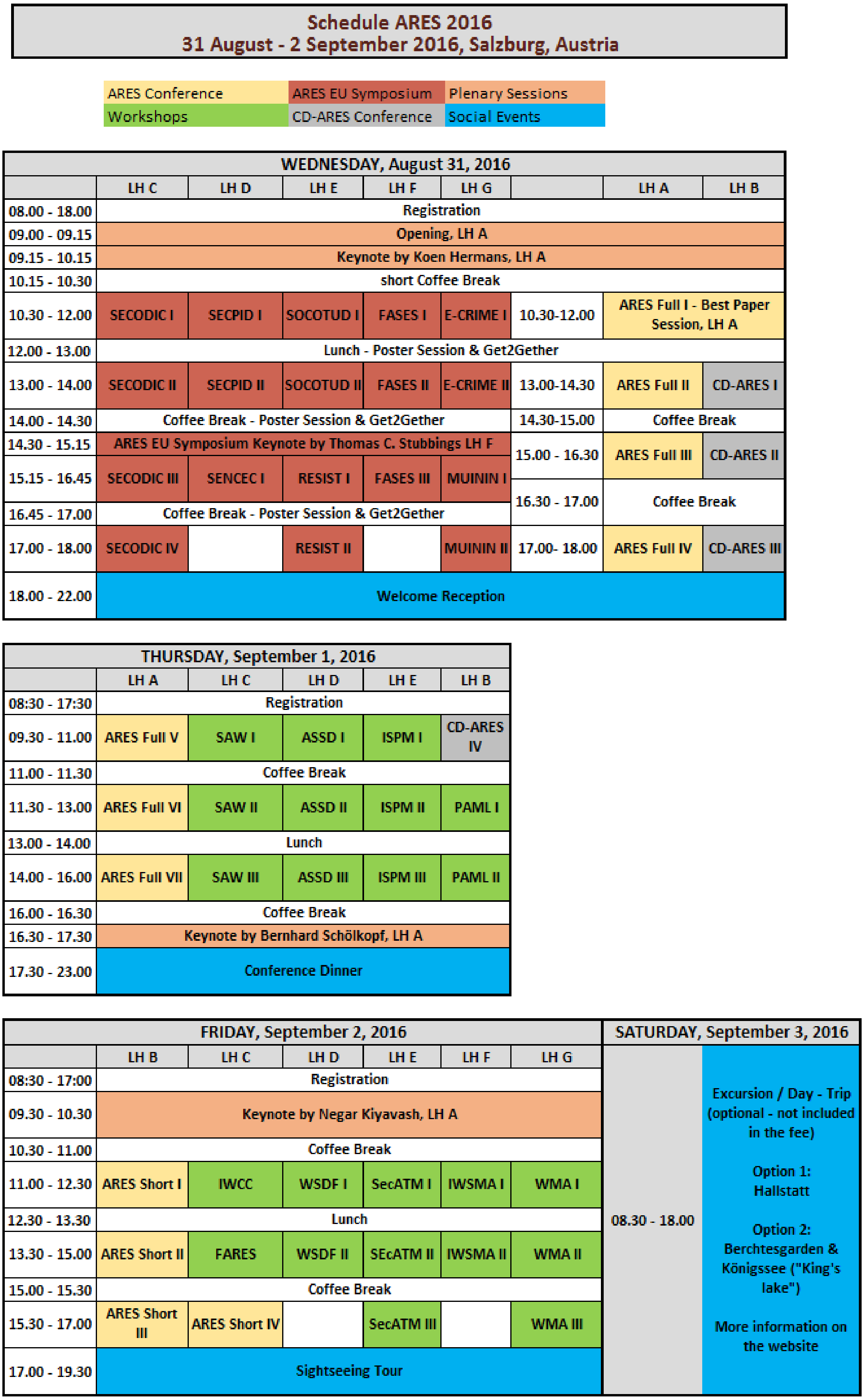
Abstract: E-CRIME (the economic impacts of cyber-crime) is a three year project that started in April 2014 and will end in March 2017. The aim of the project is to reconstruct the spread and development of cybercrime in non-information and communications technology (non-ICT) sectors from the perspective of its economic impact on the key fabrics (i.e., economic and social) and different levels of European society, while also identifying and developing concrete measures to manage and deter cybercrime.

E-CRIME focuses on:

1. Mapping the observable developments and effects of cybercrime within and among non-ICT sectors, Member States and diverse stakeholder communities
2. Assessing existing counter-measures
3. Measuring the economic impact of cybercrime on non ICT-sectors and
4. Developing concrete inter-sector and intra-sector solutions to address cyber crime

E-CRIME is funded by the European Commission, and has ten partners from eight European countries.

Program Overview



Schedule ARES 2016
31 August - 2 September 2016, Salzburg, Austria

ARES Conference	ARES EU Symposium	Plenary Sessions
Workshops	CD-ARES Conference	Social Events

WEDNESDAY, August 31, 2016								
	LH C	LH D	LH E	LH F	LH G		LH A	LH B
08.00 - 18.00	Registration							
09.00 - 09.15	Opening, LH A							
09.15 - 10.15	Keynote by Koen Hermans, LH A							
10.15 - 10.30	short Coffee Break							
10.30 - 12.00	SECODIC I	SECPID I	SOCOTUD I	FASES I	E-CRIME I	10.30-12.00	ARES Full I - Best Paper Session, LH A	
12.00 - 13.00	Lunch - Poster Session & Get2Gether							
13.00 - 14.00	SECODIC II	SECPID II	SOCOTUD II	FASES II	E-CRIME II	13.00-14.30	ARES Full II	CD-ARES I
14.00 - 14.30	Coffee Break - Poster Session & Get2Gether					14.30-15.00	Coffee Break	
14.30 - 15.15	ARES EU Symposium Keynote by Thomas C. Stubbings LH F					15.00 - 16.30	ARES Full III	CD-ARES II
15.15 - 16.45	SECODIC III	SENCEC I	RESIST I	FASES III	MUININ I	16.30 - 17.00	Coffee Break	
16.45 - 17.00	Coffee Break - Poster Session & Get2Gether							
17.00 - 18.00	SECODIC IV		RESIST II		MUININ II	17.00- 18.00	ARES Full IV	CD-ARES III
18.00 - 22.00	Welcome Reception							

THURSDAY, September 1, 2016					
	LH A	LH C	LH D	LH E	LH B
08:30 - 17:30	Registration				
09.30 - 11.00	ARES Full V	SAW I	ASSD I	ISPM I	CD-ARES IV
11.00 - 11.30	Coffee Break				
11.30 - 13.00	ARES Full VI	SAW II	ASSD II	ISPM II	PAML I
13.00 - 14.00	Lunch				
14.00 - 16.00	ARES Full VII	SAW III	ASSD III	ISPM III	PAML II
16.00 - 16.30	Coffee Break				
16.30 - 17.30	Keynote by Bernhard Schölkopf, LH A				
17.30 - 23.00	Conference Dinner				

FRIDAY, September 2, 2016							SATURDAY, September 3, 2016	
	LH B	LH C	LH D	LH E	LH F	LH G	08.30 - 18.00	Excursion / Day - Trip (optional - not included in the fee) Option 1: Hallstatt Option 2: Berchtesgarden & Königssee ("King's lake") More information on the website
08:30 - 17:00	Registration							
09.30 - 10.30	Keynote by Negar Kiyavash, LH A							
10.30 - 11.00	Coffee Break							
11.00 - 12.30	ARES Short I	IWCC	WSDF I	SecATM I	IWSMA I	WMA I		
12.30 - 13.30	Lunch							
13.30 - 15.00	ARES Short II	FARES	WSDF II	SEcATM II	IWSMA II	WMA II		
15.00 - 15.30	Coffee Break							
15.30 - 17.00	ARES Short III	ARES Short IV		SecATM III		WMA III		
17.00 - 19.30	Sightseeing Tour							

ARES EU SYMPOSIUM - Wednesday, August 31, 2016

08:00 – 18:00 Registration desk open

09:00 – 09:15 Opening

09:15 – 10:15 Plenary Session

Keynote

Location: Lecture Hall A
Time: 09:15-10:15

International Judicial Cooperation in the Fight against Cybercrime

Koen Hermanns (EUROJUST, The European Union's Judicial Cooperation Unit, Belgium)

10:15 – 10:30 short Coffee Break

10:30 – 12:00 Parallel Sessions

SECODIC I – Private and Secure Data Storage in the Cloud I

Session Chair: Eduarda Freire (IBM, Switzerland)
Location: Lecture Hall C
Time: 10:30-12:00

1. "Empowering privacy and security in non-trusted environments": a WITDOM overview (presentation only)
Elsa Prieto (Atos, Spain)

2. "Trust-aware, reliable and distributed information security in the Cloud": a TREDISEC Overview (presentation only)
Ghassan Karame (NEC, Germany)

3. Keynote: Securing cloud-assisted services
N. Asokan (Aalto University, Finland)

Abstract: All kinds of previously local services are being moved to a cloud setting. While this is justified by the scalability and efficiency benefits of cloud-based services, it also raises new security and privacy challenges. Solving them by naive application of standard security/privacy techniques can conflict with other functional requirements. In this talk, I will outline some cloud-assisted services and the apparent conflicts that arise while trying to secure these services. I will then discuss a specific instance: the case of cloud-assisted detection of malicious mobile application packages and the privacy concerns involved. I will discuss how techniques for private membership test, assisted by hardware security mechanisms, can be used to address these concerns.

4. Talk on Data Masking (presentation only)
Eduarda Freire (IBM Research, Switzerland)

SECPID I – Security and Privacy in the Cloud I

Session Chair: Stephan Krenn (AIT, Austria)
Location: Lecture Hall D
Time: 10:30-12:00

1. PRISMACLOUD Tools: A cryptographic toolbox for increasing security in cloud services

Thomas Lorünser (AIT, Austria), Daniel Smalanig (Graz University of Technology, Austria), Thomas Länger (University of Lausanne, Switzerland) and Henrich Pöhls (University of Passau, Germany)

Abstract: The EC Horizon 2020 project PRISMACLOUD aims at cryptographically addressing several severe risks threatening end user security and privacy in current cloud settings. This shall be achieved by the provision of a reusable toolbox encapsulating cryptographic functionality from which dependably secure cloud services can be assembled. In order to provide a tangible abstraction of the complexity involved with the construction of cryptographically secured cloud services, we introduce the fourlayer PRISMACLOUD architecture. Top down, it consists of a use cases (application) layer, a services layer, a tools layer, and a cryptographic primitives and protocols layer. In this paper we provide a detailed description of the PRISMACLOUD tools in terms of functional components, as well as how they interact to provide the desired security functionality. We also briefly describe the cutting-edge cryptographic primitives which are encompassed by the tools. Both the toolbox and the cryptographic primitives and protocols are being currently developed and will be provided as reference implementation by project end in July 2018.

2. CREDENTIAL: A Framework for Privacy-Preserving Cloud-Based Data Sharing

Felix Hörandner (Graz University of Technology, Austria), Stephan Krenn (AIT, Austria), Andrea Migliavacca (Lombardia Informatica S.p.A., Italy), Florian Thiemer (Fraunhofer FOKUS, Germany) and Bernd Zwattendorfer (Stiftung Secure Information and Communication Technologies, Austria)

Abstract: Data sharing – and in particular sharing of identity information – plays a vital role in many online systems. While in closed and trusted systems security and privacy can be managed more easily, secure and privacy preserving data sharing as well as identity management becomes difficult when the data are moved to publicly available and semi-trusted systems such as public clouds. CREDENTIAL is therefore aiming on the development of a secure and privacy-preserving data sharing and identity management platform which gives stronger security guarantees than existing solutions on the market. The results will be showcased close to market-readiness through pilots from the domains of eHealth, eBusiness, and eGovernment, where security and privacy are crucial. From a technical perspective, the privacy and authenticity guarantees are obtained from sophisticated cryptographic primitives such as proxy re-encryption and redact able signatures.

3. Towards Secure Collaboration in Federated Cloud Environments

Bojan Suzic and Andreas Reiter (IAIK, Austria)

Abstract: Public administrations across Europe are actively following and adopting cloud paradigms. By establishing modern data centers and consolidating their infrastructures, many organizations already benefit from cloud computing. However, there is a growing need to further support the consolidation and sharing of resources across different public entities or corporations. The ever increasing volume of processed data and diversity of organizational interactions stress this need even further, calling for the integration on infrastructure, data and services level. This is currently hindered by strict requirements in the field of data security and privacy. In this paper, we present ongoing work enabling secure private cloud federations for public administrations, performed in the scope of the SUNFISH H2020 project. We focus on architectural components and processes that establish cross-organizational enforcement of data security policies in heterogeneous environments. Our proposal introduces proactive restriction of data flows in federated environments by integrating real-time based security policy enforcement and its post-execution conformance verification. The goal of this framework is to enable secure service integration and data exchange in cross-entity contexts by inspecting data flows and assuring their conformance with security policies, both on organizational and federation level.

4. Keynote: Building a Secure and Resilient Cloud Architecture: Theoretical and Practical Challenges behind the SafeCloud Project

Hugues Mercier (Research associate at the Université de Neuchâtel, Switzerland)

Abstract: Cloud infrastructures, despite all their advantages and importance to the competitiveness of modern economies, raise fundamental questions related to the privacy, integrity, and security of offsite data storage and processing tasks. There are major privacy and security concerns about data located in the cloud, especially when data is physically located, processed, or must transit outside the legal jurisdiction of its rightful owner. These questions are currently not answered satisfactorily by existing technologies. This talk presents the objectives and challenges of the H2020 SafeCloud project. SafeCloud will re-architect cloud infrastructures to ensure that data transmission, storage, and processing can be (1) partitioned in multiple administrative domains that are unlikely to collude, so that sensitive data can be protected by design; (2) entangled with inter-dependencies that make it

impossible for any of the domains to tamper with its integrity. These two principles (partitioning and entanglement) are applied holistically across the entire data management stack, from communication to storage and processing.

SOCOTUD I – Talks and discussions on recent trends in user involvement and social collaboration

Session Chair: Dr. Sebastian Franken (Fraunhofer FIT, Germany)
Location: Lecture Hall E
Time: 10:30-12:00

1. Workshop Introduction

Sebastian Franken (Fraunhofer FIT, Germany) and Sotiris Koussouris (National Technical University of Athens, Greece)

2. Involving Users into Collaborative Software Development – The Case of CloudTeams

Sebastian Franken, Sabine Kolvenbach and Wolfgang Gräther (Fraunhofer FIT, Germany)

Abstract: Producing meaningful and usable software that meets the end users' needs is the goal of every software development process. To achieve this, there is a need for involving end users into the software development process in a collaborative way. Both parties profit from this approach: Developers receive early feedback and detect conceptual and design flaws, while customers gain insights into the software development process and ensure to get relevant software. This avoids increasing costs in the software development process. The EU-funded project CloudTeams supports early user involvement in the software development process and addresses the challenge of bridging this gap between users and developers. In this paper, we describe a concrete showcase of user involvement in the software development process with CloudTeams.

3. Social Analytics in an Enterprise Context: From Manufacturing to Software Development

Angelos Arvanitakis, Michael Petychakis, Evmorfia Biliri, Ariadni Michalitsi-Psarrou, Panagiotis Kokkinakos, Fenareti Lampathaki, and Dimitris Askounis (National Technical University of Athens, Greece)

Abstract: Although customers become more and more vocal in expressing their experiences, demands and needs in various social networks, companies of any size typically fail to effectively gain insights from such social data and to eventually catch the market realm. This paper introduces the Anlzer analytics engine that aims at leveraging the "social" data deluge to help companies in their quest for deeper understanding of their products' perceptions as well as of the emerging trends in order to early embed them into their product design phase. The proposed approach brings together polarity detection and trend analysis techniques as presented in the architecture and demonstrated through a simple walkthrough in the Anlzer solution. The Anlzer implementation is by design domain-independent and is being tested in the furniture domain at the moment, yet it brings significant added value to software design and development, as well, through its experimentation playground that may provide indirect feedback on future software features while monitoring the reactions to existing releases.

4. SmartNet: Secure content sharing for peer to peer smart group spaces

Brian Greaves and Marijke Coetzee (University of Johannesburg, South Africa)

Abstract: Modern smart devices such as smart phones and tablets are becoming more pervasive in society, and at the same time are generating and storing more content. Users have become used to maintaining data on cloud based servers using simple interfaces, but they find that it is costly due to data costs for uploading and downloading files. Due to publicity given to compromised data stored in cloud-based servers, users are hesitant to store sensitive data in the cloud. Current research points to the fact that peer-to-peer mobile data storage solutions are becoming more viable, thereby solving some concerns that users have. To complement this research focus, this research presents SmartNet, an Android application which brings peer-to-peer content sharing capabilities to smart devices. Devices are grouped in smart group spaces, where the preferences of the owner of a group determines access to content in the group. The smart group space access control policy is implemented by the SmartNet prototype. The SmartNet prototype is evaluated where results indicate that content can be shared flexibly, overcoming cloud-based storage problems.

FASES I – Data Protection, Privacy Preservation and Discrimination Discovery

Session Chair: Ángel Cuevas Rumín (Universidad Carlos III de Madrid, Spain)
Location: Lecture Hall F
Time: 10:30-12:00

1. From discrimination discovery to preventing algorithmic bias (Invited Talk)

Sara Hajian (Eurecat - Technology Centre of Catalonia, Spain)

2. Privacy preserving computations for viral marketing: the case of rational players

Rica Gonen and Tamir Tassa (The Open University, Israel)

Abstract: Viral marketing is a methodology which is based on exploiting a pre-existing social network in order to increase brand awareness or product sales through self-replicating viral processes. An essential computational task towards setting up an effective viral marketing campaign is to estimate social influence. Such estimates are usually done by analyzing user activity data. The data analysis and sharing that is needed to estimate social influence raises important privacy issues that may jeopardize the legal, ethical and societal acceptability of such practice, and in turn, the concrete applicability of viral marketing in the real world. Tassa and Bonchi (EDBT 2014) devised secure multi-party protocols that allow a group of service providers and a social networking platform to jointly compute social influence in a privacy preserving manner. They assumed that the players are semi-honest, i.e., that they follow the protocol correctly, but at the same time they examine their view of the protocol in order to extract information on inputs provided by their peers. In this paper we discuss the case of selfish rational players; such players participate in the protocol and follow it correctly only if it is in their best interest and maximizes their utility. We enhance the protocol of Tassa and Bonchi by incorporating into it mechanisms that incentivize the players to participate in the protocol truthfully.

3. Protecting sensitive information in the volatile memory from disclosure attacks

Stefanos Malliaros, Christoforos Ntantogian and Christos Xenakis (University of Piraeus, Greece)

Abstract: The protection of the volatile memory data is an issue of crucial importance, since authentication credentials and cryptographic keys remain in the volatile memory. For this reason, the volatile memory has become a prime target for memory scrapers, which specifically target the volatile memory, in order to steal sensitive information, such as credit card numbers. This paper investigates security measures, to protect sensitive information in the volatile memory from disclosure attacks. Experimental analysis is performed to investigate whether the operating systems (Windows or Linux) perform data zeroization in the volatile memory. Results show that Windows kernel zeroize data after a process termination, while the Linux kernel does not. Next, we examine functions and software techniques in C/C++ programming language that can be used by developers to modify at process runtime the contents of the allocated blocks in the volatile memory. We have identified that only the Windows operating system provide a specific function named SecureZeroMemory that can reliably zeroize data. Finally, driven by the fact that malware scrapers primarily target web browsers, we examine whether it is feasible to extract authentication credentials from the volatile memory allocated by web browsers. The presented results show that in most cases we can successfully recover user authentication credentials from all the web browsers except when the user has closed the tab that used to access the website.

E-CRIME I – The economic impacts of cyber crime I

Session Chair: Monica Lagazio (Trilateral Research, UK)
Location: Lecture Hall G
Time: 10:30-12:00

1. E-CRIME: Is measuring cybercrime elusive? (presentation only)

Monica Lagazio (Trilateral Research, UK)

2. A view from the frontline on pursuing, apprehending and prosecuting cyber criminals (presentation only)

Charlie McMurdie (PwC, UK)

3. E-CRIME: Discussing the cyber-criminal journeys (presentation only)

Bil Hallaq (the Cyber Security Centre at the University of Warwick, UK)

12:00 – 13:00 Lunch – Poster Session & Get2Gether

13:00 – 14:00 Parallel Sessions

SECODIC II – Private and Secure Data Storage in the Cloud II

Session Chair: Eduarda Freire (IBM, Switzerland)
Location: Lecture Hall C
Time: 13:00-14:00

1. Data Sharing in the cloud with Proxy-Re-Encryption and Malleable Signature (presentation only)

Florian Thiemer (Fraunhofer Institute, Germany)

2. Data-centric security is the right approach for Digital Single Market (presentation only)

Jose Ruiz (Atos, Spain)

3. Networking session with panellists

SECPID II – Security and Privacy in the Cloud II

Session Chair: Daniel Slamanig (TU Graz, Austria)
Location: Lecture Hall D
Time: 13:00-14:00

1. Cryptographically Enforced Four-Eyes Principle

Arne Bilzhause (University of Passau, Germany), Manuel Huber (Fraunhofer Research Institute AISEC, Germany), Henrich C. Pöhls (University of Passau, Germany), and Kai Samelin (IBM Research, Switzerland)

Abstract: The 4-eyes principle (4EP) is a wellknown access control and authorization principle, and used in many scenarios to minimize the likelihood of corruption. It states that at least two separate entities must approve a message before it is considered authentic. Hence, an adversarial party aiming to forge bogus content is forced to convince other parties to collude in the attack. We present a formal framework along with a suitable security model. Namely, a party sets a policy for a given message which involves multiple additional approvers in order to authenticate the message. Finally, we show how these signatures are black-box realized by secure sanitizable signature schemes.

2. Co-Creating Security-and-Privacy-by-Design Systems

Sauro Vicini, Francesco Alberti (Fondazione Centro San Raffaele, Italy), Nicolás Notario, Alberto Crespo (Atos, Spain), Juan Ramón Troncoso Pastoriza (University of Vigo, Spain) and Alberto Sanna (Fondazione Centro San Raffaele, Italy)

Abstract: The elicitation and the analysis of security and privacy requirements are generally intended as being mainly performed by field experts. In this paper we show how it is possible to integrate practical Co-Creation processes into Security-and-Privacy-by-Design methodologies. In addition, we present some guidelines showing how it is possible to translate the high-level requirements obtained from the end-user engaging into verifiable low-level requirements and technological requirements. The paper demonstrates as well the feasibility of our approach by applying it in two realistic scenarios where the outsourcing of personal and sensitive data requires high-level of security and privacy.

3. Tackling the cloud adoption dilemma – A user centric concept to control cloud migration processes by using machine learning technologies

Michael Diener, Leopold Blessing (University of Regensburg, Germany) and Nina Rappel (Brandenburg University of Technology, Germany)

Abstract: Research studies have shown that especially enterprises in European countries are afraid of losing outsourced data or unauthorized access. Despite various existing cloud security mechanisms companies are currently hesitating to adopt cloud resources. This phenomenon is also known as cloud adoption dilemma. We think that data classification is a promising technique that should be considered in the context of cloud security, supporting cloud migration processes. By using classification techniques enterprises are able to control which documents are suited for Cloud Computing and which cloud service providers are sufficient for protecting sensitive documents. In this work we present an efficient concept that involves enterprises' employees and authorities, making it possible to apply powerful security policies in a simple way. We make use of a well-established machine learning algorithm in our developed tool, identifying security levels for different types of documents. Thus, cloud migration processes can become more transparent and enterprises obtain the ability to discuss more openly about adopting innovative cloud services.

SOCOTUD II – Demonstration, talks, and discussion on social collaboration in software development

Session Chair: Iosif Alvertis (NTUA Athens, Greece)
Location: Lecture Hall E
Time: 13:00-14:00

1. Geographic Localization of an Anonymous Social Network Message Data Set

Alexander Böhm, Benjamin Taubmann, and Hans P. Reiser (University of Passau, Germany)

Abstract: Nowadays, privacy and anonymity are becoming more and more important for users of social networks. Thus, it is of particular interest for user of an anonymous, location-based social network if the network is able to provide the anonymity that it appears to provide. In this work, we present an approach to obtain the geographic location of users of the popular Jodel social network. We are able to reconstruct the exact location from which a message was sent with an accuracy of 10 meters, using only 20 requests sent from virtual clients at different locations to the social network service.

2. Using crowdsourced and anonymized Personas in the requirements elicitation and software development phases of software engineering information

Iosif Alvertis, Dimitris Papaspyros, Sotiris Koussouris, Spyros Mouzakitis, and Dimitris Askounis (National Technical University of Athens, Greece)

Abstract: This paper deals with the process of crowdsourcing requirements elicitation in software engineering and the alignment of the customer needs during the development phase, through the usage of anonymous personas, and the support of the persona builder application that allows the extraction of such information through anonymized data. Having identified the realization of users and customers' needs in the software engineering cycle, despite the adoption of agile methods, the paper suggests the usage of a persona that represents a set of users with similar characteristics, a pool of personas that software teams may share with each other through a collaborative application, and persona builder as a tool to generate such personas through real user profiles and data collected through third party services. At the end, a demo application is presented, realizing the concept of anonymized, crowdsourced personas.

FASES II – Economic value of Personal Information

Session Chair: Christos Xenakis (University of Piraeus, Greece)
Location: Lecture Hall F
Time: 13:00-14:00

1.The Value of Online Users: Empirical Evaluation of the Price of Personalized Ads

Miriam Marciel (NEC Labs Europe, Germany), Jose Gonzalez, Yonas Mitike Kassa (Universidad Carlos III de Madrid, Germany), Roberto Gonzalez and Mohamed Ahmed (NEC Labs Europe, Germany).

Abstract: Ad networks use the behaviors of online users to associate them with preferences (features), and market these features to enable advertisers to target online users. Typical features associated with users include location, interests, gender, age, and etc. Furthemore, ad networks provide their clients with campaing creation tools to help to them to configure and run campains. In this paper, we study the pricing of ads using the ad campaing planning tools of ad networks. We develop tools to collect the suggested bid prices from two platforms: YouTube and Facebook. Analyzing these prices we find that United States is the most expensive country in both platforms. We also find that the most expensive preferences are different in YouTube and Facebook. In YouTube, the top preferences are related to Oil & Gas, while in Facebook are devices, ethnics or politics depending on the type of bidding. Finally, we do not find any price difference genders in Facebook.

2. Your Data in the Eyes of the Beholders: Design of a unified data valuation portal to estimate value of personal information from market perspective

Yonas Mitike Kassa, Jose González, Ángel Cuevas, Rubén Cuevas, Miriarm Marciel (Universidad Carlos III de Madrid, Germany) and Roberto González (NEC Labs Europe, Germany)

Abstract: Nowadays Internet companies that offer valuable services "for free" are becoming ubiquitous. Users benefiting from these services have to expose their personal information through these services as they utilize them. On the other hand, personal information is becoming a merchandisable commodity, venues that sell personal information by auction are emerging. One of these markets is in the form of advertising systems. Despite being a lucrative business, the hoarding of user personal information by commercial companies is a growing issue primarily because of its non- transparent nature. In this paper we present a data valuation portal that shades light on what kinds of personal information is on market and the financial value of it.

E-CRIME II – The economic impacts of cyber crime II

Session Chair: Bill Halaq (The Cyber Security Centre at the University of Warwick, UK)
Location: Lecture Hall G
Time: 13:00-14:00

1. E-CRIME: Opportunities for effective countermeasures to fight cybercrime (presentation only)
Bil Hallaq (the Cyber Security Centre at the University of Warwick, UK)

2. Lessons learned on the fight against fraud and the protection of digital identities I (presentation only)
Julian White, Alastair Treharne (Cabinet Office, UK)

3. Lessons learned on the fight against fraud and the protection of digital identities II (presentation only)
Julian White, Alastair Treharne (Cabinet Office, UK)

14:00 – 14:30 Coffee Break – Poster Session & Get2Gether

14:30 – 15:15 Plenary Session

ARES EU Symposium Keynote

Location: Lecture Hall H
Time: 14:30-15:15

Cyber-Legislation, Standardisation and Pan-European Cooperation as strategic drivers to strengthen Cybersecurity across Europe
Thomas C. Stubbings (Thomas Stubbings Management Consulting eU, Austria)

Abstract: The ever-increasing interconnection of societies, businesses and individuals has led to a new level of cyber threats: organised crime, fraud and cyber terrorism have a direct and tangible impact on the way we live, work and do business. The evolving threat landscape demands for new strategies of cyber protection. As part of the digital single market strategy the European Commission has developed a Cybersecurity strategy in order to foster an open, safe and secure cyberspace and digital sovereignty. Elements of this strategy are closer cooperation of member states and key stakeholders, establishment of a suitable cybersecurity legal basis and development of a security ecosystem of European standards, service offerings and service providers. The presentation will outline the current situation and key elements of the approach to strengthen Cybersecurity and manage risks at an appropriate level.

15:15 – 16:45 Parallel Sessions

SECODIC III – Private and Secure Processing in the Cloud

Session Chair: Matthias Neugschwandtner (IBM, Switzerland)
Location: Lecture Hall C
Time: 15:15-16:45

1. Challenges for Isolating Computational Resources in Cloud Software Stacks (presentation only)
Matthias Neugschwandtner (IBM Research, Switzerland)

2. Hardware Assisted Fully Homomorphic Function Evaluation (presentation only)
Sujoy Sinha Roy (Ku Leuven, Belgium)

3. Malleable Cryptography for Security and Privacy in the Cloud (presentation only)
Daniel Slamanig (Graz University of Technology, Austria)

4. Networking session

SENCEC I

Session Chair: Evaldas Bruze (Lithuanian Cybercrime Centre of Excellence for Training, Research & Education (L3CE), Lithuania)
Location: Lecture Hall D
Time: 15:15-16:45

1. Possibilities for Synergies: SENTER project (presentation only)
Evaldas Bruze (*Lithuanian Cybercrime Centre of Excellence for Training, Research & Education (L3CE), Lithuania*)

2. SENTER: the way to better cooperation (presentation only)
Evaldas Bruze (*Lithuanian Cybercrime Centre of Excellence for Training, Research & Education (L3CE), Lithuania*)

3. Partnership with key stakeholders (presentation only)
Evaldas Bruze (*Lithuanian Cybercrime Centre of Excellence for Training, Research & Education (L3CE), Lithuania*)

RESIST I

Session Chair: Christian Probst (Technical University of Denmark, Denmark)
Location: Lecture Hall E
Time: 15:15-16:45

1. Risk Assessment for Socio-technical Security Models (presentation only)
Christian W Probst (Technical University of Denmark, Denmark)

2. Modelling Socio-Technical Systems (presentation only)
Christian W Probst (Technical University of Denmark, Denmark)

3. Data Collection (presentation only)
Axel Tanner (IBM Research, Switzerland)

4. Quantitative Analysis of Attacks (presentation only)
Jaco van de Pol (University of Twente, Netherlands)

5.The TREsPASS Process for Risk Assessment (presentation only)
Jan Willemson (Cybernetica)

FASES III – Novel methods for authentication, identification and certificates issuance

Session Chair: Sara Hajian (Eurecat - Technology Centre of Catalonia, Spain)
Location: Lecture Hall F
Time: 15:15-16:45

1. Ensuring the Authenticity and Fidelity of Captured Photos Using Trusted Execution and Mobile Application Licencing Capabilities
Kwstantinos Papadamou, Riginos Samaras and Michael Sirivianos (Cyprus University of Technology, Cyprus)

Abstract: Mobile devices, which users habitually carry along, have become the main data gateway for the majority of the online services. Any device is able to collect at any time various types of data through its sensors. At the same time, modern identification techniques ask users to send photos of their ID documentation in order to be verified by an online service. Those photos are captured by the device's camera and are considered extremely sensitive. They must be secured and establish that they will not be modified. This paper describes a security framework that preserves the authenticity of a captured photo and ensures that it remains intact while transferred to a remote server. The key inside is to use a background service that is tied to the photo-capturing application and uses secure key storing and cryptographic computation capabilities offered by the Trusted Execution Environment (TEE) of commodity Android devices. At the same time, we leverage Playstore's Licencing Verification Library (LVL) to remotely attest the authenticity of the photo-capturing application at registration time. We have implemented our framework as an Android application on a Nexus 5X, which is powered by a Qualcomm processor with ARM TrustZone Technology. The evaluation of our prototype implementation demonstrates the efficacy of the proposed framework in terms of performance overhead and usability

2. FEBA: An Action-Based Feature Extraction Framework for Behavioural Identification and Authentication

Luigi Stammati, Claudio Pisa, Tooska Dargahi, Alberto Caponi and Giuseppe Bianchi (University of Rome "Tor Vergata", Italy)

Abstract: While the usage of behavioral features for authentication purposes is gaining more and more consensus in the community, there is less consensus on which specific behavioral traits may be useful in eventually different settings. This calls for flexible tools which the application developer can leverage to automate the extraction and management of behavioral features for identification and authentication. This paper specifically describes a framework called FEBA (Feature Extraction Based on Action), which to the best of our knowledge is the first open-source framework that provides the developer with simple and flexible means to: i) define application-specific actions, ii) recognize actions based on the received raw data, and iii) finally extract the action-specific features. We have built a complete implementation of FEBA, and made it available online to facilitate future research in such context. To prove the performance of FEBA, we provide an experimental evaluation of a use case scenario, i.e., mouse movements feature extraction and pattern recognition. We believe that FEBA will help researchers and developers to design and implement novel behavioral authentication mechanisms.

3. Automated issuance of digital certificates through the use of federations

Thaís Bardini Idalino (University of Ottawa, Canada), Marina Da Silva Coelho and Jean Everson Martina (Universidade Federal de Santa Catarina, Brazil)

Abstract: In recent years, there has been a trend for developing single sign-on systems. One alternative to deploy such systems is the use of Federated Identity Management systems. We argue that it is possible to use identity federations to automate the digital certificate issuance and use these certificates to authenticate back into federations. We use the data provided by the user's identity provider to build his certificate, reducing the costs of maintaining several registration authorities and simplifying the certificate issuance process. Making the process simpler to the users, we also encourage them to request and use their certificates. In special, the use of digital certificates for authentication can improve the usability and security of the authentication process. Furthermore, we present a prototype proving the feasibility of our proposal, as well as a discussion of the security and potential applications.

MUININ I

Session Chair: Shane Finan (Trinity College Dublin, Ireland)
Location: Lecture Hall G
Time: 15:15-16:45

1. Introduction (project overview and current status):
Slándáil Project, Emergency Management and Social Media Monitor

Shane Finan (Trinity College Dublin, Ireland)

2. Emergency Management and Social Media Monitor Implementation:
The Slandail: Monitor Real-time Processing and Visualisation of Social Media Data for Emergency Management

Xiubo Zhang, Stephen Kelly and Khurshid Ahmad (Trinity College Dublin, Ireland)

Abstract: The use of social media platforms has grown dramatically in recent times. Combined with the rise of mobile computing, users are now more connected and spend more of their time online. Social media has been used during emergency events where the public and authorities have used it as a form of communication and to receive information. Due to this, emergency managers and first responders can use this information to increase their awareness about an ongoing crisis and aid decision making. The challenge here lies in processing this deluge of information and filtering it for insights that are useful for this purpose. This paper presents the Slandail Monitor, a system for harvesting and filtering a social media stream for emergency related social media data. Spatial and temporal data attached to each message are used with the analysed content of each message to summarize ongoing emergency events as reported on social media. This information is combined with a visualization component to allow a user to quickly assess an event by location, time, and by topic. Issues about ethical data harvesting and privacy are also addressed by the system in a computational way by logging potentially sensitive information in the Intrusion Index.

3. Legal and Ethical Use of Data in Emergency Response:
a. Ensuring Security of Data and Information Flow in Emergency Response Decision Support

Damian Jackson and Paul Hayes (Trinity College Dublin, Ireland)

Abstract: Harvested social media data has the potential to enhance emergency response decision support if its reliability can be assessed. We are working on an EU-FP7 project called Sláindáil (Project No. 607691). Sláindáil aims to develop a prototype system which automates social media data analysis for emergency response. This paper considers some of the ethical concerns that may arise with such alternate use of data. It offers technical (hardware and software) and operational measures intended to improve the security of data and information flow to mitigate those risks.

b. Legal Implications of Using Social Media in Emergency Response

Christian Berger (Leipzig University, Germany), Paolo De Stefani (University of Padova, Italy) and Taiwo Oriola (Ulster University, UK)

Abstract: Slandail is a software prototype designed for use and exploitation of digital content on social media for emergency and disaster management. This will involve the collection, reproduction, distribution, transfer, processing and, potentially, communication to the public of harvested personal data and information by emergency responders. However, the use of a system such as Slandail would have implications for the laws protecting human rights, personal data, and copyright within and outside of the European Union. This paper provides a brief overview of these laws, and the challenges they pose to the development of the Slandail software prototype, with part one focusing on data protection; part two on human rights; and part three on copyright and licensing rights

4. End User Communication Practice:
Disaster-related Public Speeches: The Role of Emotions

Khurshid Ahmad and Maria Spyropoulou (Trinity College Dublin, Ireland)

Abstract: Disaster managers are dealing with serious situations and their speeches should be factual yet empathetic; they should be objective yet show restraint. Nowadays messages to the public for the preparedness or the recovery phase of a crisis from disaster managers are disseminated through formal and social media, where the authorities delivering them appear surrounded by specialists. The common perception is that words uttered by these managers are the key, no matter how the person is perceived. The focus of technology has been on textual analytics and the acoustic quality of the deliverer's voice. However human beings tend to fuse the verbal information with the nonverbal aspect of communication, like tone of voice and facial expressions. Facial expressions are used in human communication to express the affect and attitudes of the speaker. The human aggregation process fuses data from video stream and audio stream together with the emotion stream (anger, joy, fear..). Our analysis deals with the observation of facial muscle movements- emotion proxies on face. This paper describes an important contribution to safety and security in disasters, specifically in disaster management and public communications. This initial study is based on four political authorities and their speeches.

16:30 – 17:00 Coffee Break – Poster Session & Get2Gether

17:00 – 18:00 Parallel Sessions

SECODIC IV – Integrity and Verifiability of Outsourced Data/Computation

Session Chair: Melek Önen (Eurecom, France)
Location: Lecture Hall C
Time: 17:00-18:00

1. Verifiable Polynomial Evaluation & Matrix Multiplication (presentation only)

Melek Önen (EURECOM, France)

2. Verifiable searchable encryption (presentation only)

James Alderman (Royal Holloway University of London, UK)

3.Workshop wrap-up

RESIST II

Session Chair: Christian Probst (Technical University of Denmark, Denmark)
Location: Lecture Hall E
Time: 17:00-18:00

1. The TREsPASS Attack Navigator including Demonstration (presentation only)

Christian W Probst (Technical University of Denmark, Denmark)

2. Wrap-up

MUININ II

Session Chair: Shane Finan (Trinity College Dublin, Ireland)
Location: Lecture Hall G
Time: 17:00-18:00

1. Advanced Image and Text Analysis: Project Progress:

a. The Application of Social Media Image Analysis to an Emergency Management System

Min Jing, Bryan Scotney, Sonya Coleman (Ulster University, UK) and Martin McGinnity (Nottingham Trent University, UK)

Abstract: The emergence of social media has provided vast amounts of information that is potentially valuable for emergency management. In the EU-FP7 Project Security Systems for Language and Image Analysis (Slandail), an image analysis system has been developed to recognize the flood water images from the social media resources by incorporating with text analysis. A novel image feature descriptor has been developed to facilitate fast image processing based on incorporation of the "Squiral" (Square-Spiral) Image Processing (SIP) framework with the "Speeded-up Robust Features" (SURF). A new approach is proposed to generate an index from image recognition outcomes based on a moving window average, which presents a temporal change based on the occurrence of flooding water identified by image analysis. The evaluation for computation time and recognition were based on a batch of images obtained from the US Federal Emergency Management Agency (FEMA) media library and Facebook corpus from Germany, and the outcomes show the advantages of the proposed image features. The simulation results demonstrate the concept of the index based on a moving window average, highlighting the potential for application in emergency management.

b. Computational, Communicative, and Legal Conditions for Using Social Media in Disaster Management in Germany

Sabine Gründer-Fahrer (Institute for Applied Informatics e.V., Germany), Christian Berger (University of Leipzig, Germany), Antje Schlaf (Institute for Applied Informatics e.V., Germany) and Gerhard Heyer (University of Leipzig, Germany)

Abstract: During the flood in 2013 in Germany and Austria, the engagement of volunteers was the highest ever known. Notably, these volunteers organized themselves mainly via social media and without being motivated or guided by professional management. The present paper wants to provide input and positive impulse for current discussions among the public authorities how to become more present in social networks and take benefit of their strength. By means of a corpus-based case study of German Facebook and Twitter messages during the flood in 2013, we show and analyze the real potential of social media for disaster management and reveal some of their communicative characteristics. At the same time, we discuss two of the main challenges, namely information overload and legal issues. Regarding the problem of information overload the paper shows by case of an example from state-of-the-art automatic language processing (topic model analysis), that today it is possible to establish the technical basis required to get efficient and flexible computer-based access to information in social media. With respect to the legal conditions of social media use in disaster management, paper is to give a concise overview of the current legal situation using Saxony as an example, to identify open problems and to present proposals for their potential solution.

2. Conclusion:

Final notes from Project Coordinator, Khurshid Ahmad

18:00 – 22:00 Welcome Reception

Welcome Reception will take place in a rustic setting at the Zistelalm, which is located on the mountain outside of the city. You will get the possibility to try typical Austrian dishes such as "Kasnocken" served in big pans. We are happy to announce that Dr. Pallauf, president of Salzburg´s state parliament, will give a speech during the welcome reception.

Meeting point: in front of the University, buses leave 18.15 (shortly after the last session)

Buses will take us from the university to the Zistelalm and later back to the city (the restaurant is not located in the city center).

ARES Conference – Wednesday, August 31, 2016

08:00 – 18:00 Registration desk open

09:00 – 09:15 Opening

09:15 – 10:15 Plenary Session

Keynote

Location: Lecture Hall A
Time: 09:15 – 10:15

International Judicial Cooperation in the Fight against Cybercrime

Koen Hermanns, EUROJUST, The European Union's Judicial Cooperation Unit

10:15 – 10:30 short Coffee Break

10:30 – 12:00 Parallel Sessions

ARES Full I – Best Paper Session

Session Chair: Dominik Engel (Salzburg University of Applied Sciences Austria)
Location: Lecture Hall A
Time: 10:30-12:00

1. A recommender-based system for assisting non-technical users in managing Android permissions

Arnaud Oglaza, Romain Laborde, Francois Barrere and Abdelmalek Benzekri (University of Toulouse, France)

Abstract: Today, permissions management solutions on mobile devices employ Identity Based Access Control (IBAC) models. If this approach was suitable when people had only a few games (like Snake or Tetris) installed on their mobile phones, the current situation is different. A survey from Google in 2013 showed that, on average, US users have installed 33 applications on their Android smartphones. As a result, these users must manage hundreds of permissions to protect their privacy. Scalability of IBAC is a well-known issue and many more advanced access control models have introduced abstractions to cope with this problem. However, such models are more complex to handle by non-technical users. Thus, we present a permission management system for Android devices that 1) learns users' privacy preferences, 2) proposes them abstract authorization rules, and 3) provides advanced features to manage these high-level rules. We prove this approach is more efficient than current permission management system by comparing it to Privacy Guard Manager.

2. No Need for Black Chambers: Testing TLS in the E-mail Ecosystem at Large

Wilfried Mayer, Aaron Zauner, Martin Schmiedecker (SBA Research, Austria) and Markus Huber (FH St. Pölten, Austria)

Abstract: TLS is the most widely used cryptographic protocol on the Internet today. While multiple recent studies focused on its use in HTTPS and the adoption rate of additional security measures over time, the usage of TLS in e-mail-related protocols is still lacking detailed insights. End-to-end encryption mechanisms like PGP are seldomly used, and as such today's confidentiality in the e-mail ecosystem is based entirely on the encryption of the transport layer. However, a large fraction of e-mails is still transmitted unencrypted, which is highly disproportionate with the sensitive nature of e-mail communication content. A well-positioned attacker may be able to intercept plaintext communication content as well as communication metadata passively and at ease. We are the first to collect and analyze the complete state of today's e-mail-related TLS configuration, for the entire IPv4 address range. Our methodology is based on commodity hardware and open-source software, and we draw a comprehensive picture of the current state of security mechanisms on the transport layer for e-mail by scanning cipher suite support which was previously considered impossible due to numerous constraints. We collected and scanned a massive dataset of 20 million IP/port combinations of all e-mail-related protocols (SMTP, POP3, IMAP). Over a time span of approx. three months we conducted more than 10 billion TLS handshakes. Additionally, we show that securing server-to-server communication using e.g. SMTP is inherently more difficult than securing client-to-server communication, and that while the overall trend points in the right direction there are still many steps needed towards secure e-mail.

3. Revisiting a Watermark-based Detection Scheme to Handle Cyber-Physical Attacks

Jose Manuel Rubio Hernan, Luca De Cicco (Politecnico di Bari, Italy) and Joaquin Garcia-Alfaro (Télécom SudParis, France)

Abstract: We address detection of attacks against cyber physical systems. Cyber-physical systems are industrial control systems upgraded with novel computing, communication and interconnection capabilities. In this paper we reexamine the security of a detection scheme proposed by Mo and Sinopoli (2009) and Mo et al. (2015). The approach complements the use of Kalman filters and linear quadratic regulators, by adding an authentication watermark signal for the detection of integrity attacks. We show that the approach only detects cyber adversaries, i.e., attackers with the ability to eavesdrop information from the system, but that do not attempt to acquire any knowledge about the system model itself. The detector fails at covering cyber-physical adversaries, i.e., attackers that, in addition to the capabilities of the cyber adversary, are also able to infer the system model to evade the detection. We discuss an enhanced scheme, based on a multi-watermark authentication signal, that properly detects the two adversary models.

12:00 – 13:00 Lunch – Poster Session & Get2Gether

13:00 – 14:30 Parallel Sessions

ARES Full II – Cryptography

Session Chair: Edgar Weippl (SBA Research, Austria)
Location: Lecture Hall A
Time: 13:00-14:30

1. Byzantine Set-Union Consensus using Efficient Set Reconciliation

Florian Dold and Christian Grothoff (INRIA, France)

Abstract: Applications of secure multiparty computation such as certain electronic voting or auction protocols require Byzantine agreement on large sets of elements. Implementations proposed in the literature so far have relied on state machine replication, and reach agreement on each individual set element in sequence. We introduce set-union consensus, a specialization of Byzantine consensus that reaches agreement over whole sets. This primitive admits an efficient and simple implementation by the composition of Eppstein's set reconciliation protocol with Ben-Or's ByzConsensus protocol. A free software implementation of this construction is available in GNUnet. Experimental results indicate that our approach results in an efficient protocol for very large sets, especially in the absence of Byzantine faults. We show the versatility of set-union consensus by using it to implement distributed key generation, ballot collection and cooperative decryption for an electronic voting protocol implemented in GNUnet.

2. k -time Full Traceable Ring Signature

Xavier Bultel and Pascal Lafourcade (Universite Clermont Auvergne, France)

Abstract: Ring and group signatures allow their members to anonymously sign documents in the name of the group. In ring signatures, members manage the group themselves in an adhoc manner while in group signatures, a manager is required. Moreover, k-times traceable group and ring signatures [1] allow anyone to publicly trace two signatures from a same user if he exceeds the a priori authorized number of signatures. In [2], Canard et al. give a 1-time traceable ring signature where each member can only generate one anonymous signature. Hence, it is possible to trace any two signatures from the same user. Some other works generalize it to the k-times case, but the traceability only concerns two signatures. In this paper, we define the notion of k-times full traceable ring signature (k-FTRS) such that all signatures produced by the same user are traceable if and only if he produces more than k signatures. We construct a k-FTRS called Ktrace. We extend existing formal security models of ktimes linkable signatures to prove the security of Ktrace in the random oracle model. Our primitive k-FTRS can be used to construct a k-times veto scheme or a proxy e-voting scheme that prevents denial-of-service caused by cheating users.

3. Towards Cycle-Accurate Emulation of Cortex-M Code to Detect Timing Side Channels

Johannes Bauer and Felix Freiling (FAU,Germany)

Abstract: Leakage of information through timing side channels is a problem for all sorts of computing machinery, but the impact of such channels is especially dramatic on embedded systems. The reason for this is that these environments allow attackers to exploit small timing differences down to clock cycle accuracy. On the defensive side it is therefore advisable to evaluate cautiously if security-critical code contains data dependent timing discrepancies. When working with real hardware, testing for such vulnerabilities is a tedious process. In order to reduce the burden of vetting, we study approaches that allow cycle-accurate behavioral emulation of relevant CPU behavior such as instruction pipeline flushes and bus contention. We show that our approach is feasible and efficient by implementing an emulator of the popular ARM Cortex-M core. Then we give an overview about the problems of cycle-accurate emulation and demonstrate our approach towards a cycleaccurate ARM Thumb-2 simulator. Finally,

we show how this simulator can be integrated into the build process of firmware to check for the presence of timing side channels before the system is deployed.

CD ARES I – Web and Semantics

Session Chair: Peter Kieseberg (SBA Research, Austria)
Location: Lecture Hall B
Time: 13:00-14:30

1. Algebra of RDF Graphs for Querying Large-Scale Distributed Triple-Store

Iztok Savnik (University of Primorska, Slovenia) and Kiyoshi Nitta (Yahoo JAPAN Research, Japan)

Abstract: Large-scale RDF graph databases stored in shared-nothing clusters require query processing engine that can effectively exploit highly parallel computation environment. We propose algebra of RDF graphs and its physical counterpart, physical algebra of RDF graphs, designed to implement queries as distributed dataflow programs that run on cluster of servers. Operations of algebra reflect the characteristic features of RDF graph data model while they are tied to the technology provided by relational query execution systems. Algebra of RDF graphs allows for the expression of pipelined and partitioned parallelism. Preliminary experimental results show that proposed algebra and architecture of query execution system scale well with large clusters of data servers.

2. Your Paper has been Accepted, Rejected, or whatever: Automatic Generation of Scientific Paper Reviews

Alberto Bartoli, Andrea De Lorenzo, Eric Medvet and Fabiano Tarlao (University of Trieste, Trieste, Italy)

Abstract: Peer review is widely viewed as an essential step for ensuring scientific quality of a work and is a cornerstone of scholarly publishing. On the other hand, the actors involved in the publishing process are often driven by incentives which may, and increasingly do, undermine the quality of published work, especially in the presence of unethical conduits. In this work we investigate the feasibility of a tool capable of generating fake reviews for a given scientific paper automatically. While a tool of this kind cannot possibly deceive any rigorous editorial procedure, it could nevertheless find a role in several questionable scenarios and magnify the scale of scholarly frauds. A key feature of our tool is that it is built upon a small knowledge base, which is very important in our context due to the difficulty of finding large amounts of scientific reviews. We experimentally assessed our method 16 human subjects. We presented to these subjects a mix of genuine and machine generated reviews and we measured the ability of our proposal to actually deceive subject's judgment. The results highlight the ability of our method to produce reviews that often look credible and may subvert the decision.

3. Generic UIs for requesting complex products within Distributed Market Spaces in the Internet of Everything

Michael Hitz (Baden-Wuerttemberg Cooperative State University Stuttgart, Germany) Mirjana Radonjic-Simic, Julian Reichwald (Baden-Wuerttemberg Cooperative State University Mannheim, Germany) and Dennis Pfisterer (University of Lübeck, Germany)

Abstract: Distributed Market Spaces (DMS), refer to an exchange environment in emerging Internet of Everything that supports users in making transactions of complex products; a novel type of products made up of different products and/or services that can be customized to better fit the individual context of the user. In order to express their demand for a particular complex product in a way that is interpretable by the DMS, users need flexible User Interfaces (UIs) that allow context-focused data collection related to the complexity of the user's demand. This paper proposes a concept for generic UIs that enables users to compose their own UIs for requesting complex products, by combining existing UI descriptions for different parts of the particular complex product, as well as to share and improve UI descriptions among other users within the markets.

14:30 – 15:00 Coffee Break

15:00 – 16:30 Parallel Sessions

ARES Full III – Network and Software Security

Session Chair: Sebastian Schrittwieser (Josef Ressel Zentrum TARGET, St. Pölten University of Applied Sciences, Austria)
Location: Lecture Hall A
Time: 15:00-16:30

1. POTR: Practical On-the-fly Rejection of Injected and Replayed 802.15.4 Frames

Konrad-Felix Krentz, Christoph Meinel (Hasso-Plattner-Institut, Germany) and Maxim Schnjakin (Bundesdruckerei, Germany)

Abstract: The practice of rejecting injected and replayed 802.15.4 frames only after they were received leaves 802.15.4 nodes vulnerable to broadcast and droplet attacks. Basically, in broadcast and droplet attacks, an attacker injects or replays plenty of 802.15.4 frames. As a result, victim 802.15.4 nodes stay in receive mode for extended periods of time and expend their limited energy. He et al. considered embedding one-time passwords in the synchronization headers of 802.15.4 frames so as to avoid that 802.15.4 nodes detect injected and replayed 802.15.4 frames in the first place. However, He et al.'s, as well as similar proposals lack support for broadcast frames and depend on special hardware. In this paper, we propose Practical On-the-fly Rejection (POTR) to reject injected and replayed 802.15.4 frames early during receipt. Unlike previous proposals, POTR supports broadcast frames and can be implemented with many off-the-shelf 802.15.4 transceivers. In fact, we implemented POTR with CC2538 transceivers, as well as integrated POTR into the Contiki operating system. Furthermore, we demonstrate that, compared to using no defense, POTR reduces the time that 802.15.4 nodes stay in receive mode upon receiving an injected or replayed 802.15.4 frame by a factor of up to 16. Beyond that, POTR has a small processing and memory overhead, and incurs no communication overhead.

2. Stopping amplified DNS DDoS attacks through query rate sharing between DNS resolvers

Saurabh Verma (University of Minnesota, US), Ali Hamieh (Rutgers University, US), Jun Ho Huh (Honeywell ACS Labs, US), Henrik Holm (Forest Glen Research, LLC, US), Siva Raj Rajagopalan (Honeywell ACS Labs, US), Nina Fefferman (Rutgers University, US) and Maciej Korczynski (Delft University of Technology, Netherlands)

Abstract: An Amplified DNS DDoS (ADD) attack involves tens of thousands of DNS resolvers that send huge volumes of amplified DNS responses to a single victim host, quickly flooding the victim's network bandwidth. Because ADD attacks are distributed, it is difficult for individual DNS resolvers to detect them based on local DNS query rates alone. Even if a victim detects an ADD attack, it cannot stop the attacker from flooding its network bandwidth. To address this problem, we present a novel mitigation system called "Distributed Rate Sharing based Amplified DNS-DDoS Attack Mitigation" (DRSADAM). DRS-ADAM facilitates DNS query rate sharing between DNS resolvers that are involved in an attack to detect and completely stop an ADD attack. Each DNS resolver quickly builds the global DNS query rate for potential victims by accumulating the shared rate values, and uses that global rate to make mitigation decisions locally. DRS-ADAM can be easily deployed through a small software update on resolvers and victim hosts, and does not require any additional server component. Our simulation results show that DRS-ADAM can contain the peak attack rates close to a victim's acceptable threshold values (which are far smaller than their sustainable bandwidth) at all times, regardless of the number of resolvers involved in ADD attacks. ADD attacks can be fully mitigated within a few seconds.

3. HyperCrypt: Hypervisor-based Encryption of Kernel and User Space

Johannes Götzfried, Nico Dörr, Ralph Palutke and Tilo Müller (FAU, Germany)

Abstract: We present HyperCrypt, a hypervisor-based solution that encrypts the entire kernel and user space to protect against physical attacks on main memory, such as cold boot attacks. HyperCrypt is fully transparent for the guest operating system and all applications running on top of it. At any time, only a small working set of memory pages remains in clear while the vast majority of pages are constantly kept encrypted. By utilizing CPU-bound encryption, the symmetric encryption key is never exposed to RAM. We evaluated our prototype running a standard Linux system with an nginx web server. With the default configuration of 1024 clear text pages, successful cold boot attacks are rendered highly unlikely due to large caches of at least 4 MB in modern CPUs. The performance overhead of nginx is raised by factor 1.37 compared to a non-virtualized system.

CD ARES II – Diagnosis, Prediction and Machine Learning

Session Chair: Andreas Holzinger (Holzinger Group HCI-KDD, Austria)
Location: Lecture Hall B
Time: 15:00-16:30

1. Diagnosis of complex active systems with uncertain temporal observations

Gianfranco Lamperti (University of Brescia, Italy) and Xiangfu Zhao (Zhejiang Normal University, China)

Abstract: Complex active systems have been proposed as a formalism for modeling real dynamic systems that are organized in a hierarchy of behavioral abstractions. As such, they constitute a conceptual evolution of active systems, a class of discrete-event systems introduced into the literature two decades ago. A complex active system is a hierarchy of active systems, each one characterized by its own behavior expressed by the interaction of several communicating automata. The interaction between active systems within the hierarchy is based on special events, which are generated when specific behavioral patterns occur. Recently, the task of diagnosis of complex active systems has been studied, with an efficient diagnosis technique being proposed. However, the observation of the system is assumed to be linear and certain, which turns out to be an over-assumption in real, large, and distributed systems. This paper extends diagnosis of complex active systems to cope with uncertain temporal observations. An uncertain temporal observation is a DAG where nodes are marked by candidate labels (logical uncertainty), whereas arcs denote partial temporal ordering between nodes (temporal uncertainty). By means of indexing techniques, despite the uncertainty of temporal observations, the intrinsic efficiency of the diagnosis task is retained in both time and space.

2. A Cloud-based Prediction Framework for Analyzing Business Process Performances

Eugenio Cesario, Francesco Folino, Massimo Guarascio and Luigi Pontieri (National Research Council of Italy, Italy)

Abstract: This paper presents a framework for analyzing and predicting the performances of a business process, based on historical data gathered during its past enactments. The framework hinges on an inductive-learning technique for discovering a special kind of predictive process models, which can support the runtime prediction of some performance measure (e.g., the remaining processing time or a risk indicator) for an ongoing process instance, based on a modular representation of the process, where major performance-relevant variants of it are equipped with different regression models, and discriminated through context variables. The technique is an original combination of different data mining methods (namely, non-parametric regression methods and a probabilistic trace clustering scheme) and ad hoc data transformation mechanisms, meant to bring the log traces to suitable level of abstraction. In order to overcome the severe scalability limitations of current solutions in the literature, and make our approach really suitable for large logs, both the computation of the trace clusters and of the clusters' predictors are implemented in a parallel and distributed manner, on top of a cloud-based service-oriented infrastructure. Tests on a real-life log confirmed the validity of the proposed approach, in terms of both effectiveness and scalability.

3. Towards Interactive Machine Learning: Applying Ant Colony Algorithms to Solve the Traveling Salesman Problem with the human-in-the-loop approach

Andreas Holzinger, Markus Plass, Katharina Holzinger (Holzinger Group HCI-KDD, Austria), Gloria Crisan (Vasile Alecsandri University of Bacău, Romania), Camelia Pintea (Technical University of Cluj-Napoca, Romania) and Vasile Palade (Coventry University, UK)

Abstract: Most Machine Learning (ML) researchers focus on automatic Machine Learning (aML) where great advances have been made, for example, in speech recognition, recommender systems, or autonomous vehicles. Automatic approaches greatly benefit from the availability of ”big data”. However, sometimes, for example in health informatics, we are confronted not a small number of data sets or rare events, and with complex problems where aML-approaches fail or deliver unsatisfactory results. Here, interactive Machine Learning (iML) may be of help and the “human-in-the-loop” approach may be beneficial in solving computationally hard problems, where human expertise can help to reduce an exponential search space through heuristics. In this paper, experiments are discussed which help to evaluate the effectiveness of the iML-”human-in-the-loop” approach, particularly in opening the ”black box”, thereby enabling a human to directly and indirectly manipulating and interacting with an algorithm. For this purpose, we selected the Ant Colony Optimization (ACO) framework, and use it on the Traveling Salesman Problem (TSP) which is of high importance in solving many practical problems in health informatics, e.g. in the study of proteins.

16:30 – 17:00 Coffee Break

17:00 – 18:00 Parallel Sessions

ARES Full IV – Privacy-Enhancing Technologies

Session Chair: Daniel Slamanig (Graz University of Technology, Austria)
Location: Lecture Hall A
Time: 17:00-18:00

1. Efficient and Privacy Preserving Third Party Auditing for a Distributed Storage System

Denise Demirel, Giulia Traverso (TU Darmstadt, Germany), Stephan Krenn and Thomas Lorunser (AIT, Austria)

Abstract: When using distributed storage systems to outsource data storage into the cloud, it is often vital that this is done in a privacy preserving way, i.e., without the storage servers learning anything about the stored data. Especially when storing critical data, one often further requires efficient means to check whether the data is actually stored correctly on these servers. In the best case, such an auditing could itself be outsourced to a third party which does not need to be trusted by the data owner. That is, also the auditing mechanism should guarantee privacy, even if the auditor collaborates with a (sub) set of the storage servers. However, so far only a small number of privacy preserving third party auditing mechanisms has been presented for single server storage solutions, and no such protocols exist at all for a distributed storage setting. In this paper, we therefore define and instantiate a privacy preserving auditable distributed storage system. Our instantiation can be based on any homomorphic secret sharing scheme, and is fully keyless, efficient, and information-theoretically private. Furthermore, it supports batch audits, and is backward compatible with existing secret sharing based storage solutions.

2. Introducing Proxy Voting to Helios

Oksana Kulyk, Karola Marky, Stephan Neumann and Melanie Volkamer (TU Darmstadt, Germany)

Abstract: Proxy voting is a form of voting, where the voters can either vote on an issue directly, or delegate their voting right to a proxy. This proxy might for instance be a trusted expert on the particular issue. In this work, we extend the widely studied end-to-end verifiable Helios Internet voting system towards the proxy voting approach. Therefore, we introduce a new type of credentials, so-called delegation credentials. The main purpose of these credentials is to ensure that the proxy has been authorized by an eligible voter to cast a delegated vote. If voters, after delegating, change their mind and want to vote directly, cancelling a delegation is possible throughout the entire voting phase. We show that the proposed extension preserves the security requirements of the original Helios system for the votes that are cast directly, as well as security requirements tailored toward proxy voting.

CD ARES III – Security and Privacy

Session Chair: Angelo Furfaro (University of Calabria, Italy)
Location: Lecture Hall B
Time: 17:00-18:00

1. A threat to friendship privacy in Facebook

Francesco Buccafurri, Gianluca Lax, Serena Nicolazzo and Antonino Nocera (University Mediterranea of Reggio Calabria, Italy)

Abstract: The rapid growth of social networks, primarily Facebook, has coincided with an increasing concern over personal privacy. This explains why more and more users personalize their Facebook privacy settings. As a matter of fact, the list of friends is often one of the profile sections kept private, meaning that this information is perceived as sensible. In this paper, we study the robustness of this privacy protection feature, showing that it can be broken even in the less advantageous conditions for the adversary. To do this, we exploit both the potential information extracted from user alter accounts in Twitter and a social network property, recently demonstrated for Twitter, called interest assortativity. The preliminary experimental results reported in this paper, give a first evidence of the effectiveness of our attack, which succeeds even in the most difficult case that is when the information about the victim are minimum.

2. A Blockcipher based Authentication Encryption

Rashed Mazumder (Japan Advanced Institute of Science and Technology, Japan), Atsuko Miyaji and Chunhua Su (Osaka University, Japan)

Abstract: Authentication encryption (AE) is a procedure that satisfies both privacy and authenticity on the data. It has many applications in the field of secure data communication such as digital signatures, ip-security, data-authentication, e-mail security, and security of pervasive computing. Additionally, the AE is a potential primitive of security solution for IoT-end device, RfID, and constrained device. Though there are many constructions of AE, but the most important argument is whether the AE is secure under nonce-reuse or nonce-respect. As far our understanding, the McOE is the pioneer construction of nonce-reuse AE. Following that, many schemes have been proposed such as APE, PoE, TC, COPA, ElmE, ElmD, COBRA, and Minalphar. However, Hoang et. al. (OAE1) claimed that the concept of nonce-reuse in the AE is not secure and proper. Hence, a door is re-opened for the nonce-respect AE. Moreover, the construction of AE should satisfies the properties of efficiency and upper security bound due to limitation of power and memory for the constrained device. Therefore, we propose a blockcipher based AE that satisfies upper privacy security bound (Priv = 0(22n/3)) and it operates in parallel mode. It doesn't need decryption oracle in the symmetric encryption module of the AE. The proposed construction satisfies padding free encryption. Furthermore, the efficiency-rate of the proposed scheme is 1.

3. An Efficient Construction of a Compression Function for Cryptographic Hash

Rashed Mazumder (Japan Advanced Institute of Science and Technology, Japan), Atsuko Miyaji and Chunhua Su (Osaka University, Japan)

Abstract: A cryptographic hash (CH) is an algorithm that invokes an arbitrary domain of the message and returns fixed size of an output. The numbers of application of cryptographic hash are enormous such as message integrity, password verification, and pseudorandom generation. Furthermore, the CH is an efficient primitive of security solution for IoT-end devices, constrained devices, and RfID. The construction of the CH depends on a compression function, where the compression function is constructed through a scratch or blockcipher. Generally, the blockcipher based cryptographic hash is more applicable than the scratch based hash because of direct implementation of blockcipher rather than encryption function. Though there are many (n, 2n) blockcipher based compression functions, but most of the prominent schemes such as MR, Weimar, Hirose, Tandem, Abreast, Nandi, and ISA09 are focused for rigorous security bound rather than efficiency. Therefore, a more efficient construction of blockcipher based compression function is proposed, where it provides higher efficiency-rate including a satisfactory collision security bound. The efficiency-rate (r) of the proposed scheme is r ≈ 1. Furthermore, the collision security is bounded by q = 2125.84 (q = numer of query). Moreover, the proposed construction requires two calls of blockcipher under single iteration of encryption. Additionally, it has double key scheduling and its operational mode is parallel.

18:00 – 22:30 Welcome Reception

Our Welcome Reception will take place in a rustic setting at the Zistelalm, which is located on the mountain outside of the city. You will get the possibility to try typical Austrian dishes such as "Kasnocken" served in big pans. We are happy to announce that Dr. Pallauf, president of Salzburg´s state parliament, will give a speech during the welcome reception.

Meeting point: in front of the University, buses leave 18.15 (shortly after the last session)

Buses will take us from the university to the Zistelalm and later back to the city (the restaurant is not located in the city center).

Thursday, September 1, 2016

08:30 – 17:30 Registration desk open

09:30 – 11:00 Parallel Sessions

ARES Full V – Applications

Session Chair: Andreas Unterweger (Salzburg University of Applied Sciences, Austria)
Location: Lecture Hall A
Time: 09:30-11:00

1. ARTIST: The Android Runtime Instrumentation Toolkit

Lukas Dresel, Mykolai Protsenko and Tilo Müller (FAU, Germany)

Abstract: Smartphones are becoming more and more ubiquitous in the modern world, entrusted with such sensitive information as the user's location and banking data. Since Android is the most widespread smartphone platform, reliable and versatile means for Android application analysis are of great importance. Most of the existing code instrumentation approaches for Android suffer from two important shortcomings: the need for root access and limited support for the new Android Runtime (ART). We aim to fill this gap by proposing ARTIST, the Android Runtime Instrumentation Toolkit1. ARTIST is a framework that allows analysts to easily monitor the execution of Java and native code using native instrumentation techniques. ARTIST, to the best of our knowledge, is the first tool allowing monitoring of both native and Java code with the same instrumentation technique. ARTIST provides two methods to locate instrumentation targets. First, it can parse OAT executable files in memory to find classes and methods of interest. This allows monitoring a specific set of Java methods. Second, ARTIST can locate internal structures of the Android Runtime in memory. Monitoring function pointers found in these allows the user to track specific interactions of Java code with the Android Runtime. We evaluate the applicability of native instrumentation for Java code using a set of the most popular Android apps. The results show that over 80% of the tested Java methods are targetable using this approach. The performance impact, estimated with the CaffeineMark benchmark suite, does not exceed 20% and therefore can be considered generally acceptable.

2. Development of an AUTOSAR Compliant Cryptographic Library on State-of-the-Art Automotive Grade Controllers

Pal-Stefan Murvay, Cristina Solomon, Alexandru Matei and Bogdan Groza (Politehnica University Timisoara, Romania)

Abstract: In the light of the recently reported attacks on intra-vehicle networks, it has become clear that cryptography is vital for assuring the security of in-vehicle communications. The current preoccupation of industry professionals in this direction is proved by the inclusion of a comprehensive cryptographic extension in the recent-most version of the AUTOSAR (AUTomotive Open System ARchitecture) standard. In this work we try to give an answer on how prepared are current state-of-the-art automotive controllers for implementing cryptographic primitives and what is the exact cost of software implementations. We take into account automotive grade controllers that range from some of the most constrained platforms, e.g., from 8051 based tire sensors with 8-bit cores, up to 32-bit Infineon TriCore architectures, as well as devices that lay in between these two. We provide experimental results on several symmetric cryptographic primitives, i.e., block ciphers and hash functions, mainly focusing on the lightest constructions proposed in the literature, e.g., Speck, Katan, Blake, as well as on past or current standards, e.g., AES, SHA2 or SHA3. As expected, the results are sparse, some of the platforms being well prepared, capable to easily handle software implementation or carrying dedicated hardware, while for others no dedicated hardware exists while software implementation of current cryptographic standards cannot be handled, especially with the overhead incurred by the cohesion to the AUTOSAR standard.

3. Using Expert Systems to Statically Detect “Dynamic” conflicts in XACML

Bernard Stepien and Amy Felty (University of Ottawa, Canada)

Abstract: Policy specification languages such as XACML often provide mechanisms to resolve dynamic conflicts that occur when trying to determine if a request should be permitted or denied access by a policy. Examples include “deny-overrides” or “first-applicable.” Such algorithms are primitive and potentially a risk for corporate computer security. While they can be useful for resolving dynamic conflicts, they are not justified for conflicts that can be easily detected statically. It is better to find those at compile time and remove them before run time. Many different approaches have been used for static conflict detection. However, most of them do not scale well because they rely on pair-wise comparison of the access control logic of policies and rules. We propose an extension of a Prolog-based expert system approach due to Eronen and Zitting. This approach uses constraint logic programming techniques (CLP), which are well-adapted to hierarchical XACML policy logic and avoid pair-wise comparisons altogether by taking advantage of Prolog's built-in powerful indexing system. We demonstrate that expert systems can indeed detect conflicts statically, even those that are generally believed to only be detectable at run time, by inferring the values of attributes that would cause a conflict. As a result, relying on the XACML policy combining algorithms can be avoided in most cases except in federated systems. Finally we provide performance measurements for two different architectures represented in Prolog and give some analysis.

Workshop SAW I

Session Chair: Jungwoo Ryoo (Pennsylvania State University, USA)
Location: Lecture Hall C
Time: 09:30-11:00

1. Towards a Unified Secure Cloud Service Development and Deployment Life-cycle

Aleksandar Hudic, Philipp M. Radl, Thomas Lorünser (AIT, Austria), Matthias Flittner and Roland Bless (KIT, Germany)

Abstract: Designing and developing cloud services is a challenging task that includes requirements engineering, secure service deployment, maintenance, assurance that proper actions have been taken to support security and, in addition, considering legal aspects. This is unfortunately not possible by taking current methods and techniques into consideration. Therefore, we require a systematic and comprehensive approach for building such services that starts the integration of security concerns from early stages of design and development, and continuous to refines and integrate them in the deployment phase. In this paper we therefore propose a solution that integrates security requirements engineering and continuous refinement in a comprehensive security development and deployment lifecycle for cloud services and applications. Our approach is focused on iterative refinement of the security-based requirements during both software engineering (development phase) and software maintenance (deployment phase).

2. A Security Game Model for Remote Software Protection

Nicola Basilico, Andrea Lanzi and Mattia Monga (Universita degli Studi di Milano, Italy)

Abstract: When a piece of software is loaded on an untrusted machine it can be analyzed by an attacker who could discover any secret information hidden in the code. Software protection by continuously updating the components deployed in an untrusted environment forces a malicious user to restart her or his analyses, thus reducing the time window in which the attack is feasible. In this setting, both the attacker and the defender need to know how to direct their (necessarily limited) efforts. In this paper, we analyze the problem from a game theoretical perspective in order to devise a rational strategy to decide when and which orthogonal updates have to be scheduled in order to minimize the security risks of tampering. We formalize the problem of protecting a set of software modules and we cast it as a game. Since the update strategy is observable by the attacker, we show that the Leader-Follower equilibrium is the proper solution concept for such a game and we describe the basic method to compute it.

3. SPARER: Secure Cloud-Proof Storage for e-Health Scenarios

Gabriela Gheorghe, Muhammad Rizwan Asghar (University of Auckland, New Zealand), Jean Lancrenon and Sankalp Ghatpande (University of Luxembourg)

Abstract: With the surge of data breaches, practitioner ignorance and unprotected hardware, secure information management in healthcare environments is becoming a challenging problem. In the context of healthcare systems, confidentiality of patient data is of particular sensitivity. For economic reasons, cloud services are spreading, but there is still no clear solution to the problem of truly secure data storage at a remote location. To tackle this issue, we first examine if it is possible to have a secure storage of healthcare data without fully relying on trusted third-parties, and without impeding system usability on the side of the caregivers. The novelty of this approach is that it offers a standard-based deployable solution tailored for healthcare scenarios, using cloud services, but where trust is shifted from the cloud provider to the healthcare institution. This approach is unlike state-of-the-art solutions: there are secure cloud storage solutions that insist on having no knowledge of the stored data, but we discovered that they still require too much trust to manage user credentials; these credentials actually give them access to confidential data. In the paper, we present SPARER as a solution to the secure cloud storage problem and discuss the trade-offs of our approach. Moreover, we look at performance benchmarks that can hint to the feasibility and cost of using off-the-shelf cryptographic tools as building blocks in SPARER.

Workshop ASSD I – Secure DevOps

Session Chair: Lotfi Ben Othmane (Fraunhofer SIT, Germany)
Location: Lecture Hall D
Time: 09:30-11:00

1. Invited talk: How to include Security into Software Lifecycle: Secure DevOps!

Hasan Yasar (Carnegie Mellon University, US)

Abstract: As general thought, “Software security” often evokes negative feelings among software developers since this term is associated with additional programming effort, uncertainty and road blocker activity on fast development and release cycle. To secure software, developers must follow a lot of guidelines that, while intended to satisfy some regulation or other, can be very restricting and hard to understand. As a result a lot of fear, uncertainty, and doubt can surround software security. This talk describes how the Secure DevOps movement attempts to combat the toxic environment surrounding software security by shifting the paradigm from following rules and guidelines to creatively determining solutions for tough security problems. Emphasizing a set of DevOps principles enables developers to learn more about what they are developing and how it can be exploited. Rather than just blindly following the required security practices and identified security controls, developers can understand how to think about making their applications secure. As a result, they can derive their own creative ways to solve security problems as part of understanding the challenges associated with secure software development. Rather than reacting to new attacks, secure software should be proactively focused on surviving by providing reliable software with a reduced attack surface that is quick both to deploy and restore. In other words, developers worry less about being hacked and more about preventing predictable attacks and quickly recovering from cyber incident. In the past, software security focused on anticipating where and how the attacks would come and putting up barriers to prevent those attacks. However, most attacks–especially sophisticated attacks–can’t be anticipated, which means that fixes are bolted on as new attacks are discovered. The inability to anticipate attacks is why we often see patches coming out in response to new 0-day vulnerabilities. Secure DevOps developers would rather their software absorb the attacks and continue to function. In other words, it should bend but not break. This shift in thinking from a prevent to a bend-don’t-break mindset allows for a lot more flexibility when it comes to dealing with attacks. Becoming secured lifecycle requires the development team to focus on continuous integration, infrastructure as code, eliminating denial of service (DOS), and limiting the attack surface. A look at how DevOps principles can be applied to software development process on regardless of size or industry types. The burgeoning concepts of DevOps include a number of concepts that can be applied to increasing the security of developed applications. These include adding automated security testing techniques such as fuzz testing, software penetration testing to the software development cycle or the system integration cycle. Other techniques include standardizing the integration cycle in order to reduce the possibility of the introduction of faults and introducing security concerns and constraints to software and system development teams at the inception of projects rather than applying them after the fact. Applying these and other DevOps principles can have a big impact on creating an environment that is resilient and secure. Examples of how DevOps principles were applied on projects will be discussed along with lessons learned and some ideas on how to apply them to development and acquisition. Specifically in this talk, I will clearly explain on how to address security concern at early development lifecycle and the way of addressing these threads at many decisions point. And share a reference architecture to have automation security analysis during integration or in deployment and delivery phases.

2. SecDevOps: Is It a Marketing Buzzword? Mapping Research on Security in DevOps

Vaishnavi Mohan (TU Darmstadt; Germany) and Lotfi Ben Othmane (Fraunhofer SIT, Germany)

Abstract: DevOps is changing the way organizations develop and deploy applications and service customers. Many organizations want to apply DevOps, but they are concerned by the security aspects of the produced software. This has triggered the creation of the terms SecDevOps and DevSecOps. These terms refer to incorporating security practices in a DevOps environment by promoting the collaboration between the development teams, the operations teams, and the security teams. This paper surveys the literature from academia and industry to identify the main aspects of this trend. The main aspects that we found are: definition, security best practices, compliance, process automation, tools for SecDevOps, software configuration, team collaboration, availability of activity data and information secrecy. Although the number of relevant publications is low, we believe that the terms are not buzzwords; they imply important challenges that the security and software communities shall address to help organizations develop secure software while applying DevOps processes.

Workshop ISPM I – Challenges, Threats and Solutions

Session Chair: Gerald Quirchmayr (University of Vienna, Austria)
Location: Lecture Hall E
Time: 09:30-11:00

1. Invited talk: The Strategic Trends in Cybersecurity

Jarno Limnéll (Aalto University, Finland)

Abstract: Cyber security is primarily a strategic issue in today´s world. This mean raising the level of discussion from mere technology to pondering the big picture - the influence of cyber security on societies as a whole. Especially multidisciplinary understanding is needed since the line between physical and digital worlds is blurring. What are the current strategic trends in cybersecurity - and cyber warfare - and how we are able to face these trends? The keynote will provide visionary ideas into the future, in order to make it more secure.

2. The Perfect Storm: The Privacy Paradox and the Internet-of-Things

Meredydd Williams, Jason Nurse and Sadie Creese (University of Oxford, UK)

Abstract: Privacy is a concept found throughout human history and opinion polls suggest that the public value this principle. However, while many individuals claim to care about privacy, they are often perceived to express behaviour to the contrary. This phenomenon is known as the Privacy Paradox and its existence has been validated through numerous psychological, economic and computer science studies. Several contributory factors have been suggested including user interface design, risk salience, social norms and default configurations. We posit that the further proliferation of the Internet-of-Things (IoT) will aggravate many of these factors, posing even greater risks to individuals' privacy. This paper explores the evolution of both the paradox and the IoT, discusses how privacy risk might alter over the coming years, and suggests further research required to address a reasonable balance. We believe both technological and socio-technical measures are necessary to ensure privacy is protected in a world of ubiquitous technology.

CD ARES IV – Visualization and Risk Management

Session Chair: Francesco Buccafurri (University of Reggio Calabria, Italy)
Location: Lecture Hall B
Time: 09:30-11:00

1. Visualization Model for Monitoring of Computer Networks Security based on the Analogue of Voronoi Diagrams

Maxim Kolomeets, Andrey Chechulin and Igor Kotenko (St. Petersburg Institute for Informatics and Automation, Russia)

Abstract: In this paper we propose an approach to the development of the computer network visualization system for security monitoring, which uses a conceptually new model of graphic visualization that is similar to the Voronoi diagrams. The proposed graphical model uses the size, color and opacity of the cell to display host parameters. The paper describes a technique for new graphical model construction and gives examples of its application along with traditional graph based and other models.

2. Modeling cyber systemic risk for the business continuity plan of a Bank

Angelo Furfaro, Teresa Gallo and Domenico Sacca (University of Calabria, Italy)

Abstract: The pervasive growth and diffusion of complex IT systems, which handle critical business aspects of today's enterprises and which cooperate through computer networks, has given rise to a significant expansion of the exposure surface towards cyber security threats. A threat, affecting a given IT system, may cause a ripple effect on the other interconnected systems often with unpredictable consequences. This type of exposition, known as cyber systemic risk, is a very important concern especially for the international banking system and it needs to be suitably taken into account during the requirement analysis of a bank IT system. This paper proposes the application of a goal-oriented methodology (GOReM), during the requirements specification phase, in order to consider adequate provisions for prevention and reaction to cyber systemic risk in banking systems. In particular, the context of the Italian banking system is considered as a case study.

3. Differentiating cyber risk of insurance customers: the insurance company perspective

Inger Anne Tøndel, Fredrik Seehusen, Erlend Andreas Gjære and Marie Elisabeth Gaup Moe (SINTEF ICT, Norway)

Abstract: As a basis for offering policy and setting tariffs, cyber-insurance carriers need to assess the cyber risk of companies. This paper explores the challenges insurance companies face in assessing cyber risk, based on literature and interviews with representatives from insurers. The interview subjects represent insurance companies offering cyber-insurance in a market where this is a new and unknown product. They have limited historical data, with few examples of incidents leading to payout. This lack of experience and data, together with the need for an efficient sales process, highly impacts their approach to risk assessment. Two options for improving the ability to perform thorough yet efficient assessments of cyber risk are explored in this paper: basing analysis on reusable sector specific risk models, and including managed security service providers (MSSPs) in the value chain.

11:00 - 11:30 Coffee Break

11:30 – 13:00 Parallel Sessions

ARES Full VI – Intrusion Detection and Incident Response

Session Chair: Abdelmalek Benzekri (Universtié Paul Sabatiér, France)
Location: Lecture Hall A
Time: 11:30-13:00

1. Selection of Mitigation Actions Based on Financial and Operational Impact Assessments

Gustavo Gonzalez Granadillo (CNRS Samovar UMR 5157, France), Alexander Motzek (Universitat zu Lubeck, Germany), Joaquin Garcia-Alfaro and Hervé Debar (CNRS Samovar UMR 5157, France)

Abstract: Finding adequate responses to ongoing attacks on ICT systems is a pertinacious problem and requires assessments from different perpendicular viewpoints. However, current research focuses on reducing the impact of an attack irregardless of side-effects caused by responses. In order to achieve a comprehensive yet accurate response to possible and ongoing attacks on a managed ICT system, we propose an approach that relies on a response system that continuously quantifies risks, and decides how to respond to cyber-threats that target a monitored ICT system. Our Dynamic Risk Management Response (DRMR) model is composed of two main modules: a Response Financial Impact Assessor (RFIA), which provides an assessment concerning the potential financial impact that responses may cause to an organization; and a Response Operational Impact Assessor (ROIA), which assesses potential impacts that efficient mitigation actions may cause on the organization in an operational perspective. As a result, the DRMR model proposes response plans to mitigate identified risks, enable choice of the most suitable response possibilities to reduce identified risks below an admissible level while minimizing potential negative side effects of deliberately taken actions.

2. A Host-based Intrusion Detection and Mitigation Framework for Smart Home IoT Using OpenFlow

Mehdi Nobakht, Vijay Sivaraman (NICTA, Australia) and Roksana Boreli (UNSW, Australia)

Abstract: Smart devices are gaining popularity in our homes with the promise to make our lives easier and more comfortable. However, the increased deployment of such smart devices brings an increase in potential security risks. In this work, we propose an intrusion detection and mitigation framework, called IoT-IDM, to provide a network-level protection for smart devices deployed in home environments. IoT-IDM monitors the network activities of intended smart devices within the home and investigates whether there is any suspicious or malicious activity. Once an intrusion is detected, it is also capable of blocking the intruder in accessing the victim device on the fly. The modular design of IoT-IDM gives its users the flexibility to employ customized machine learning techniques for detection based on learned signature patterns of known attacks. Software-defined networking technology and its enabling communication protocol, OpenFlow, are used to realise this framework. Finally, a prototype of IoT-IDM is developed and the applicability and efficiency of proposed framework demonstrated through a real IoT device: a smart light bulb.

3. Towards a CDS-Based Intrusion Detection Deployment Scheme for Securing Industrial Wireless Sensor Networks

Lyes Bayou, Nora Cuppens-Boulahia (Telecom Bretagne, France), David Espes (University of Brest, France) and Frédéric Cuppens (Telecom Bretagne, France)

Abstract: The use of wireless communication is a major trend in the so called Supervisory Control and Data Acquisition systems (SCADA). Consequently, Wireless Industrial Sensor Networks (WISN) were developed to meet real time and security requirements needed by SCADA systems. In term of security, WISN suffer from the same threats that those targeting classical WSN. Indeed, attackers mainly use wireless communication as a medium to launch these attacks. But as these networks are used to manage critical systems, consequences of such attacks can be more harmful. Therefore, additionally to the use of cryptographic and authentication mechanisms, Intrusion Detection Systems (IDS) are also used as a second line of defense. In this paper we propose an efficient IDS deployment scheme specially tailored to fit WISN characteristics. It builds a virtual wireless backbone that adds security purposes to the WISN. We also show that the proposed deployment scheme provides a good traffic monitoring capability with an acceptable number of monitoring nodes. It particularly allows detecting that a packet has been forged, deleted, modified or delayed during its transmission.

Workshop SAW II

Session Chair: Sebastian Schrittwieser (Josef Ressel Zentrum TARGET, St. Pölten University of Applied Sciences, Austria)
Location: Lecture Hall C
Time: 11:30-13:00

1. How Secure are Web Servers? An Empirical Study of Slow HTTP DoS Attacks and Detection

Neminath Hubballi, Nikhil Tripathi and Yogendra Singh (Indian Institute of Technology Indore, India)

Abstract: Slow HTTP Denial of Service (DoS) is an application layer DoS attack in which large number of incomplete HTTP request s are sent. If number of such open connections in the server exhaust a preset threshold, server does not accept any new connections thus creating DoS. In this paper we make twofold contributions. We do an empirical study on different HTTP servers for their vulnerability against slow HTTP DoS attacks. Subsequently we propose a method to detect Slow HTTP Dos attack. The proposed detection system is an anomaly detection system which measures the Hellinger distance between two probability distributions generated in training and testing phases. In the training phase it creates a normal profile as a probability distribution comprising of complete and incomplete HTTP requests. In case of Slow HTTP attack the proportion of incomplete messages is increased in the overall traffic and detection system leverages this for detection by generating another probability distribution and finding difference between two probability distributions. We experiment by collecting data from a real web server and report the detection performance of proposed detection system.

2. A Type System for Quantified Information-Flow Security in Java-Like Languages

Gohar Shakoori, Mehran Fallah and Zeinab Iranmanesh (Amirkabir University of Technology, Iran)

Abstract: Quantified information-flow policies put an upper bound on the allowable amount of information flow from high inputs to low outputs of a program. Earlier research in this area has mainly focused on simple imperative languages. In this paper, we present a type system that derives the amount of information flow in the programs of a Java-like language. For this purpose, we adopt the Middlewieght Java (MJ) which is small enough for formal proofs, although it is a proper subset of Java with a fairly rich set of features. Promotable expressions, which also behave as statements, as well as method invocations and the loops they may create are of particular attention in the study of quantified information flow in such a language. We prove that our typing rules are sound and derive correct bounds of information flow for a given program. The proofs are based on a denotational semantics for MJ that we propose as part of this research.

3. On Analyzing Program Behavior Under Fault Injection Attacks

Jakub Breier (Nanyang Technological University, Singapore)

Abstract: Fault attacks pose a serious threat to cryptographic algorithm implementations. It is a non-trivial task to design a code that minimizes the risk of exploiting the incorrect output that was produced by inducing faults in the algorithm execution process. In this paper we propose a design of an instruction set simulator capable of analyzing the code behavior under fault attack conditions. Our simulator is easy to use and provides a valuable insights for the designers that could help to harden the code they implement.

Workshop ASSD II – Experiences in agile development of secure software

Session Chair: Juha Röning (University of Oulu, Finland)
Location: Lecture Hall D
Time: 11:30-13:00

1. An Empirical Study on the Relationship between Software Security Skills, Usage and Training needs in Agile Settings

Tosin Daniel Oyetoyan, Daniela S. Cruzes and Martin Gilje Jaatun (SINTEF ICT, Norway)

Abstract: Organizations recognize that protecting their assets against attacks is an important business. However, achieving what is adequate security requires taking bold steps to address security practices within the organization. In the Agile software development world, security engineering process is unacceptable as it runs counter to the agile values. Agile teams have thus approached software security activities in their own way. To improve security within agile settings requires that management understands the current practices of software security activities within their agile teams. In this study, we use survey to investigate software security usage, competence, and training needs in two agile organizations. We find that (1) The two organizations perform differently in core software security activities but are similar when activities that could be leveraged for security are considered (2) regardless of cost or benefit, skill drives the kind of activities that are performed (3) Secure design is expressed as the most important training need by all groups in both organizations (4) Effective software security adoption in agile setting is not automatic, it requires a driver.

2. Case Study of Security Development in an Agile Environment: Building Identity Management for a Government Agency

Kalle Rindell, Sami Hyrynsalmi and Ville Leppänen (University of Turku, Finland)

Abstract: In contemporary software development projects and computing tasks, security concerns have an increasing effect, and sometimes even guide both the design and the project's processes. In certain environments, the demand for the security becomes the main driver of the development. In these cases, the development of the product requires special security arrangements for development and hosting, and specific security-oriented processes for governance. Compliance with these requirements using agile development methods may not only be a chance to improve the project efficiency, but can in some cases, such as in the case discussed in this paper, be an organizational requirement. This paper describes a case of building a secure identity management system and its management processes, in compliance with the Finnish government's VAHTI security instructions. The building project was to be implemented in accordance to the governmental security instructions, while following the service provider's own management framework. Project itself was managed with Scrum. The project's steering group required the use of Scrum, and this project may be viewed as a showcase of Scrum's suitability to multi-teamed, multi-site, security standard-compliant work. We also discuss the difficulties of fulfilling strict security regulations regarding both the development process and the end product in this project, and the difficulties utilizing Scrum to manage a multi-site project organization. Evaluation of the effects of the security work to project cost and efficiency is also presented. Finally, suggestions to enhance the Scrum method for security-related projects are made.

3. Towards Effective Security Assurance for Incremental Software Development – The Case of Zen Cart Application

Azmat Ali (TU Darmstadt, Germany) and Lotfi Ben Othmane (Fraunhofer SIT, Germany)

Abstract: Incremental software development methods, such as Scrum embrace code changes to meet changing customer requirements. However, changing the code of a given software invalidates the security assurance of the software. Thus, each new version of a given software requires a new full security assessment. This paper investigates the impact of incremental development of software on their security assurances using the e-commerce software Zen Cart as a case study. It also describes a prototype we are developing to design security assurance cases and trace the impact of code changes on the security assurance of the given software. A security assurance case shows how a claim, such as ”The system is acceptably secure” is supported by objective evidence

Workshop ISPM II – Models and Communication

Session Chair: Kari Jussila (Aalto University, Finland)
Location: Lecture Hall E
Time: 11:30-13:00

1. Privacy Impact Assessment Template for Provenance

Jenni Reuben, Leonardo Martucci, Simone Fischer-Hübner (Karlstad University, Sweden), Heather S. Packer (University of Southampton, UK), Hans Hedbom (Karlstad University, Sweden) and Luc Moreau (University of Southampton, UK)

Abstract: Provenance data can be expressed as a graph with links informing who and which activities created, used and modified entities. The semantics of these links and domain specific reasoning can support the inference of additional information about the elements in the graph. If such elements include personal identifiers and/or personal identifiable information, then inferences may reveal unexpected links between elements, thus exposing personal data beyond an individual's intentions. Provenance graphs often entangle data relating to multiple individuals. It is therefore a challenge to protect personal data from unintended disclosure in provenance graphs. In this paper, we provide a Privacy Impact Assessment (PIA) template for identifying imminent privacy threats that arise from provenance graphs in an application-agnostic setting. The PIA template identifies privacy threats, lists potential countermeasures, helps to manage personal data protection risks, and maintains compliance with privacy data protection laws and regulations.

2. Major Challenges in Structuring and Institutionalizing CERT-Communication

Otto Hellwig (SBA Research, Austria), Gerald Quirchmayr (University of Vienna, Austria), Edith Huber (Danube University Krems, Austria), Gernot Goluch (SBA Research, Austria), Franz Vock (Federal Chancellery, Austria) and Bettina Pospisil (Danube University Krems, Austria).

Abstract: This paper describes an approach to the definition of requirements for CERT-Communication in a changing environment. CERTs play an outstanding role for the detection, analysis and mitigation of vulnerabilities, threats and cyber-attacks in a multistakeholder cyberspace on which society relies more and more. Furthermore CERTs are a very valuable backbone for national and regional (e.g. European Union) cyber strategies and their role is partly defined in national and European legislation.

It can be difficult to bring these obligations in line with the current primarily informal communication channels of CERTs that rely on person to person trust. This paper is devoted to the question of which kind of communication requirements have to be fulfilled to best use and support the work of CERTs in this complex environment.

3. Towards a Complex Systems Approach to Legal and Economic Impact Analysis of Critical Infrastructures

Thomas Schaberreiter, Gerald Quirchmayr (University of Vienna, Austria), Anna-Maija Juuso (University of Oulu, Finland), Moussa Ouedraogo (Luxembourg Institute of Science and Technology, Luxembourg) and Juha Röning (University of Oulu, Finland)

Abstract: Information security has become interdependent, global and critical - it has become cybersecurity. In this complex environment, legal consideration and economic incentives are as integral to ensuring the security of information systems as the technological realization. In this paper, we argue that comprehensive cybersecurity requires that these three disciplines are considered together. To this end, we propose a legal analysis framework, which can be used to study legal and economic requirements for cybersecurity in relation to technological realities. The framework yields concrete recommendations, which complex system and critical infrastructure stakeholders can utilize to improve security within their networks. The analysis framework aims to offer key stakeholders a better understanding of the legal and economic requirements for cybersecurity and provide them with recommendations that are in line with modern cybersecurity strategies, including the enhancement of cooperation and collaboration capabilities and the implementation of other state-of-the-art security mechanisms.

Workshop PAML I

Session Chair: Peter Kieseberg (SBA Research, Austria)
Location: Lecture Hall B
Time: 11:30-13:00

1. Data Anonymization as a Vector Quantization Problem: Control over Privacy for Health Data

Yoan Miche, Ian Oliver, Silke Holtmanns, Aapo Kalliola (Bell Labs, Nokia, Finland), Anton Akusok (Arcada University of Applied Sciences, Finland), Amaury Lendasse (The University of Iowa, USA) and Kaj-Mikael Björk (Arcada University of Applied Sciences, Finland)

Abstract: This paper tackles the topic of data anonymization from a vector quantization point of view. The admitted goal in this work is to provide means of performing data anonymization to avoid single individual or group re-identification from a data set, while maintaining as much as possible (and in a very specific sense) data integrity and structure. The structure of the data is first captured by clustering (with a vector quantization approach), and we propose to use the properties of this vector quantization to anonymize the data. Under some assumptions over possible computations to be performed on the data, we give a framework for identifying and “pushing back outliers in the crowd”, in this clustering sense, as well as anonymizing cluster members while preserving cluster-level statistics and structure as defined by the assumptions (density, pairwise distances, cluster shape and members. . .).

2. An Open-Source Object-Graph-Mapping Framework for Neo4j and Scala: renesca

André Calero Valdez, Felix Dietze, Johannes Karoff, Christoph Greven, Ulrik Schroeder and Martina Ziefle (RWTH Aachen University, Germany)

Abstract: The usage and application of graph databases is increasing. Many research problems are based on understanding relationships between data entities. This is where graph databases are powerful. Nevertheless, software developers model and think in object-oriented software. Combining both approaches leads to a paradigm mismatch. This mismatch can be addressed by using object graph mappers (OGM). OGM adapt graph databases for object-oriented code, to relieve the developer. Most graph database access frameworks only support tablebased result outputs. This defeats one of the strongest purposes of using graph databases. In order to harness both the power of graph databases and object-oriented modeling (e.g. type-safety, inheritance, etc.) we propose an open-source framework with two libraries: 1) renesca, which is a graph database driver providing graph-query-results and change tracking. 2) renesca-magic, a macro-based ER-modeling domain specific language (DSL). Both were tested in a graph-based application and lead to dramatic improvements in code size (factor 10) and extensibility of the code, with no significant effect on performance.

3. Publishing Differentially Private Medical Events Data

Sigal Shaked and Lior Rokach (Ben-Gurion University, Israel)

Abstract: Sequential data has been widely collected in the past few years; in the public health domain it appears as collections of medical events such as lab results, electronic chart records, or hospitalization transactions. Publicly available sequential datasets for research purposes promises new insights, such as understanding patient types, and recognizing emerging diseases.

Unfortunately, the publication of sequential data presents a significant threat to users' privacy. Since data owners prefer to avoid such risks, much of the collected data is currently unavailable to researchers. Existing anonymization techniques that aim at preserving sequential patterns lack two important features: handling long sequences and preserving occurrence times. In this paper, we address this challenge by employing an ensemble of Markovian models trained based on the source data. The ensemble takes several optional periodicity levels into consideration. Each model captures transitions between times and states according to shorter parts of the sequence, which is eventually reconstructed. Anonymity is provided by utilizing only elements of the model that guarantee differential privacy. Furthermore, we develop a solution for generating differentially private sequential data, which will bring us one step closer to publicly available medical datasets via sequential data. We applied this method to two real medical events datasets and received some encouraging results, demonstrating that the proposed method can be used to publish high quality anonymized data.

4. A Peer-to-Peer Protocol and System Architecture for Privacy-Preserving Statistical Analysis

Katerina Zamani, Angelos Charalambidis, Stasinos Konstantopoulos, Maria Dagioglou and Vangelis Karkaletsis (NCSR 'Demokritos', Greece)

Abstract: The insights gained by the large-scale analysis of health related data can have an enormous impact in public health and medical research, but access to such personal and sensitive data poses serious privacy implications for the data provider and a heavy data security and administrative burden on the data consumer. In this paper we present an architecture that fills the gap between the statistical tools ubiquitously used in medical research on the one hand, and privacy-preserving data mining methods on the other. This architecture foresees the primitive instructions needed to re-implement the elementary statistical methods so that they only access data via a privacy-preserving protocol. The advantage is that more complex analysis and visualization tools that are built upon these elementary methods can remain unaffected. Furthermore, we introduce RASSP, a secure summation protocol that implements the primitive instructions foreseen by the architecture. An open-source reference implementation of this architecture is provided for the R language. We use these results to argue that the tension between medical research and privacy requirements can be technically alleviated and we outline a research plan towards a system that covers further requirements on computation efficiency and on the trust that the medical researcher can place on the statistical results obtained by it.

5. The right to be forgotten: Towards Machine Learning on perturbed knowledge bases

Bernd Malle, Peter Kieseberg, Edgar Weippl (SBA Research, Austria) and Andreas Holzinger (Holzinger Group HCI-KDD, Austria)

Abstract: Today's increasingly complex information infrastructures represent the basis of any data-driven industries which are rapidly becoming the 21st century's economic backbone. The sensitivity of those infrastructures to disturbances in their knowledge bases is therefore of crucial interest for companies, organizations, customers and regulating bodies. This holds true with respect to the direct provisioning of such information in crucial applications like clinical settings or the energy industry, but also when considering additional insights, predictions and personalized services that are enabled by the automatic processing of those data. In the light of new EU Data Protection regulations applying from 2018 onwards which give customers the right to have their data deleted on request, information processing bodies will have to react to these changing jurisdictional (and therefore economic) conditions. Their choices include a re-design of their data infrastructure as well as preventive actions like anonymization of databases per default. Therefore, insights into the effects of perturbed / anonymized knowledge bases on the quality of machine learning results are a crucial basis for successfully facing those future challenges. In this paper we introduce a series of experiments we conducted on applying four different classifiers to an established dataset, as well as several distorted versions of it and present our initial results.

13:00 – 14:00 Lunch

14:00 – 16:00 Parallel Sessions

ARES Full VII – Security Models and Architectures

Session Chair: Marijke Coeetze (University of Johannesburg, South Africa)
Location: Lecture Hall A
Time: 14:00-16:00

1. Role Mining with Missing Values

Sokratis Vavilis, Alexandru Egner, Milan Petkovic and Nicola Zannone (Eindhoven University of Technology, Netherlands)

Abstract: Over the years several organizations are migrating to Role-Based Access Control (RBAC) as a practical solution to regulate access to sensitive information. Role mining has been proposed to automatically extract RBAC policies from the current set of permissions assigned to users. Existing role mining approaches usually require that this set of permissions is retrievable and complete. Such an assumption, however, cannot be met in practice as permissions can be hard-coded in the applications or distributed over several subsystems. In those cases, permissions can be obtained from activity logs recording the actions performed by users. This, however, can provide an incomplete representation of the permissions within the system. Thus, existing role mining solutions are not directly applicable. In this work, we study the problem of role mining with incomplete knowledge. In particular, we investigate approaches for two instances of the role mining problem with missing values. Moreover, we study metrics to properly evaluate the obtained RBAC policies. We validate the investigated approaches using both synthetic and real data.

2. Towards a Systemic Approach for Information Security Risk Management

Yannick Naudet, Nicolas Mayer and Christophe Feltus (Luxembourg Institute of Science and Technology, Luxembourg)

Abstract: Risk management in the field of information security is most often handled individually by enterprises, taking only a limited view on the influential factors coming from their providers, clients or more globally from their environment. This approach becomes less appropriate in the case of networked enterprises, which tend to form ecosystems with complex influence links. A more holistic approach is needed to take these into account, leading to systemic risk management, i.e. risk management on the entire system formed by the networked enterprises, to avoid perturbations of the ecosystem due to local, individual, decision-making. In this paper, we propose a new metamodel for Information System Security Risk Management (ISSRM), comprising systemic elements as defined in the General Systems Theory. We discuss the design of this new model, highlighting in particular how risk management can be related to a problem-solving approach and the important concepts that are instantiated when taking a systemic approach to ISSRM.

3. Towards a metamodel for SABSA Conceptual Architecture Descriptions

Patrick Pleinevaux (Kudelski Security, Switzerland)

Abstract: The SABSA framework allows to develop an Enterprise Security Architecture from business requirements down to controls and associated security management. The purpose of this paper is to propose a metamodel that includes key constructs used in SABSA for conceptual security architecture description and relationships between these constructs. We propose five metamodel fragments that correspond to five of the six views of SABSA and illustrate with an example how the metamodel can be used to develop a conceptual architecture.

4. Threat Modelling Service Security and Privacy as a Security Ceremony

Taciane Martimiano and Jean Everson Martina (Universidade Federal de Santa Catarina, Brazil)

Abstract: Security ceremonies are extensions for security protocols. One goal of ceremony designers is to be able to use symbolic evaluation methods to verify claims embedded in ceremonies. Unfortunately, there are some pieces missing for that, such as, a base description language and a tailored threat model for security ceremonies. Our contributions in this paper are: a proposal for message description syntax, an augmented threat model to encompass the subtleties of security ceremonies and a strategy for symbolic evaluation using First Order Logic (FOL) and an automatic theorem prover. Furthermore, we propose a new threat model named Distributed Attacker (DA), which uses the adaptive threat model proposed by Carlos et al. and the Security Ceremony Concertina Traversal layers proposed by Bella et al. As a result, we present scenarios which can be formally analysed with our proposal.

Workshop SAW III

Session Chair: Simon Tjoa (St. Pölten University of Applied Sciences, Austria)
Location: Lecture Hall C
Time: 14:00-16:00

1. Authentication Techniques in the Context of E-participation: Current Practice, Challenges, and Recommendations

Maria Leitner and Arndt Bonitz (AIT, Austria)

Abstract: Authentication as well as identification are key functions when it comes to online and democratic participatory processes that can be found in the context of e-participation. Until now, research has centered on the development of authentication and identification techniques. Why and how these techniques are currently used and what their benefits are in the context of e-participation is missing so far. In this paper, we aim to address these challenges by reviewing state of the art literature and practice in order to determine how current authentication techniques are used in e-participation. Furthermore, we conduct an expert survey in order to establish a baseline how current techniques are used and perceived. The results show that current practice focuses strongly on the use of the de facto standard user/password in e-participation. However, experts believe that multiple other authentication techniques such as biometrics or electronic signatures will become more important in future applications. Moreover, experts acknowledge the use of various authentication methods suitable for the level of participation, as opposed to current practice that often provides only one way of authentication. These findings will help to further develop and improve future technologies and applications to support participatory processes for citizens' involvement.

2. Secure Software Design with Tactics and Patterns (presentation only)

Jungwoo Ryoo (Pennsylvania State University, USA) and Simon Tjoa (St. Pölten University of Applied Sciences, Austria)

Workshop ASSD III – Assessment of research on agile development of secure software

Session Chair: Juha Röning (University of Oulu, Finland)
Location: Lecture Hall D
Time: 14:00-16:00

1. Misuse, Abuse, and Reuse: Economic utility functions for characterising security requirements

Chad Heitzenrater (U.S. Air Force Research Laboratory, USA) and Andrew Simpson (University of Oxford, UK)

Abstract: Negative use cases — in the form of 'misuse' or 'abuse' cases — have found a broad following within the security community due to their ability to make explicit the knowledge, assumptions and desires of stakeholders regarding real and perceived threats to systems. As an accepted threat modelling tool, they have become a standard part of many Secure Software Engineering (SSE) processes. Despite this widespread adoption, aspects of the original misuse case concept have yet to receive a formal treatment in the literature. This paper considers the application of economic utility functions within the negative use case development process, as a means of addressing existing challenges. We provide a simple demonstration of how existing practice might integrate economic factors to describe the business, management and functional concerns that surround system security and software development.

2. Agile Team Members Perceptions on Non-Functional Testing – Influencing Factors from an Empirical Study

Cristina Rosa Camacho, Sabrina Marczak (PUCRS University, Brazil) and Daniela S. Cruzes (SINTEF – ICT, Norway)

Abstract: Non-functional requirements define the overall qualities or attributes of a system. Although important, they are often neglected for many reasons, such as pressure of time and budget. In agile software development, there is a focus on the feature implementation and delivery of value to the customer and, as such, non-functional aspects of a system should also be of attention. Non-functional requirements testing is challenging due its cross-functional aspects and lack of clarity of their needs by business in the most part of projects. The goal of this paper is to empirically investigate how do agile team members handle non-functional testing in their projects, aiming to identify preliminary factors influencing the testing of non-functional requirements, specifically performance and security in agile development. We conducted interviews with twenty IT professionals in large multinational company. As result we could identify seven main factors influencing non-functional testing and four main practices adopted by them to overcome the challenges faced. We aim to replicate our investigation in a larger scale. Meanwhile, our work provides initial contributions to practitioners and inspires our future research.

Workshop ISPM III – Panel Discussion on Arising Challenges for Information Security Management

Session Chair: Juhani Anttila (IAQ, Finland)
Location: Lecture Hall E
Time: 14:00-16:00

Panel discussion on Challenges for Information Security Management

Chaired by Juhani Anttila, IAQ, Finland

Panelists:

Alfredo Cuzzocrea, University of Trieste, Italy

Abdelmalek Benzekri, Universtié Paul Sabatiér, France

Johannes Göllner, BMLVS/LVAk/ZentDok, Austria

Martin Gilje Jaatun, SINTEF, Norway

Robert Hayes, Microsoft UK, UK

Juha Roning, University of Oulu, Finland

Chris Wills, CARIS Research, United Kingdom

PAML II

Session Chair: Andreas Holzinger (Holzinger Group HCI-KDD, Austria)
Location: Lecture Hall B
Time: 14:00-16:00

1. An Open-Source Object-Graph-Mapping Framework for Neo4j and Scala: renesca

Felix Dietze, Johannes Karoff, André Calero Valdez, Martina Ziefle, Christoph Greven and Ulrik Schroeder (RWTH Aachen University, Germany)

Abstract: The usage and application of graph databases is increasing. Many research problems are based on understanding relationships between data entities. This is where graph databases are powerful. Nevertheless, software developers model and think in object-oriented software. Combining both approaches leads to a paradigm mismatch. This mismatch can be addressed by using object graph mappers (OGM). OGM adapt graph databases for object-oriented code, to relieve the developer. Most graph database access frameworks only support tablebased result outputs. This defeats one of the strongest purposes of using graph databases. In order to harness both the power of graph databases and object-oriented modeling (e.g. type-safety, inheritance, etc.) we propose an open-source framework with two libraries: 1) renesca, which is a graph database driver providing graph-query-results and change tracking. 2) renesca-magic, a macro-based ER-modeling domain specific language (DSL). Both were tested in a graph-based application and lead to dramatic improvements in code size (factor 10) and extensibility of the code, with no significant effect on performance.

2. A Peer-to-Peer Protocol and System Architecture for Privacy-Preserving Statistical Analysis

Katerina Zamani, Angelos Charalambidis, Stasinos Konstantopoulos, Maria Dagioglou and Vangelis Karkaletsis (NCSR 'Demokritos', Greece)

Abstract: The insights gained by the large-scale analysis of health related data can have an enormous impact in public health and medical research, but access to such personal and sensitive data poses serious privacy implications for the data provider and a heavy data security and administrative burden on the data consumer. In this paper we present an architecture that fills the gap between the statistical tools ubiquitously used in medical research on the one hand, and privacy-preserving data mining methods on the other. This architecture foresees the primitive instructions needed to re-implement the elementary statistical methods so that they only access data via a privacy-preserving protocol. The advantage is that more complex analysis and visualization tools that are built upon these elementary methods can remain unaffected. Furthermore, we introduce RASSP, a secure summation protocol that implements the primitive instructions foreseen by the architecture. An open-source reference implementation of this architecture is provided for the R language. We use these results to argue that the tension between medical research and privacy requirements can be technically alleviated and we outline a research plan towards a system that covers further requirements on computation efficiency and on the trust that the medical researcher can place on the statistical results obtained by it.

16:00 – 16:30 Coffee Break

16:30 – 17:30 Plenary Session

16:30 – 17:30 Keynote

Time: 16:30 – 17:30
Location: Lecture Hall A

Toward Causal Machine Learning

Bernhard Schölkopf (Max-Planck-Campus Tübingen, Germany)

Abstract: In machine learning, we use data to automatically find dependences in the world, with the goal of predicting future observations. Most machine learning methods build on statistics, but one can also try to go beyond this, assaying causal structures underlying statistical dependences. Can such causal knowledge help prediction in machine learning tasks? We argue that this is indeed the case, due to the fact that causal models are more robust to changes that occur in real world datasets. We touch upon the implications of causal models for machine learning tasks such as domain adaptation, transfer learning, and semi-supervised learning. We also present an application to the removal of systematic errors for the purpose of exoplanet detection. Machine learning currently mainly focuses on relatively well-studied statistical methods. Some of the causal problems are conceptually harder, however, the causal point of view can provide additional insights that have substantial potential for data analysis.

17.30 – 23.00 Conference Dinner

Our Conference Dinner – a highlight at ARES 2016 – will take place high above the roofs of Salzburg in the high-class restaurant M32. The restaurant is located at the “Mönchsberg”, one of the five mountains in the city of Salzburg.

Meeting point: in front of the University, buses leave 17.45 (shortly after the last keynote session)

Buses will take us from the university to the city, there won’t be a transfer back to the university (the restaurant is located in the city center).

Friday, September 2, 2016

08:30 – 17:00 Registration desk open

09:30 – 10:30 Plenary Session

Keynote

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

Data Analytic in Anonymized Networks: Is There Hope for Privacy?

Negar Kiyavash (University of Illinois at Urbana-Champaign, US)

Abstract: The proliferation of online social networks has helped in generating large amounts of graph data which has immense value for data analytics. Network operators, like Facebook, often share this data with researchers or third party organizations, which helps both the entities generate revenues and improve their services. As this data is shared with third party organizations, the concern of user privacy becomes pertinent. Hence, it becomes essential to balance utility and privacy while releasing such data. Advances in graph matching and the resulting recent attacks on graph datasets paints a grim picture.
We discuss the feasibility of privacy preserving data analytics in anonymized networks and provide an answer to the question "Does there exist a regime where the network cannot be deanonymized, yet data analytics can be performed?"

10:30 – 11:00 Coffee Break

11:00 – 12:30 Parallel Sessions

ARES Short I – Cloud Security

Session Chair: Jakub Breier (Nanyang Technological University, Singapore)
Location: Lecture Hall B
Time: 11:00-12:30

1.Access Control and Data Separation Metrics in Cloud Infrastructures

Bernd Jäger (COLT Technology Services, Germany), Reiner Kraft (Fraunhofer SIT, Germany), Sebastian Luhn (Westfaelische Wilhelms-Universitaet Muenster, Germany), Annika Selzer and Ulrich Waldmann (Fraunhofer SIT, Germany)

Abstract: An automatically controlled and analyzed privacy level in cloud environments would probably help to allay or at least reduce privacy concerns of prospective clients, in particular if the clients themselves can check the compliance with a required privacy level during regular data processing. However, for each intended control firstly an appropriate set of data sources has to be determined carefully, then the results have to be combined to useful metrics, so that the measurements results approximate specific privacy objectives. This paper proposes appropriate data sources and a partly automatic approach to collect measurement data for controls of separate data processing and access control for clients of cloud infrastructure services (IaaS).

2. IFCaaS: Information Flow Control as a Service for Cloud Security

Marwa Elsayed and Mohammad Zulkernine (Queen's University, Canada)

Abstract: With the maturity of service-oriented architecture (SOA) and Web technologies, web services have become critical components of Software as a Service (SaaS) applications in cloud ecosystem environments. Most SaaS applications leverage multi-tenant data stores as a back end to keep and process data with high agility. Although these technologies promise impressive benefits, they put SaaS applications at risk against novel as well as prevalent attack vectors. This security risk is further magnified by the loss of control and lack of security enforcement over sensitive data manipulated by SaaS applications. An effective solution is needed to fulfill several requirements originating in the dynamic and complex nature of such applications. Inspired by the rise of Security as a Service (SecaaS) model, this paper introduces "Information Flow Control as a Service (IFCaaS)". IFCaaS lays the foundation of cloud-delivered IFC-based security analysis and monitoring services. As an example of the adoption of the IFCaaS, this paper presents a novel framework that addresses the detection of information flow vulnerabilities in SaaS applications. Our initial experiments show that the framework is a viable solution to protect against data integrity and confidentiality violations leading to information leakage.

3. Your Cloud in my Company: Modern Rights Management Services Revisited

Martin Grothe, Paul Roesler, Johanna Jupke, Jan Kaiser, Christian Mainka and Joerg Schwenk (Ruhr-University Bochum, Germany)

Abstract: We provide a security analysis of modern Enterprise Rights Management (ERM) solutions and reveal security threats. We first take a look on Microsoft Azure, and discuss severe attack surfaces that companies enabling Azure in their own trusted infrastructure have to take care of. In addition, we analyze Tresorit, one of the most frequently used End-to-End encrypted cloud storage systems. Tresorit can use Azure and its Rights Management Services (RMS) module as an additional security layer: a user should be able to either trust Tresorit or Azure. Our systematic evaluation reveals a serious breach to their security architecture: we show that the whole security of Tresorit RMS relies on Tresorit being trusted, independent of trusting Azure.

Workshop IWCC – International Workshop on Cyber Crime

Session Chair: Andreas Holzinger (Holzinger Group HCI-KDD, Austria)
Location: Lecture Hall C
Time: 11:00-12:30

1. Keynote: Steganography in the Internet Telephony

Artur Janicki (Warsaw University of Technology, Poland)

Abstract: Internet telephony during the last decade has become intensively used all over the world, and the VoIP traffic volume is constantly growing. It is no wonder that for a couple of years researchers have tried to use the VoIP traffic also as a carrier for hidden transmission. So far, several approaches have been proposed. They include methods based on voice payload modification, methods based on packet header modification, methods which modify packets' arrival time, as well as hybrid methods, which combine two or more of these steganographic techniques. Various techniques have been elaborated, such as LACK, TranSteg or HideF0. These methods will be briefly explained and compared.

2. Law Enforcement Access to Password Protected and/or Encrypted Mobile Data

Murdoch Watney (University of Johannesburg, South Africa)

Abstract: The use of mobile phones in the commission of crime and terrorism pose serious investigative challenges to law enforcement agencies across the world. The discussion deals primarily with the extent a mobile phone service provider and/or or messaging applications provider and/or manufacturer must assist a law enforcement agency in gaining access to mobile data, specifically where the data is encrypted and/or password protected. It should be established whether a mobile phone service and/or applications provider and/or manufacturer must design security and/or privacy measures in such a way that law enforcement may gain access to the encrypted data. It may be argued that national security interests regarding the investigation of serious crimes such as kidnapping, child pornography, corruption and terrorism outweigh user privacy and user security. Terrorism affects all countries globally and in many instances result in the indiscriminate killing of a large number of people as illustrated by the Paris November 2015, the US December 2015, Abidjan, Ivory Coast, Brussels and Pakistan March 2016 killings. Although a law enforcement agency is pressurized to gather as much as possible evidence to investigate such heinous acts and prevent future attacks, the mobile phone evidence must be gathered within a legal framework that provides checks and balances to prevent the development of a police state resulting in the erosion or elimination of human rights. It is necessary to debate whether banning encryption and/or compelling a provider to have the technology to decrypt encrypted mobile communications or override password protected mobile data would serve as an investigative solution in the interest of national security or whether it would ultimately result in weakening user security and privacy to such an extent that all users around the world would be vulnerable to unlawful intrusions.

3.Towards Digital Investigation in Virtual Networks: A Study of Challenges and Open Problems

Daniel Spiekermann (FernUniversität Hagen, Germany) and Tobias Eggendorfer (Hochschule Ravensburg-Weingarten, Germany)

Abstract: The evolution of virtualization techniques is still changing operating principles in today's datacenters (DC). The virtualization of ordinary servers was just the first step, which increased the dynamic and flexibility of the DC. Providers are now able to offer different virtual machines (VM) faster and with less overhead to their customers. But this provision raises new problems for the providers. Aspects like isolation, security or multi-tenancy are increasingly relevant and demand new setups in the DC. Current network infrastructures are not able to handle these aspects with an acceptable effort, but the development of virtual networks offers new possibilities, with benefits for the provider and the user. Based on a physical underlay network, different virtual networks can be defined, either by a provider or the customer. Protocols like VXLAN or GENEVE appear to eliminate restrictions of current networks. New paradigms like Software-defined-Networks (SDN) or Network Function Virtualization (NFV) offer new capabilities to redesign the whole network infrastructure in the DC. But the need for digital investigation is still necessary regardless of all new paradigms and evolution. As a branch of digital investigation, network forensic investigation (NFI) is used to examine network traffic by capturing the data of a suspicious target system and analyzing this data. The modern virtual data

centers and the implemented virtual networks impede the NFI, proved techniques and methods fail because of the increased complexity of the new logical networks. Not only the analysis of the new network protocols impede the NFI, even the capture process of relevant data needs to be refined. In this paper, we analyze in detail new arising problems of digital investigation in virtual networks and explore the new challenges for NFI. Based on the discussion of network forensics and current utilized methodologies and the new techniques of network virtualization the arising problems are defined and classified in three categories. This classification helps to develop new methods and possible solutions, which might simplify further necessary investigations in cloud-computing environments.

4. Threat from Within: Case studies of insiders who committed information technology sabotage

Jason W. Clark (Carnegie Mellon University, USA)

Abstract: In this paper, we investigate insider information technology sabotage. After an analysis of over 1200 cases in our insider threat corpus, we identified 97 insider information technology sabotage cases that are found in public records. In all of our cases, the insider has pleaded guilty or was convicted in a courtroom. The majority of the cases are (United States) domestic. We begin by providing an introduction to the problem space. Next, we provide an abridged case summary for a sample of the cases. Based on all of the cases, we perform an analysis to answer the following research questions: 1) Who are the insiders that commit insider information technology sabotage? 2) What is the motivation behind the insider attacking? 3) What technical means were used to launch the attack? 4) How were the insiders caught? 5) What damage did they cause? 6) What sentence did the insider receive? Lastly, we describe our aggregated results and provide best practices to help mitigate the type of insider threat we describe.

5. Malware in Pirated Software: Case Study of Malware Encounters in Personal Computers

Sravana Kumar, Logesh Madhavan, Mangalam Nagappan and Biplab Sikdar (National University of Singapore, Singapore)

Abstract: Software piracy is a common occurrence, and a significant fraction of the personal computers have some pirated software installed. Cyber-criminals often use pirated software as a vector to spread malware by bundling malicious software with the pirated software. This paper presents the results of a case study that aims to quantify the incidence of malware in pirated software that come bundled with new personal computer purchases. The paper also evaluates the types of malware that are present in the samples in our case study, and the locations in the file system where these malware are detected. The results show that 63% of the samples procured for the case study showed presence of malware and the incidence of malware varies with the geographical location where the sample was procured. Our results also indicate that Trojans and Hacktools are the most prevalent families of malware in our samples.

Workshop WSDF I – Mobile and OS Forensics

Session Chair: Richard Overill (King´s College, UK)
Location: Lecture Hall D
Time: 11:00-12:30

1. Keynote: Behavioural profiling for forensic attribution of attacks

Christian W. Probst (Technical University of Denmark, DK)

Abstract: Digital forensics focusses on extraction, preservation and analysis of digital evidence obtained from electronic devices in a manner that is legally acceptable. Digital evidence, however, rarely reveals why or how it was created, or by whom. Digital investigations aim at attributing the generation of digital artefacts, and transitively of attacks they contributed to.The attacks we are facing today exploit vulnerabilities in the IT infrastructure, the physical infrastructure, and the human factor. Investigating such attacks consequently requires to consider all three levels both for collecting evidence and attibuting attacks. Integrating the human factor in the forensic process promises to understand the motivation of attackers, and to provide causal evidence. In this talk we will present an approach for combining behavioral frameworks, originally developed for explanation of insider attacks, with digital forensics. The work presented is part of the TREsPASS project, which will be presented in the RESIST session at the ARES EU workshop.

2. Identification and Analysis of Email and Contacts Artefacts on iOS and OS X

Kenneth Martin Ovens and Gordon Morison (Glasgow Caledonian University, Scotland)

Abstract: Acquiring data from cloud storage services has become increasingly important to digital forensic investigations. As more providers offer greater online storage facilities and user data is synchronised across multiple devices, an abundance of data sources has become available to assist with forensic investigations. However, such data can only become evidence when there is a thorough understanding of the data dynamics between client devices and the cloud, and there are explanations for any variations. This paper documents and analyses the artefacts created by interactions between Apple’s cloud service, email, and contacts applications. An explanation of why some artefacts synchronised over the cloud do not have matching cryptographic hashes is offered, and the ability to establish email origin on a system of multiple devices sharing a single account is established.

3. Extraction and analysis of volatile memory in Android systems: an approach focused on trajectory reconstruction based on NMEA 0183 standard

João Sousa (PCDF, Brazil) and João Gondim (UnB, Brazil)

Abstract: Android devices are widely used in the world and can function as GPS receivers. Time and position information have great relevance in investigation, however, data stored in non-volatile media may be limited with respect to the reconstruction of trajectories, since data from GPS receivers usually remains in RAM and is not written on log files, databases, and other artifacts. A prospective method for recovering data with GPS-coordinates stored in RAM memory of Android mobile devices is presented. Experiments were performed in different scenarios, with different device architectures, to analyze the feasibility of reconstruction of trajectories based on the NMEA 0183 protocol sentences retrieved from RAM memory. In developing the technique, it was possible to verify issues that can hinder the process of extraction and analysis of data and also assess tools that have been developed to aid the process.

4. Digital Forensic Artifacts of the Cortana Device Search Cache on Windows 10 Desktop

Patricio Domingues and Miguel Frade (Polytechnic Institute of Leiria, Portugal)

Abstract: Microsoft Windows 10 Desktop edition has brought some new features and updated other ones that are of special interest to digital forensics analysis. The search box available on the taskbar, next to the Windows start button is one of these novelties. Although the primary usage of this search box is to act as an interface to the intelligent personal digital assistant Cortana, in this paper, we study the digital forensic artifacts of the search box on machines when Cortana is explicitly disabled. Specifically, we locate, characterize and analyze the content and dynamics of the JSON-based files that are periodically generated by the Cortana device search cache system. Forensically important data from these JSON files include the number of times each installed application has been run, the date of the last execution and the content of the custom jump list of the applications. Since these data are collected per user and saved in a resilient text format, they can help in digital forensics, mostly in assisting the validation of other sources of information.

Workshop SecATM I – ATM Security Research and Development

Session Chair: Rainer Koelle (Lancaster University, UK)
Location: Lecture Hall E
Time: 11:00-12:30

1. Air Traffic Management Security Research in SESAR

John Hird (EUROCONTROL, Belgium), Martin Hawley (Winsland Ltd, UK) and Chris Machin (Aztech BVBA)

Abstract: The future ATM system must evolve to meet demanding performance targets. This transition will potentially introduce new vulnerabilities into the system. To address this issue, the SESAR programme has developed a comprehensive set of methods, tools and guidance material to support the concept of “designing-in” security from the beginning of the development life-cycle. This paper summarises the deliverables produced and recommendations made in the area of SESAR ATM Security.

2. A New Vision for ATM Security Management – The Security Management Platform

Claudio Porretti (FINMECCANICA S.p.A., Italy), Raoul Lahaije (42Solutions, Netherlands) and Denis Kolev (University of Lancaster, UK)

Abstract: The aim of this paper is to describe a new vision for ATM Security Management that is proposed by the GAMMA project, and implemented by its “core” prototype called Security Management Platform. GAMMA is an FP7 project with the goal of developing solutions capable to manage emerging ATM vulnerabilities. The GAMMA vision recognizes the opportunities opened by a collaborative framework for managing security, building a solution based on the self-protection and resilience of the ATM system, with the possibility to share security information in a distributed federated environment. This concept is implemented with the Security Management Platform prototype, and can be conceptualized as a network of distributed nodes embedded within the ATM system, providing interfaces to (ATM) internal and external security stakeholders. The Security Management Platform prototype provides a basis for the management of security throughout phases, from prevention to the identification of security incidents and the efficient resolution of the resulting ATM crises.

3. ‘CTRL_S’ – A security tool for SESAR’s design-in security approach

Karol Gotz, Martin Hawley (Winsland Ltd, UK), John Hird (EUROCONTROL, Belgium) and Chris Machin (Aztech BVBA, Belgium)

Abstract: To support the approach of ‘design-in security’ taken by the SESAR Programme, the authors have iteratively developed a support tool, known as ‘CTRL_S’ that guides users through the security risk assessment process. Whilst these risks are mostly generic, based on prototype system architectures or extrapolations from current systems, the approach supports the development of security controls through to operations. Key aspects of the CTRL_S tool have been to support ‘cross-sectional’ analyses of risk

assessments and to create a collaborative knowledge-based approach, whereby users may take advantage of prior risk assessments in building new ones. Future development of the tool is proposed, including alignment with SESAR's Enterprise Architecture modelling.

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

Session Chair: Peter Kieseberg (SBA Research, Austria)
Location: Lecture Hall F
Time: 11:00-12:30

1. Welcome by Workshop Chairs

Peter Kieseberg (SBA Research, Austria), Sebastian Schrittwieser (Josef Ressel Zentrum TARGET, St. Pölten University of Applied Sciences, Austria)

Keynote: "Reclaiming Digital Privacy – The Evolution of Secure Mobile Messaging"

Sebastian Schrittwieser (Josef Ressel Zentrum TARGET, St. Pölten University of Applied Sciences, Austria)

2. Notary-assisted Certificate Pinning for Improved Security of Android Apps

Georg Merzdovnik, Damjan Buhov, Artemios G. Voyiatzis and Edgar R. Weippl (SBA Research, Austria)

Abstract: The security provided to Internet applications by the TLS protocol relies on the trust we put on Certificate Authorities (CAs) issuing valid identity certificates. TLS certificate pinning is a proposed approach to defend against man-in-the-middle (MitM) attacks that are realized using valid albeit fraudulent certificates. Yet, the implementation of certificate pinning for mobile applications, and especially for Google Android apps, is cumbersome and error-prone, resulting in inappropriate connection handling and privacy leaks of user information. We propose the use of TLS notary-assisted certificate pinning at the Android Runtime level. Our approach defends against a wide range of MitM attacks without needing to update the application using TLS. Furthermore, by relying on the collective knowledge of the trusted TLS notaries, we increase both the security and the usability, while at the same time we remove the burden for the user making trust decisions about system security issues. We describe a proofof-concept implementation demonstrating its capabilities and discuss the next steps necessary towards general availability of our solution.

3. Spotting the Malicious Moment: Characterizing Malware Behavior Using Dynamic Features

Alberto Ferrante (Universita della Svizzera italiana, Switzerland), Eric Medvet (Universita di Trieste, Italy), Francesco Mercaldo (Universita del Sannio, Italy), Jelena Milosevic (Universita della Svizzera italiana, Switzerland) and Corrado Aaron Visaggio (Universita del Sannio, Italy)

Abstract: While mobile devices have become more pervasive every day, the interest in them from attackers has also been increasing, making effective malware detection tools of ultimate importance for malware investigation and user protection. Most informative malware identification techniques are the ones that are able to identify where the malicious behavior is located in applications. In this way, better understanding of malware can be achieved and effective tools for its detection can be written. However, due to complexity of such a task, most of the current approaches just classify applications as malicious or benign, without giving any further insights. In this work, we propose a technique for automatic analysis of mobile applications which allows its users to automatically identify the sub-sequences of execution traces where malicious activity happens, hence making further manual analysis and understanding of malware easier. Our technique is based on dynamic features concerning resources usage and system calls, which are jointly collected while the application is executed. An execution trace is then split in shorter chunks that are analyzed with machine learning techniques to detect local malicious behaviors. Obtained results on the analysis of 3,232 Android applications show that collected features contain enough information to identify suspicious execution traces that should be further analysed and investigated.

Workshop WMA I

Session Chair: Corrado Aaron Visaggio (University of Sannio, Italy)
Location: Lecture Hall G
Time: 11:00-12:30

1. Keynote: Learning from examples in the presence of adversaries for malware detection and classification

Giorgio Giacinto (University of Cagliari, Italy)

Abstract: Nowadays, machine learning techniques are increasingly employed to perform detection and classification tasks for computer security. Malware analysis is one of the prominent tasks, due to the vast amount of samples that need to be scrutinized daily. The effectiveness of machine learning approaches for malware classification and detection strictly depends on the effort spent in feature engineering, and in the choice of the learning function, with the goals of achieving high detection rate on known malware, reducing the false detection rate, and, in particular, making the system capable of detecting new malware samples specifically designed to evade the machine learning system. In this talk, I will outline some of the challenges posed by the current malware scenario, both for x86, and Android architectures, and some of the solutions proposed to design robust and effective malware detection and classification systems based on machine learning approaches.

2. A Peek Under the Hood of iOS Malware

Laura García (MLW.RE NPO, Spain) and Ricardo J. Rodríguez (University of Zaragoza, Spain)

Abstract: Malicious software specially crafted to proliferate in mobile platforms are becoming a serious threat, as reported by numerous software security vendors during last years. Android and iOS are nowadays the leaders of mobile OS market share. While malware targeting Android are largely studied, few attention is paid to iOS malware. In this paper, we fill this gap by studying and characterizing malware targeting iOS devices. To this regard, we study the features of iOS malware and classify samples of 36 iOS malware families discovered between 2009 and 2015. We also show the methodology for iOS malware analysis and provide a detailed analysis of a malware sample. Our findings evidence that most of them are distributed out of official markets, target jailbroken iOS devices, and very few exploit any vulnerability.

12:30 – 13:30 Lunch

13:30 – 15:00 Parallel Sessions

ARES Short II – Applications

Session Chair: Johanna Ullrich (SBA Research, Austria)
Location: Lecture Hall B
Time: 13:30-15:00

1. A Hazus-based method for assessing robustness of electricity supply to critical smart grid consumers during flood events

Alexandr Vasenev, Lorena Montoya (University of Twente, Netherlands) and Andrea Ceccarelli (University of Florence, Italy)

Abstract: Ensuring an external electricity supply to critical city components during flood events requires adequate urban grid planning. The proliferation of smart grid technologies means that such planning needs to assess how smart grids might function during floods. This paper proposes a method to qualitatively investigate robustness of electricity supply to smart grid consumers during flood events. This method builds on the Hazus methodology and aims to provide inputs for the risk analysis of urban grids.

2. Hybrid Focused Crawling for Homemade Explosives Discovery on Surface and Dark Web

Christos Iliou, George Kalpakis, Theodora Tsikrika, Stefanos Vrochidis and Ioannis Kompatsiaris (CERTH, Greece)

Abstract: This work proposes a generic focused crawling framework for discovering resources on any given topic that reside on the Surface or the Dark Web. The proposed crawler is able to seamlessly traverse the Surface Web and several darknets present in the Dark Web (i.e. Tor, I2P and Freenet) during a single crawl by automatically adapting its crawling behavior and its classifier-guided hyperlink selection strategy based on the network type. This hybrid focused crawler is demonstrated for the discovery of Web resources containing recipes for producing homemade explosives. The evaluation experiments indicate the effectiveness of the proposed approach both for the Surface and the Dark Web.

3. The Case for RAID 4: Cloud-RAID Integration with Local Storage

Christopher Hansen and James Archibald (Brigham Young University, USA)

Abstract: The proliferation of the Internet of Things (IoT) requires innovative solutions for all aspects of computing, including storage. The small footprint of IoT devices limits their capacity for local reliable storage. A solution is presented which combines local and cloud storage in a RAID-like (Redundant Array of Independent Disks) configuration, increasing the amount of storage, access speed, and/or data reliability and availability for systems which implement the discussed configurations. Previously, cloud-RAID, where data is distributed across multiple cloud storage providers, has been proposed and implemented. However, the current architectures place an emphasis on RAID 0, and other levels of RAID with their application to cloud storage have not been thoroughly explored. A novel architecture for local+cloud-RAID storage is presented, and benefits provided by the architecture in the areas of availability, reliability, and security are discussed. An effort to quantify the reliability of various configurations of RAID, cloud-RAID, and hybrid local+cloud-RAID levels will be made. While RAID 4 has been widely regarded as obsolete and supplanted by RAID 5, we argue that RAID 4 can be useful in a local+cloud-RAID configuration. A new RAID level based on RAID 4, with the addition of a second dedicated parity drive, is proposed, and is deemed RAID 4.5. We conclude that cloud storage, from the perspectives of availability, reliability, security, and performance, is beneficial to include in various RAID configurations which include local drives.

4.An Empirical Study on GSN Usage Intention: Factors Influencing the Adoption of Geo-Social Networks

Esma Aïmeur (Université de Montréal, Canada), Sébastien Gambs (Université de Québec à Montréal, Canada) and Cheu Yien Yep (Université de Montréal, Canada)

Abstract: Nowadays, geosocial networks (GSNs) have become a significant component of people's daily lives as they are one of the most popular applications that are being widely accessed through smart devices such as smartphones and tablets. Their rapid widespread use and their invasion of our private life warrant a better understanding. In particular, the impact of trust in GSN, the privacy concerns of users, their perception of risk and the social influence on the use of such mobile applications is not yet fully understood. In this paper, we study the factors influencing the usage intention of GSN users. To realize this, we propose a model based on the user's perspective. Our model focuses on four overall factors that influence the users' concerns and in turn their intention and aim of using GSNs: privacy concerns, trust, social influence and risk perception. We tested empirically the proposed research model by running a web-based survey. The participants consisted of 396 persons with at least a past experience with GSNs. The results revealed that among all the possible factors the privacy concerns, social influence and trust have a significant impact on the intention and usage of GSNs. In contrast, personality traits have almost no effects on trust or social influence. One notable exception is computer self-efficacy that was found to induce a strong influence on the four principal factors.

Workshop FARES

Session Chair: Edgar Weippl (SBA Research, Austria)
Location: Lecture Hall C
Time: 13:30-15:00

1. Collaborative Attribute Retrieval in Environment with Faulty Attribute Managers

Mario Faiella, Fabio Martinelli, Paolo Mori, Andrea Saracino and Mina Sheikhalishai (Consiglio Nazionale delle Ricerche, Italy)

Abstract: Attributes describing the features of subjects, objects and of the environment are used in access and usage control models to determine the right of a subject to use an object in a given environment. Hence, it is crucial for the effective enforcement of access and usage policies that authorization systems are able to promptly retrieve the values of the required attributes from the Attribute Providers. However, sometimes attribute providers could not respond when queried by Authorization systems, because they could be temporary down or unreachable. This could affect the decision processes, causing some requests to be unduly denied or some ongoing accesses to be unduly interrupted. This paper proposes a strategy that can be adopted by an Authorization system to estimate the value of the attributes it requires when the corresponding attribute providers are not responding. This strategy leverages on the collaboration of the other Authorization systems which exploit the same attribute providers, and which could have cached a value for the required attributes. We validate the presented approach through a set of simulative experiments which consider the presence of malicious authorization systems in the cooperative environment.

2. Recognizing Time-Efficiently Local Botnet Infections – A Case Study

Tanja Heuer, Ina Schiering, Frank Klawonn and Alexander Gabel (Ostfalia University of Applied Sciences, Germany) and Martin Seeger (NetUSE AG, Germany)

Abstract: The domain name system (DNS) is often abused by criminals as resilient infrastructure for their network architecture. Examples for malicious activities based on these networks comprise e.g. phishing, click fraud, spam, command and control structure of botnets. Most of the proposed detection methods rely on machine learning based on complex feature sets which require a considerable computational power. This paper investigates the approach of passively monitoring and analyzing DNS traffic in a time efficient manner based on machine learning on a reduced and robust feature set. For the evaluation the full DNS data stream of a regional ISP is used. To enhance the amount of traffic that can be labeled for the training process and reduce the number of false negatives in the case study, this is combined with a semi-manual labeling approach which addresses domains created by Domain-GenerationAlgorithms (DGAs). That allows also medium sized, regional service providers to train classifiers with typical DNS traffic and to deploy systems based on the approach proposed here, in the network of organizations as an alternative to cloud services. The evaluation shows that this approach is feasible and prototypes are already deployed. Hence this approach can serve as an important aspect of the internal risk management of organizations.

3. VoIP Profiler: Profiling Voice Over IP User Communication Behavior

Sainath Batthalla, Mayank Swarnkar, Neminath Hubballi (Indian Institute of Technology Indore, India) and Maitreya Natu (Tata Research Development and Design Centre, India)

Abstract: Understanding the user behavior in Voice over IP (VoIP) communication has twofold advantages. It helps in detecting anomalies and also helps in planning VoIP infrastructure deployment and optimization. Anomalies arise out of various attacks and misuses like flooding, malformed messages and spam messages. In this paper we propose VoIP Profiler a method for profiling the VoIP activities at user level. For profiling users we identify a set of parameters and compute statistics of these parameters for each user using VoIP traffic. Subsequently we use these parameters to classify users (and detect anomalies). We simulate an enterprise network and experiment with a large scale VoIP dataset and identify different types of users with high success rate.

Workshop WSDF II – Cloud Forensics

Session Chair: Richard Overill (King´s College, UK)
Location: Lecture Hall D
Time: 13:30-15:00

1. A Forensic Acquisition and Analysis System for IaaS: Architectural Model and Experiment

Saad Alqahtany, Nathan Clarke, Steven Furnell (Plymouth University, UK) and Christoph Reich (Hochschule Furtwangen University, Germany)

Abstract: Cloud computing has been advancing at a feverish pace. It has become one of the most important research topics in computer science and information systems. Cloud computing offers enterprise-scale platforms in a short time frame with little effort. Thus, it delivers significant economic benefits to both commercial and public entities. Despite this, the security and subsequent incident management requirements are major obstacles to adopting the cloud. Current cloud architectures do not support digital forensic investigators, nor comply with today's digital forensics procedures – largely due to the dynamic nature of the cloud. When an incident has occurred, an organization-based investigation will seek to provide potential digital evidence while minimizing the cost of investigation. However, all members engaging in digital forensics must rely, to a very significant degree, upon the assistance of cloud providers to present relevant evidence. Unfortunately, providers often lack appropriate tools and features to perform adequate acquisition and analysis. Therefore, dependence on the CSPs is considered one of the most significant challenges when investigators need to acquire evidence in a timely yet forensically sound manner from cloud systems. This paper aims to achieve two objectives: the first objective is the development and validation of a forensic acquisition system in an Infrastructure as a Service (IaaS) model in order to ensure organizations remain in complete control, remove the burden/liability from the CSPs and make it easy to acquire the evidence in a forensically sound and timely manner. Secondly, it is to investigate the technical implications and costs resulting from such a system on the day-to-day operation of a cloud system.

2. A Log-structured Block Preservation and Restoration System for Proactive Forensic Data Collection in the Cloud

Manabu Hirano and Hiromu Ogawa (National Institute of Technology, Toyota College, Japan)

Abstract: Preservation and data collection in cloud environments are difficult because forensic data are volatile and they are scattered in many servers. This paper describes a novel surveillance mechanism for virtual block devices on IaaS cloud environments. We first describe some related work on backup applications, versioning file systems, and virtual machine introspection systems that can be applied to cloud forensics. The proposed log-structured block preservation and restoration system can be used for recording cloud consumers' write operations on virtual block devices and for restoring the state of a virtual block device at an arbitrary point in time. This paper presents a design and an implementation of the proposed system by using Xen hypervisor. The prototype implementation achieved better read and write performance compared to the baseline driver provided by Xen when we ran four or more virtual machines simultaneously. This paper shows two forensic applications for preserved data blocks: a file tracking application and a novel diff command that supports time travel.

Workshop SecATM II – Risk Assessment and Incident Management

Session Chair: John Hird (EUROCONTROL, Belgium
Location: Lecture Hall E
Time: 13:30-15:00

1. Security Risk Assessment and Risk Treatment for Integrated Modular Communication

Hamid Asgari, Sarah Haines and Adrian Waller (Thales UK Limited, UK)

Abstract: Integrated Modular Communication (IMC) is an on-board platform to provide secure and reliable aircraft communications for a diverse set of applications. IMC is viewed as an important part of the future Air Traffic Management (ATM) infrastructure. Integrating communication links and combining diverse applications in a single platform (IMC) do come with some

risks to the ATM communications that could potentially increase vulnerabilities and make the system more prone to security attacks. There are several types of attacks on network communications such as disrupting or blocking communication, intercepting, injecting fabricated packets, accessing and modifying the information. In this study, the Security Risk Assessment Methodology (SecRAM) is applied to IMC for identifying runtime threats, assessing the risks involved, and defining measures to mitigate them. The risk assessment is performed to evaluate the impact and likelihood of occurrence of attacks relevant to the identified threats and the resulting risk levels. Consequently, specific mitigation measures as IMC's security controls are proposed to provide cyber resiliency for the IMC. The IMC security controls will be validated in an emulated testbed environment in the GAMMA project.

2. Cyber Security Incident Management in the Aviation Domain

Martin Gilje Jaatun (SINTEF ICT, Norway) and Rainer Koelle (Lancaster University, UK)

Abstract: Cyber Security Incident Management is an emerging paradigm and capability within the aviation domain. To date, limited research has addressed the requirements and developed tangible solutions for the deployment of such a capability. This paper leverages good practice and experiences from other critical infrastructure settings in order to sketch a recommendation for cyber incident response management for the aviation domain.

3. A Model-Based Approach for Aviation Cyber Security Risk Assessment

Tobias Kiesling, Josef Niederl, Jürgen Ziegler (IABG mbH, Germany) and Matias Krempel (Deutsche Flugsicherung, Germany)

Abstract: The air transport infrastructure is an attractive target for cyber-attacks due to its importance and prominence. The current system is already vulnerable and the advent of more automation and pervasion of standard IT in the future leads to ever more complex and interconnected systems with an increasing attack surface. To cope with this situation, we need suitable methods and tools to achieve understanding of the consequences in potential cyber threat situations. We propose a model-based approach for aviation cyber security risk assessment in support of holistic understanding of threats and risk in complex interconnected systems. We introduce our modeling approach and show how computer-based reasoning can be used for threat and risk analysis based on these models. This paper presents the promising results of initial research. Substantial effort is still needed to mature the approach. We expect major challenges to be of an organizational rather than technical nature.

Workshop IWSMA II

Session Chair: Sebastian Schrittwieser (Josef Ressel Zentrum TARGET, St. Pölten University of Applied Sciences, Austria)
Location: Lecture Hall F
Time: 13:30-15:00

1. Lightweight Encryption for Smart Home

Sanaah Al Salami, Joonsang Baek, Khaled Salah and Ernesto Damiani (Khalifa University, UAE)

Abstract: Smart home is one of the most popular IoT (Internet of Things) applications, which connects a wide variety of objects and home appliances in a single logical network. Smart home applications have benefited from interactions and data transmissions among different devices over the integrated network with or without human interventions. However, like other technologies, smart home likely introduces new security vulnerabilities due to its dynamic and open nature of connectivity with heterogeneous features. Among such vulnerabilities, is the breach of confidentiality which needs to be addressed urgently as data exchanged between smart home devices can contain crucial information related to user's privacy and safety. However, some of the challenges in providing smart home system with confidentiality service are the flexibility of key management and efficiency of computation and communication. These challenges should be addressed carefully as many small and resource-constrained devices are usually involved in smart home systems. In this paper, we address these challenges by proposing a lightweight encryption scheme for smart homes. This scheme will provide users and smart objects with confidentiality service without incurring much overhead cost associated with computation and communication. Our proposed scheme also supports flexible public key management through adopting identitybased encryption, which does not require complex certificate handling. We provide a formal security analysis of our scheme and a performance simulation study. The simulation shows that our scheme provides favorable level of efficiency in terms of overhead cost associated with computation and communication.

2. Hand Dynamics for Behavioral User Authentication

Fuensanta Torres Garcia, Katharina Krombholz, Rudolf Mayer and Edgar Weippl (SBA Research, Austria)

Abstract: We propose and evaluate a method to authenticate individuals by their unique hand dynamics, based on measurements from wearable sensors. Our approach utilises individual characteristics of hand movement when opening a door. We implement a sensor-fusion machine learning algorithm to classify individuals based on their hand movement and conduct a lab study with 20 participants to test the feasibility of the concept in the context of accessing physical doors as found in office buildings. Our results show that our approach yields an accuracy of 92% in classifying an individual and thus highlights the potential for behavioral hand dynamics for authentication.

3. Panel Discussion “Future of mobile integration into daily lives – Threats and Chances for Security”

Moderation: Peter Kieseberg (SBA Research, Austria)

Workshop WMA II

Session Chair: Francesco Mercaldo (University of Sannio, Italy)
Location: Lecture Hall G
Time: 13:30-15:00

1. What’s your major threat? On the differences between the network behavior of targeted and commodity malware

Enrico Mariconti, Jeremiah Onaolapo, Gordon Ross and Gianluca Stringhini (University College London, UK)

Abstract: This work uses statistical classification techniques to learn about the different network behavior patterns demonstrated by targeted malware and generic malware. Targeted malware is a recent type of threat, involving bespoke software that has been created to target a specific victim. It is considered a more dangerous threat than generic malware, because a targeted attack can cause more serious damage to the victim. Our work aims to automatically distinguish between the network activity generated by the two types of malware, which then allows samples of malware to be classified as being either targeted or generic. For a network administrator, such knowledge can be important because it assists to understand which threats require particular attention. Because a network administrator usually manages more than an alarm simultaneously, the aim of the work is particularly relevant. We set up a sandbox and infected virtual machines with malware, recording all resulting malware activity on the network. Using the network packets produced by the malware samples, we extract features to classify their behavior. Before performing classification, we carefully analyze the features and the dataset to study all their details and gain a deeper understanding of the malware under study. Our use of statistical classifiers is shown to give excellent results in some cases, where we achieved an accuracy of almost 96% in distinguishing between the two types of malware. We can conclude that the network behaviors of the two types of malicious code are very different.

2. Exploring the usage of Topic Modeling for Android Malware Static Analysis

Eric Medvet (University of Trieste, Italy) and Francesco Mercaldo (University of Sannio, Italy)

Abstract: The rapid growth in smartphone and tablet usage over the last years has led to the inevitable rise in targeting of these devices by cyber-criminals. The exponential growth of Android devices, and the buoyant and largely unregulated Android app market, produced a sharp rise in malware targeting that platform. Furthermore, malware writers have been developing detection-evasion techniques which rapidly make anti-malware technologies ineffective. It is hence advisable that security expert are provided with tools which can aid them in the analysis of existing and new Android malware. In this paper, we explore the use of topic modeling as a technique which can assist experts to analyse malware applications in order to discover their characteristic. We apply Latent Dirichlet Allocation (LDA) to mobile applications represented as opcode sequences, hence considering a topic as a discrete distribution of opcode. Our experiments on a dataset of 900 malware applications of different families show that the information provided by topic modeling may help in better understanding malware characteristics and similarities.

3. Classification of Short Messages Initiated by Mobile Malware

Marian Kühnel and Ulrike Meyer (RWTH Aachen University, Germany)

Abstract: In this paper we show that supervised machine learning algorithms can reliably detect short messages initiated by mobile malware based on features derived from the content of short messages. In particular, we compare the detection capabilities of the classifiers Support Vector Machines, K-Nearest Neighbor, Decision Trees, Random Forests, and Multinomial Naive Bayes in three different evaluation scenarios. The first scenario is the standard k-fold cross validation, treating all short messages as independent from each other. In the second scenario, we evaluate, how the classifiers perform if only a certain portion of malware families are known during training. Here, we are able to show that training with only 50% of the malware families already lead to an accuracy of over 90%. Finally, in the third scenario we evaluate the performance chronologically, i.e. the classifiers are trained with the short messages available at a certain point in time and tested on the newly arriving messages. Here, we show that classifiers can detect the majority of new short messages initiated by mobile malware even months after the training.

15:00 – 15:30 Coffee Break

15:30 – 17:00 Parallel Sessions

ARES Short III – Cryptography

Session Chair: Peter Kieseberg (SBA Research, Austria)
Location: Lecture Hall B
Time: 15:30-17:00

1. Energy Efficient Mutual Authentication and Key Agreement Scheme with Strong Anonymity Support for Secure Ubiquitious Roaming Services

Prosanta Gope, Ruei-Hau Hsu, Jemin Lee (Singapore University of Technology and Design, Singapore) and Tony Q.S. Quek (Daegu Gyeongbuk Institute of Technology and Design, South Korea)

Abstract: This article proposes a secure and energy efficient user authentication protocol, which can preserve the user anonymity for roaming service in the mobile network. Compared to other state of the art solutions, the proposed scheme has several considerable advantages. Firstly, no encryption/ decryption, modular and exponential operations have been introduced in our design. Instead, it uses the low cost function such as HMAC and exclusive-OR operations to accomplish the goals of authentication and key agreement. This makes the protocol more suitable for battery-powered mobile devices. Secondly, the proposed scheme can resolve several existing security issues like forgery attack, known session key attack, etc., with the limited computation and communication overheads which are indeed essential for offering a secure and expeditious roaming services in mobile communication environment.

2. Provable user authentication scheme in telecare medicine information system using elliptic curve cryptosystem

Toan Thinh Truong, Duong Tien Phan, Minh Triet Tran (University of Science, HCM-VNU, Vietnam), Anh Duc Duong (University of Information Technology, VNU-HCM, Vietnam) and Isao Echizen (National Institute of Informatics, Japan)

Abstract: Recently, the telecare medicine information system (TMIS) is one of the most convenient health-care deliveries. It helps the patient and doctor keep frequent connection, so the quality of medical treatment is enhanced. Two main problems needed to be considered are the security and privacy of patient. Many schemes proposed to satisfy such requirements are not suitable for public medical environment because of their some limitations. For example, the patients identity and password are not protected; time-consuming computations in such schemes take a lot of time in authentication phase. In this paper, we survey some typical previous results in this area to inherit some advantages. Afterward, we propose a provable lightweight dedicated scheme appropriate for TMIS in insecure channel.

3. Synchronous One Time Biometrics With Pattern Based Authentication

Patrick Lacharme and Christophe Rosenberger (ENSICAEN, France)

Abstract: One time passwords are commonly used for authentication purposes in electronic transactions. Nevertheless, providing such a one time password is not really a strong authentication proof because the token generating the passwords can be given by an impostor. In order to cope with this problem, biometric recognition is more and more employed. Even if biometric data are strongly linked with the user, their revocability nor diversity is possible, without an adapted postprocessing. Biometric template protection schemes, including the BioHashing algorithm, are used to manage the underlying privacy and security issues. These schemes are used for the protection of several biometric modalities, but are not necessary adapted for all of them. In this paper, we propose a new protocol combining protected biometric data and a classical synchronous one time password to enhance the security of user authentication while preserving usability and privacy. Behavioral biometrics is used to provide a fast and a usable solution for users. We show through experimental results the efficiency of the proposed method.

4. V-DIFT: Vector-Based Dynamic Information Flow Tracking with Application to Locating Cryptographic Keys for Reverse Engineering

Antonio Espinoza, Jeffrey Knockel, Jedidiah Crandall (University of New Mexico, USA) and Pedro Comesaña (University of Vigo, Spain)

Abstract: Dynamic Information Flow Tracking (DIFT) is a technique for tracking information as it flows through a program's execution. DIFT systems track information by tainting data and propagating the taint marks throughout execution. These systems are designed to have minimal overhead and thus often miss indirect flows. If indirect flows were propagated naively overtainting would result, whereas propagating them effectively causes overhead. We describe the design and evaluation of a system intended for offline analysis, such as reverse engineering, that can track information through indirect flows. Our system, V-DIFT, uses a vector of floating point values for each taint mark. The use of vectors enables us to track a taint's provenance and handle indirect flows, trading off some performance for these abilities. These indirect flows via control and address dependencies are thought to be critical to tracking information flow of cryptographic programs. Therefore we tested VDIFT's effectiveness by automatically locating keys in simple programs that use a variety of symmetric cryptographic algorithms found in three common libraries. This application does not require that the program run in real time, just that it be much faster than a manual approach. Our VDIFT implementation tests average 3.6 seconds, and with the right parameters can identify memory locations that contain keys for 24 out of 27 algorithms tested. Our results show that many cryptographic algorithm implementations' address and/or control dependencies must be tracked for DIFT to be effective.

ARES Short IV – Security Methods

Session Chair: Michael Diener (University of Regensburg, Germany)
Location: Lecture Hall C
Time: 15:30-17:00

1. Usable Privacy-aware Logging for Unstructured Log Entries

Christof Rath (Graz University of Technology, Austria)

Abstract: Log files are a basic building block of computer systems. They typically contain sensitive data, for example, information about the internal structure of a service and its users. Additionally, log records are usually unstructured in the sense that sensitive data will not occur in every entry and not always occur at defined positions within a record. To mitigate the threat of illicit access to log files, we propose a flexible framework for the creation of privacy-preserving log records. A crucial step is the annotation of sensitive data, by using arbitrary labels, during the development of a system. These labels are mapped to redaction filters to form a redaction policy. Thus, we can create two parallel log streams. One log stream contains fully redacted log entries. It, hence, does not contain any sensitive information and is intended for everyday use. The second stream contains the original entires. Here, confidentiality must be ensured. Our framework fosters privacy by default principles and can support selective disclosure of relevant data. We developed an implementation of our solution for logback, one of the major logging frameworks in Java, and successfully evaluated its applicability.

2. pwnPr3d: a Model-Based Probabilistic Threat Modeling Approach

Pontus Johnson, Alexandre Vernotte, Mathias Ekstedt and Robert Lagerström (KTH Royal Institute of Technology, Sweden)

Abstract: In this paper we introduce pwnPr3d, a probabilistic threat modeling approach for automatic attack graph generation based on network modeling. The aim is to provide stakeholders in organizations with a holistic approach that both provides high-level overview and technical details. Unlike many other threat modeling and attack graph approaches that rely heavily on manual work and security expertise, our language comes with built-in security analysis capabilities. pwnPr3d generates probability distributions over the time to compromise assets.

3. The Landscape of Domain Name Typosquatting: Techniques and Countermeasures

Jeffrey Spaulding, Shambhu Upadhyaya and Aziz Mohaisen (SUNY Buffalo, USA)

Abstract: With more than 294 million registered domain names as of late 2015, the domain name ecosystem has evolved to become a cornerstone for the operation of the Internet. Domain names today serve everyone, from individuals for their online presence to big brands for their business operations. Such ecosystem that facilitated legitimate business and personal uses has also fostered "creative" cases of misuse, including phishing, spam, hit and traffic stealing, online scams, among others. As a first step towards this misuse, the registration of a legitimatelylooking domain is often required. For that, domain typosquatting provides a great avenue to cybercriminals to conduct their crimes. In this paper, we review the landscape of domain name typosquatting, highlighting models and advanced techniques for typosquatted domain names generation, models for their monetization, and the existing literature on countermeasures. We further highlight potential fruitful directions on technical countermeasures that are lacking in the literature.

Workshop SecATM III – Testing and Validation

Session Chair: Martin Gilje Jaatun (SINTEF ICT, Norway)
Location: Lecture Hall E
Time: 15:30-17:00

1. Security Testing With Controller-Pilot Data Link Communications

Doris Di Marco (ENAV, Italy), Alessandro Manzo (SICTA, Italy), John Hird (EUROCONTROL, Belgium) and Marco Ivaldi (@Mediaservice.net, Italy)

Abstract: A security testing method and a supporting toolset were developed to evaluate the robustness of communication protocols, application end-points and other system components. Using a packet injection and manipulation test case it was demonstrated that, due to weaknesses in authentication mechanisms, the CPDLC protocol is subject to threats affecting data integrity. In order to mitigate the risks, recommendations are made for a holistic approach to implementing security controls at the Network, System, Application, Procedural, and Physical levels.

2. Addressing Security in the ATM Environment

Patrizia Montefusco (LEONARDO, Italy), Rosana Casar Rodriguez (ISDEFE, Spain), Tim H. Stelkens-Kobsch (German Aerospace Center, Germany) and Rainer Koelle (Lancaster University, UK)

Abstract: This paper addresses the full lifecycle of security countermeasures identified in the Security Risk Analysis of the future Air Traffic Management System (ATM). The process establishes new security functions identified in the GAMMA project and their implementations in order to ensure acceptable levels of security for ATM. In this project, ATM Security is addressed by focusing on two dimensions defined by Single European Sky ATM Research: establishing a collaborative support capability by defining a framework embracing three-levels for Security Management (i.e. European, National, and Local) and developing security measures for the self-protection/resilience of the ATM Systems by exploiting automated security-related functions to handle potential threats. This paper concentrates on the second dimension and how the countermeasures are identified, implemented and developed in prototypes. The prototypes will then be validated in an operational scenario, through the new concept introduced by the project. The reader will be accompanied through a practical example of the whole process on how ATM Security needs have been identified. The objective is to protect the core ATM Security functionalities (Primary Assets) and corresponding Supporting Assets. We identified 44 of the most feared threat scenarios in terms of impact on the SESAR Key Performance Areas (KPA). The threat scenario described in this paper is “False ATCO”, affecting the Supporting Asset “Voice system”. The developed prototype is “SACom” (Secure ATC Communication) that considers the security countermeasures identified in the risk treatment analysis to reduce the risks. The paper concludes with the description of the activities planned for validating the SACom prototype as part of the proposed global solution.

Workshop WMA III

Session Chair: Eric Medvet (University of Trieste, Italy)
Location: Lecture Hall G
Time: 15:30-17:00

1. Ransomware Inside Out

Francesco Mercaldo, Vittoria Nardone and Antonella Santone (University of Sannio, Italy)

Abstract: Android is currently the most widely used mobile environment. This trend encourages malware writers to develop specific attacks targeting this platform with threats designed to covertly collect data or financially extort victims, the so-called ransomware. In this paper we use formal methods, in particular model checking, to automatically dissect ransomware samples. Starting from manual inspection of few samples, we define a set of rule in order to check whether the behaviours we find are representative of ransomware functionalities.

2. Detecting Packed Executable File: Supervised or Anomaly Detection Method?

Neminath Hubballi and Himanshu Dogra (Indian Institute of Technology Indore, India)

Abstract: Executable packing is an evasion technique used to propagate malware in the wild. Packing uses compression and/or encryption to thwart static analysis. There are universal unpackers available which can extract original binary from any type of packer, however they are computationally expensive as they are based on dynamic analysis which requires malware execution. A possible approach is to use machine learning techniques for classifying whether an executable is packed or not packed. Although supervised machine learning methods are good at learning packer specific features, these require collecting data from each packer and extracting features specific to it which may not be feasible practically. In this paper we propose a semi supervised technique and an anomaly based detection method to identify packed executable files. We measure the distance between representative generated from a packed and non-packed binary training data and estimate the class based on its nearest distance in semi-supervised method. In anomaly detection we generate a representative cluster from known non-packed samples and find the radius of cluster and compare the distance of a test executable with that of radius to decide either it as normal or packed one. We experiment with few distance measures and report detection performance of these methods on two datasets.

17:00 – 19:30 Sightseeing Tour

A guided tour through the old town of Salzburg. Discover the well-known sights of the city such as the house where Mozart was born, the Old Market and the Salzburg Festival houses. Enjoy stories about the filming of "Sound of Music" while strolling through the Mirabell Garden.

Meeting point: in front of the University, buses leave 17.15 (shortly after the last session)
Tour start: 18.00
Tour end: 19.30

Buses will take us from the university to the city, you will have the possibility to store your belongings in the bus during the tour. The tour will end at the bus terminal "Paris-Lodron-Straße" (near Schloss Mirabell).

Keynotes

ARES Keynote Speakers

Koen Hermanns

EUROJUST, The European Union's Judicial Cooperation Unit, The Netherlands

Keynote: International Judicial Cooperation in the Fight against Cybercrime

Wednesday, August 31, 2016, 09.15 – 10.15

Koen Hermans is a Dutch public prosecutor, working for the EU agency Eurojust. At Eurojust he was involved in the judicial coordination of various cases, i.e. Operation Blackshades, Operation Onymous / SilkRoad 2.0 and Operation EMMA. He started his career in 1999 at the legal aid office in 's-Hertogenbosch, where he provided pro bono legal assistance and specialized in prison and migration law. Before starting his judge / public prosecutor traineeship at the Regional Court of Zwolle, he worked for several years as a (senior) lawyer at the Migration Chamber of the Court in Arnhem. In 2007, he began working as a prosecutor in Arnhem, dealing with a variety of cases (i.e. murder, homicide, armed robberies, drug trafficking) with a special focus on Cybercrime. Mr Hermans also spent one year with the Dutch division of the European Court of Human Rights in Strasbourg. He is the Vice Chair of the Eurojust Taskforce on Cybercrime, Member of the Eurojust Counter Terrorism Team and Eurojust Contact Point for Maritime Piracy.

Bernhard Schölkopf

Max-Planck-Campus Tübingen, Germany

Keynote: Toward Causal Machine Learning

Thursday, September 1, 2016, 16.30 – 17.30

Abstract: *In machine learning, we use data to automatically find dependences in the world, with the goal of predicting future observations. Most machine learning methods build on statistics, but one can also try to go beyond this, assaying causal structures underlying statistical dependences. Can such causal knowledge help prediction in machine learning tasks? We argue that this is indeed the case, due to the fact that causal models are more robust to changes that occur in real world datasets. We touch upon the implications of causal models for machine learning tasks such as domain adaptation, transfer learning, and semi-supervised learning. We also present an application to the removal of systematic errors for the purpose of exoplanet detection. Machine learning currently mainly focuses on relatively well-studied statistical methods. Some of the causal problems are conceptually harder, however, the causal point of view can provide additional insights that have substantial potential for data analysis.*

Bernhard Schölkopf is heading the Department of Empirical Inference. His scientific interests are in the field of machine learning and inference from empirical data. In particular, he studies kernel methods for extracting regularities from possibly high-dimensional data. These regularities are usually statistical ones, however, in recent years he has also become interested in methods for finding causal structures that underly statistical dependences. He has worked on a number of different applications of machine learning – in data analysis, you get "to play in everyone's backyard."

Negar Kiyavash

University of Illinois at Urbana-Champaign, US

Keynote: Data Analytic in Anonymized Networks: Is There Hope for Privacy?

Friday, September 2, 2016, 09.30 – 10.30

Abstract: *The proliferation of online social networks has helped in generating large amounts of graph data which has immense value for data analytics. Network operators, like Facebook, often share this data with researchers or third party organizations, which helps both the entities generate revenues and improve* *their services. As this data is shared with third party organizations, the concern of user privacy becomes pertinent. Hence, it becomes essential to balance utility and privacy while releasing such data. Advances in graph matching and the resulting recent attacks on graph datasets paints a grim picture. We discuss the feasibility of privacy preserving data analytics in anonymized networks and provide an answer to the question "Does there exist a regime where the network cannot be deanonymized, yet data analytics can be performed?."*

Negar Kiyavash is Willett Faculty Scholar and an Associate of Center for Advance Study at the University of Illinois at Urbana-Champaign. She is a joint Associate Professor of Industrial and Enterprise Engineering and Electrical and Computer Engineering. She is also affiliated with the Coordinated Science Laboratory (CSL) and the Information Trust Institute. She received her Ph.D. degree in electrical and computer engineering from the University of Illinois at Urbana-Champaign in 2006. Her research interests are in design and analysis of algorithms for network inference and security. She is a recipient of National Science Foundation's CAREER and The Air Force Office of Scientific Research Young Investigator awards, and the Illinois College of Engineering Dean's Award for Excellence in Research.

ARES EU Symposium Keynote Speaker

Thomas C. Stubbings

Thomas Stubbings Management Consulting eU, Austria

Keynote: Cyber-Legislation, Standardisation and Pan-European Cooperation as strategic drivers to strengthen Cybersecurity across Europe

The keynote will be held in the ARES EU Symposium 2016 on Wednesday August 31, 2016 14.30 – 15.15

***Abstract:** The ever-increasing interconnection of societies, businesses and individuals has led to a new level of cyberthreats: organised crime, fraud and cyber terrorism have a direct and tangible impact on the way we live, work and do business. The evolving threat landscape demands for new strategies of cyber protection. As part of the digital single market strategy the European Commission has developed a Cybersecurity strategy in order to foster an open, safe and secure cyberspace and digital souvereignity. Elements of this strategy are closer cooperation of member states and key stakeholders, establishment of a suitable cybersecurity legal basis and development of a security ecosystem of European standards, service offerings and service providers. The presentation will outline the current situation and key elements of the approach to strengthen Cybersecurity and manage risks at an appropriate level.*

Dr. Thomas C. Stubbings is Senior Security Expert and Strategy Consultant working for large corporates and SMEs. He is also chairman of the Cybersecurity Platform of the Austrian Federal government. Before starting his consulting business, Thomas Stubbings was 12 years Chief Security Officer and head of Group Security Management at Raiffeisen Bank International AG, leading a team of experts in 23 organizations in CEE and overseas. Before being with Raiffeisen, Thomas Stubbings worked as managing consultant at a large international consulting firm. He holds a PhD in technical sciences and several certifications in the information security and risk management area. He is invited speaker at various national and international conferences and member of the CSO roundtable.

Workshop Keynote Speakers

N. Asokan

Professor of Computer Science at Aalto University, Finland

Keynote: Securing cloud-assisted services

Workshop SECODIC 2016, Wednesday, August 31, 2016, 10.30 – 12.00

Abstract: *All kinds of previously local services are being moved to a cloud setting. While this is justified by the scalability and efficiency benefits of cloud-based services, it also raises new security and privacy challenges. Solving them by naive application of standard security/privacy techniques can conflict with other functional requirements. In this talk, I will outline some cloud-assisted services and the apparent conflicts that arise while trying to secure these services. I will then discuss a specific instance: the case of cloud-assisted detection of malicious mobile application packages and the privacy concerns involved. I will discuss how techniques for private membership test, assisted by hardware security mechanisms, can be used to address these concerns.*

Between 1995 and 2012, he worked in industrial research laboratories designing and building secure systems, first at the IBM Zurich Research Laboratory and then at Nokia Research Center. His primary research interest has been in applying cryptographic techniques to design secure protocols for distributed systems. Recently, he has also been investigating the use of Trusted Computing technologies for securing endnodes, and ways to make secure systems usable, especially in the context of mobile devices. **Asokan** received his doctorate in Computer Science from the University of Waterloo, MS in Computer and Information Science from Syracuse University, and BTech (Hons.) in Computer Science and Engineering from the Indian Institute of Technology at Kharagpur. He is an ACM Distinguished Scientist and an IEEE Senior Member.

Hugues Mercier

Research Associate at the Université de Neuchâtel, Switzerland

Keynote: Building a Secure and Resilient Cloud Architecture: Theoretical and Practical Challenges behind the SafeCloud Project

Workshop SECPID 2016, Wedneyday, August 31, 2016, 10.30 – 12.00

Abstract: *Cloud infrastructures, despite all their advantages and importance to the competitiveness of modern economies, raise fundamental questions related to the privacy, integrity, and security of offsite data storage and processing tasks. There are major privacy and security concerns about data located in the cloud, especially when data is physically located, processed, or must transit outside the legal jurisdiction of its rightful owner. These questions are currently not answered satisfactorily by existing technologies. This talk presents the objectives and challenges of the H2020 SafeCloud project. SafeCloud will re-architect cloud infrastructures to ensure that data transmission, storage, and processing can be (1) partitioned in multiple administrative domains that are unlikely to collude, so that sensitive data can be protected by design; (2) entangled with inter-dependencies that make it impossible for any of the domains to tamper with its integrity. These two principles (partitioning and entanglement) are applied holistically across the entire data management stack, from communication to storage and processing.*

Hugues Mercier received the B.Sc. degree in mathematics from Université Laval, the M.Sc. degree in computer science from the Université de Montréal, and the Ph.D. degree in electrical and computer engineering from the University of British Columbia, Canada, in 2008. From 2008 to 2011, he was a postdoctoral research fellow at the Harvard School of Engineering and Applied Sciences, and at McGill University. Currently, he is a research associate at the Université de Neuchâtel in Switzerland. My current interests are the applications of coding theory, information theory, combinatorics, and algorithms to the study of communication networks. He is the scientific and technical director of SafeCloud.

Evaldas Bruze

Lithuanian Cybercrime Centre of Excellence for Training, Research & Education (L3CE), Lithuania

Strengthening Cooperation of European Network Centres of Excellence in Cybercrime

Workshop SENCEC 2016. Wednesday, August 31, 2016, 15.15 – 16.45

***Abstract:** More than 10 Centres of Excellence (hereinafter – CoE) in the area of cybercrime are operating in Europe today. Despite some of the great achievements of certain CoE most of them have been operating mainly in isolation of each other, they have different goals and may frequently result in duplication of effort. Such a lack of visible agreement and commitment to cooperate among the CoE and the current virtual nature of the European network limits a lot the possibilities to go into any kind of mutual, long-term agreement.*

In order to synchronize the activities of different CoE, it is currently aimed (within the framework of SENTER project) to create a sustainable international cross-organizational partnership by establishment of European network, which will lead research, training and education in the area of cybercrime at the EU level, and act as a facilitator of the transfer and adoption of the best practices developed in Europe and other continents.

Possibility offered by the network of bridging the resources and using the European network as a communications, distribution & dissemination channel has encouraged European organizations (such as EUROPOL, FRONTEX, E.C.T.E.G and etc.) and industry clusters to express their support to the network.

SENCEC I aims to present the current state of development of the European network of CoE (namely, SENTER project activities) and to draw the attention of the part of scientific community concerned with the issues of cybercrime.

Evaldas Bruze – business development analyst and consultant having more than 12 years of experience in implementation, supervision and maintenance of information systems. Evaldas has considerable consulting and business management experience and has accumulated an expertise in local as well as international projects while implementing business management solutions, such as Atava, TIA, iFlex, in Lithuanian, Danish, Swedish, Netherlands, Latvian and other companies. He is currently the Deputy Director of Lithuanian Cybercrime Centre of Excellence for Training, Research & Education (L3CE).

Jarno Limnéll

Professor of Cybersecurity at Aalto University, Finland

Keynote: The Strategic Trends in Cybersecurity

Workshop ISPM 2016, Thursday, September 1, 2016, 09.30 – 11.00

***Abstract:** Cyber security is primarily a strategic issue in today´s world. This mean raising the level of discussion from mere technology to pondering the big picture – the influence of cyber security on societies as a whole. Especially multidisciplinary understanding is needed since the line between physical and digital worlds is blurring. What are the current strategic trends in cybersecurity – and cyber warfare – and how we are able to face these trends? The keynote will provide visionary ideas into the future, in order to make it more secure.*

Jarno Limnéll is the Professor of Cybersecurity in Finnish Aalto University. He also works as a Vice President of Cybersecurity in Insta Group plc. He has been working with security issues more than 20 years, and he has profound understanding of the global threat landscape, combined with the courage to address the most complex issues. Prof. Limnéll holds a Doctor of Military Science degree in Strategy from the National Defense University in Finland; a Master of Social Science degree from Helsinki University; and an Officer´s degree from the National Defense University. Mr. Limnéll has published a comprehensive list of works on security issues. His most recent book is “Cybersecurity for decision makers.” Limnéll served a long career as an officer in the Finnish Defense Forces and has worked as Director of Cybersecurity in McAfee.

Hasan Yasar
Carnegie Mellon University, US

Keynote: How to include Security into Software Lifecycle: Secure DevOps!

Workshop ASSD 2016, Thursday, September 1, 2016, 09.30 – 11.00

Abstract: *As general thought, “Software security” often evokes negative feelings among software developers since this term is associated with additional programming effort, uncertainty and road blocker activity on fast development and release cycle. To secure software, developers must follow a lot of guidelines that, while intended to satisfy some regulation or other, can be very restricting and hard to understand. As a result a lot of fear, uncertainty, and doubt can surround software security. This talk describes how the Secure DevOps movement attempts to combat the toxic environment surrounding software security by shifting the paradigm from following rules and guidelines to creatively determining solutions for tough security problems. Emphasizing a set of DevOps principles enables developers to learn more about what they are developing and how it can be exploited. Rather than just blindly following the required security practices and identified security controls, developers can understand how to think about making their applications secure. As a result, they can derive their own creative ways to solve security problems as part of understanding the challenges associated with secure software development. Rather than reacting to new attacks, secure software should be proactively focused on surviving by providing reliable software with a reduced attack surface that is quick both to deploy* and restore*. In other words, developers worry less about being hacked and more about preventing predictable attacks and quickly recovering from cyber incident. In the past, software security focused on anticipating where and how the attacks would come and putting up barriers to prevent those attacks. However, most attacks–especially sophisticated attacks–can’t be anticipated, which means that fixes are bolted on as new attacks are discovered. The inability to anticipate attacks is why we often see patches coming out in response to new 0-day vulnerabilities. Secure DevOps developers would rather their software absorb the attacks and continue to function. In other words, it should* bend *but not break. This shift in thinking from a prevent to a bend-don’t-break mindset allows for a lot more flexibility when it comes to dealing with attacks. Becoming secured lifecycle requires the development team to focus on continuous integration, infrastructure as code, eliminating denial of service (DOS), and limiting the attack surface. A look at how DevOps principles can be applied to software development process on regardless of size or industry types. The burgeoning concepts of DevOps include a number of concepts that can be applied to increasing the security of developed applications. These include adding automated security testing techniques such as fuzz testing, software penetration testing to the software development cycle or the system integration cycle. Other techniques include standardizing the integration cycle in order to reduce the possibility of the introduction of faults and introducing security concerns and constraints to software and system development teams at the inception of projects rather than applying them after the fact. Applying these and other DevOps principles can have a big impact on creating an environment that is resilient and secure. Examples of how DevOps principles were applied on projects will be discussed along with lessons learned and some ideas on how to apply them to development and acquisition. Specifically in this talk, I will clearly explain on how to address security concern at early development lifecycle and the way of addressing these threads at many decisions point. And share a reference architecture to have automation security analysis during integration or in deployment and delivery phases.*

Hasan Yasar is the technical manager of the Secure Lifecycle Solutions group in the CERT Division of the Software Engineering Institute, Carnegie Mellon University. Hasan leads an engineering group on software development processes and methodologies, specifically on DevOps and development; and researches advanced image analysis, cloud technologies, and big data problems while providing expertise and guidance to SEI’s clients. Hasan has more than 25 years’ experience as senior security engineer, software engineer, software architect and manager in all phases of secure software development and information modeling processes. He has an extensive knowledge of current software tools and techniques. He is also specialized on secure software solutions design and development experience in the cybersecurity domain including data-driven investigation and collaborative incident management, network security assessment, automated, large-scale malware triage/analysis, medical records management, accounting, simulation systems and document management. He is also Adjunct Faculty member in CMU Heinz Collage and Institute of Software Research where he currently teaches “Software and Security” and “DevOps – Modern Deployment”. His current areas of professional interests focus on: Secure Software Development including threat modeling, risk management framework and software assurance model; Secure DevOps process, methodologies and implementation; Software Development Methodologies (Agile, SAFe, DevOps); Cloud based application development, deployment and operations; Software Architecture, Design, Develop and Management of large-scale enterprise systems.

Giorgio Giacinto

Associate Professor of Computer Engineering at the University of Cagliari, Italy

Keynote: Learning from examples in the presence of adversaries for malware detection and classification

Workshop WMA 2016, Friday September 2, 2016, 11.00 – 12.30

Abstract: *Nowadays, machine learning techniques are increasingly employed to perform detection and classification tasks for computer security. Malware analysis is one of the prominent tasks, due to the vast amount of samples that need to be scrutinized daily. The effectiveness of machine learning approaches for malware classification and detection strictly depends on the effort spent in feature engineering, and in the choice of the learning function, with the goals of achieving high detection rate on known malware, reducing the false detection rate, and, in particular, making the system capable of detecting new malware samples specifically designed to evade the machine learning system. In this talk, I will outline some of the challenges posed by the current malware scenario, both for x86, and Android architectures, and some of the solutions proposed to design robust and effective malware detection and classification systems based on machine learning approaches.*

Prof. Giorgio Giacinto is Associate Professor of Computer Engineering at the University of Cagliari, Italy. He obtained the MS degree in Electrical Engineering in 1994, and the Ph.D. degree in Computer Engineering in 1999. Since 1995 he joined the research group on Pattern Recognition and Applications of the DIEE, University of Cagliari, Italy. His main research interest is in the area of pattern recognition and machine learning for computer security tasks, and he is also involved in some activities for image classification and retrieval. During his career Giorgio Giacinto has published more than one hundred papers on international journals, conferences, and books. He is a senior member of the ACM and the IEEE. He has been involved in the scientific coordination of several research projects at the local, national and international level. In particular, he coordinated two projects funded by the regional government of Sardinia, and he was involved in the scientific coordination of two EU Projects in the field of computer security, namely CyberRoad, and IllBuster. Since 2012 he is the director of the Summer School on Computer Security and Privacy “Building Trust in the Information Age”.

Artur Janicki

Assistant professor at the Institute of Telecommunications, Warsaw University of Technology, Poland

Keynote: Steganography in the Internet Telephony

Workshop IWCC 2016, Friday September 2, 2016, 11.00 – 12.30

Abstract*: Internet telephony during the last decade has become intensively used all over the world, and the VoIP traffic volume is constantly growing. It is no wonder that for a couple of years researchers have tried to use the VoIP traffic also as a carrier for hidden transmission. So far, several approaches have been proposed. They include methods based on voice payload modification, methods based on packet header modification, methods which modify packets’ arrival time, as well as hybrid methods, which combine two or more of these steganographic techniques. Various techniques have been elaborated, such as LACK, TranSteg or HideF0. These methods will be briefly explained and compared.*

Artur Janicki received MSc and PhD (1997 and 2004, respectively, both with honors) in telecommunications from the Faculty of Electronics and Information Technology, Warsaw University of Technology (WUT). Assistant Professor at the Institute of Telecommunications, WUT. In 2014 he took his sabbatical at the Multimedia Department at EURECOM, Sophia Antipolis, France. His research and teaching activities focus on speech processing, including speaker recognition, speech coding and synthesis, with elements of data mining, information theory and hidden transmission. He took part in elaborating efficient steganographic techniques for the Internet telephony using speech transcoding and pitch modification. Author or co-author of over 50 conference and journal papers, supervisor of over 40 bachelor and master theses. Member of the International Speech Communication Association (ISCA).

Christian W. Probst

Associate professor at the Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark

Keynote: Behavioural profiling for forensic attribution of attacks

Workshop WSDF 2016, Friday, September 2, 2016, 11.00 – 12.30

Abstract: *Digital forensics focusses on extraction, preservation and analysis of digital evidence obtained from electronic devices in a manner that is legally acceptable. Digital evidence, however, rarely reveals why or how it was created, or by whom. Digital investigations aim at attributing the generation of digital artefacts, and transitively of attacks they contributed to.*

The attacks we are facing today exploit vulnerabilities in the IT infrastructure, the physical infrastructure, and the human factor. Investigating such attacks consequently requires to consider all three levels both for collecting evidence and attibuting attacks. Integrating the human factor in the forensic process promises to understand the motivation of attackers, and to provide causal evidence.

In this talk we will present an approach for combining behavioral frameworks, originally developed for explanation of insider attacks, with digital forensics. The work presented is part of the TREsPASS project, which will be presented in the RESIST session at the ARES EU workshop.

Christian W. Probst is an associate professor at the Department of Applied Mathematics and Computer Science at the Technical University of Denmark. Christian’s research aims at guaranteeing the robustness of systems, from IT security to organizational security. He has developed the ExASyM model for socio-technical systems, which enables risk assessment of these systems and, eg, the identification of insider threats. The ExASyM model supports both designing secure systems and guide forensic analyses after an attack. Christian is the technical lead of the TREsPASS project.

Social Events

Every evening all participants will be picked up from the University to get together to the social events locations. If you come directly to a social event (and you are not using the organized transport) please contact us at the registration desk to find an appropriate meeting point.

Wednesday, August 31, 2016 – Welcome Reception

Our Welcome Reception will take place in a rustic setting at the Zistelalm, which is located on the mountain outside of the city. You will get the possibility to try typical Austrian dishes such as “Kasnocken” served in big pans. We are happy to announce that Dr. Pallauf, president of Salzburg´s state parliament, will give a speech during the welcome reception.

Meeting point: in front of the University, buses leave 18.15 (shortly after the last session)

Buses will take us from the university to the Zistelalm and later back to the city (the restaurant is not located in the city center).

Thursday, September 1, 2016 – Conference Dinner

Our Conference Dinner – a highlight at ARES 2016 – will take place high above the roofs of Salzburg in the high-class restaurant M32. The restaurant is located at the “Mönchsberg”, one of the five mountains in the city of Salzburg.

Meeting point: in front of the University, buses leave 17.45 (shortly after the last keynote session)

Buses will take us from the university to the city, there won’t be a transfer back to the university (the restaurant is located in the city center).

Friday, September 2, 2016 – Sightseeing Tour Salzburg

A guided tour through the old town of Salzburg. Discover the well-known sights of the city such as the house where Mozart was born, the Old Market and the Salzburg Festival houses. Enjoy stories about the filming of “Sound of Music” while strolling through the Mirabell Garden.

Meeting point: in front of the University, buses leave 17.15 (shortly after the last session)
Tour start: 18.00
Tour end: 19.30

Buses will take us from the university to the city, you will have the possibility to store your belongings in the bus during the tour. The tour will end at the bus terminal “Paris-Lodron-Straße” (near Schloss Mirabell).

Saturday, September 3, 2016 – Excursion / Day-trip

For all of our ARES 2016 participants who want to enjoy Salzburg and its surroundings a day more we will organize two different optional excursions, which will take place on Saturday, August 3, 2016. You have to be signed-up to participate in one of the excursions.

Option 1: Saturday, September 3, 2016 – Day-trip (8.30 – 18.00) Hallstatt

This daytrip will take you from Salzburg to Hallstatt (75 minutes driving time from Salzburg). The village Hallstatt is such an unbelievably spectacular place that even the Chinese have created a copy of the ancient salt mine village. But only in the original will you discover this truly unique culture with such a history all in a breath-taking mountain setting. In Hallstatt we will have a historical village tour through Hallstatt including the famous charnel house or “Bone House” in St. Michael´s Chapel. Each year, visitors from throughout the world come to admire the unusual collection of over 600 artistically painted skulls. Many of the skulls were decorated at the end of the 18th century, but a few are from even the 20th century. After the tour you will have the possibility to have a traditional lunch at the Bräugasthof Inn. Afterwards you will take a one hour tour through the world heritage museum of Hallstatt. During an impressive travel through time, you will about the history of the salt mine village of Hallstatt from the beginning of human history to the promotion of Hallstatt region to World Heritage of Humanity. Later on you will have some free time to explore Hallstatt on your own. We will arrive back in Salzburg around 6 pm.

Option 2: Saturday, September 3, 2016 – Day-trip (8.30 – 18.00) Berchtesgaden and Königssee (“king´s lake”)

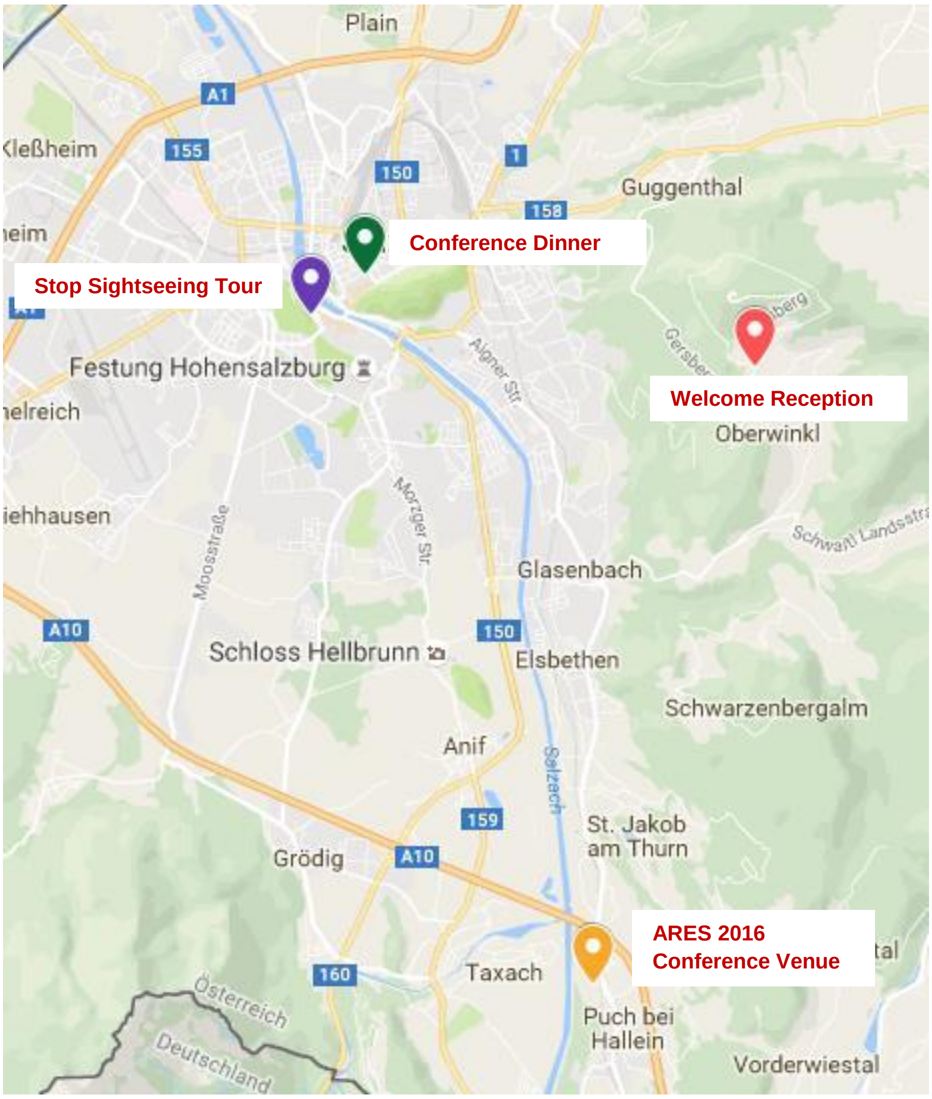
This day-trip will take you from Salzburg to the beautiful lake “Königssee” partly located in the national park “Berchtesgaden” (75 minutes driving time from Salzburg). During the one hour crossing by boat from Schönau to Salet you can enjoy the lush green forests, emerald waters and – with luck – a bright blue sky. All this surrounded by a breathtakingly beautiful backdrop consisting of the impressive Watzmann and the Berchtesgaden Alps. In Salet you will have the option to enjoy a traditional lunch, where you can also try the famous smoked fish from the Königssee and you will have some free time to walk around and admire the scenery. Afterwards we will go back by boat to Schönau and drive to the salt mine Berchtesgaden (about 15 minutes away). There we will have a 1,5 hour private tour through the mine before driving back to Salzburg. We will arrive in Salzburg around 6 pm.

Please note (mine Berchtesgaden)

- The temperature underground is constant +12 degree, whether it is summer or winter. It’s advisable to take warm clothes. You also need sturdy shoes. Attention: slip hazard!
- Additionally to your clothes you will get „miners ‘clothes” to protect your clothes.
- There are no age restrictions for children however please note, that the way underground is not suitable for baby buggies or carrying frames. Baby slings are not allowed.
- If you are a wheelchair user note that it is only possible to enter the salt mine if you have two grown strong companions, as the mine includes 2 slides, where you have to be lifted on the slide.
  In case you want to participate without visiting the salt mine, we will have an alternative as well.

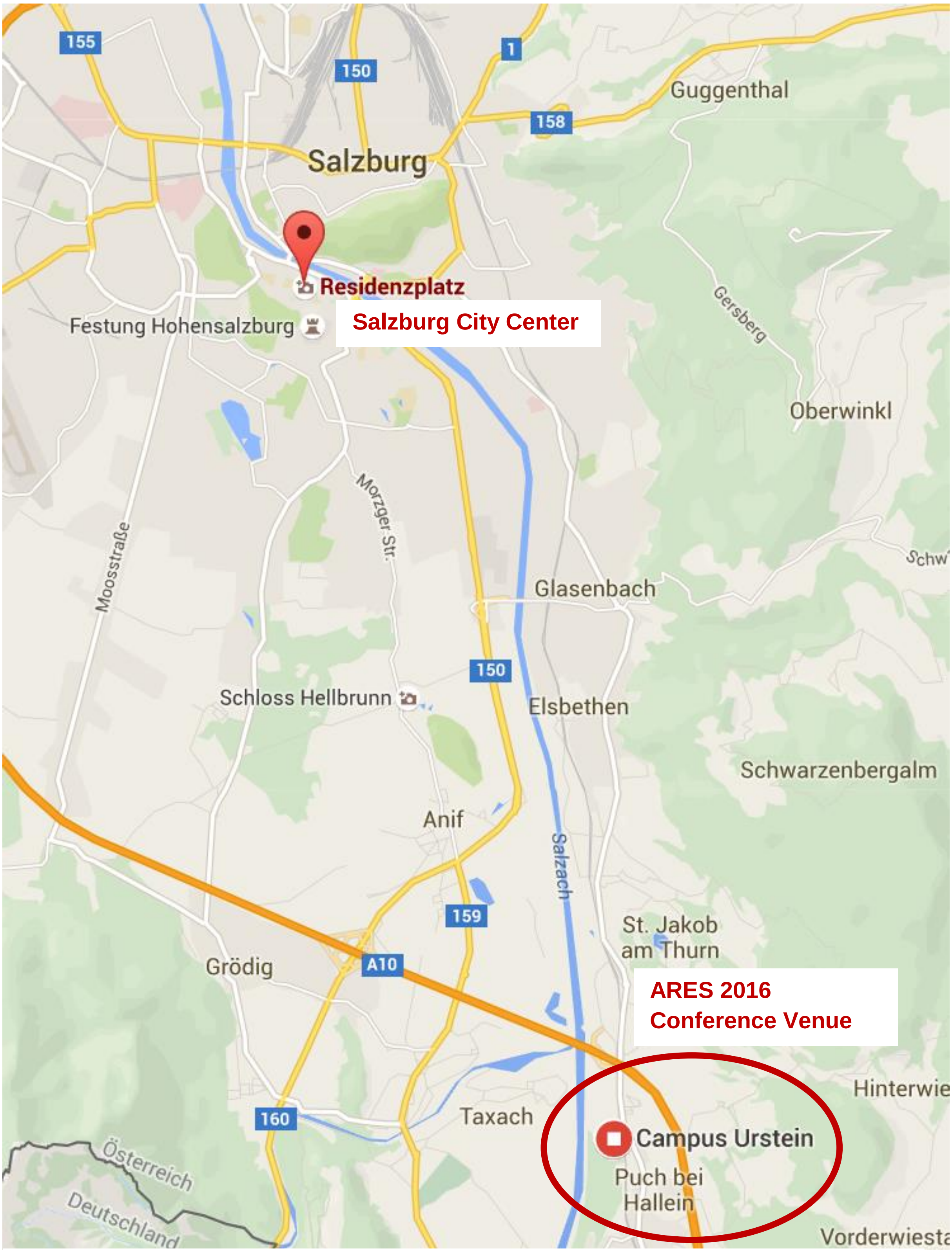
Overview Map Social Events

Below you can find an overview map of the social event locations and conference venue.



Map 1: Overview Map Social Events

Venue Overview



Map 2 Venue Overview

Conference Venue

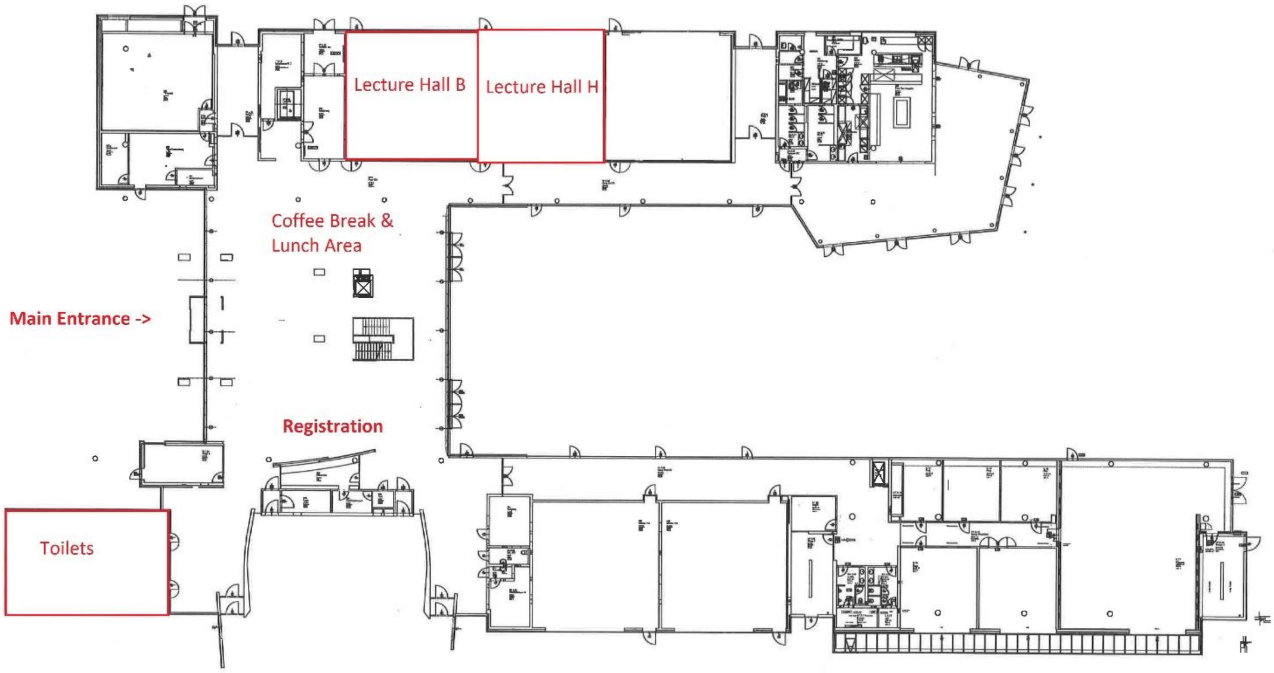
Address of the Conference Venue:
Salzburg University of Applied Sciences
Campus Urstein Süd 1
5412 Puch
Austria

The Conference Venue is located about 5 minutes walking distance away from the S-Bahn (train) S3 station “Puch- Urstein”. Signs along the way from the station to the venue will be provided. For more information see “Directions”

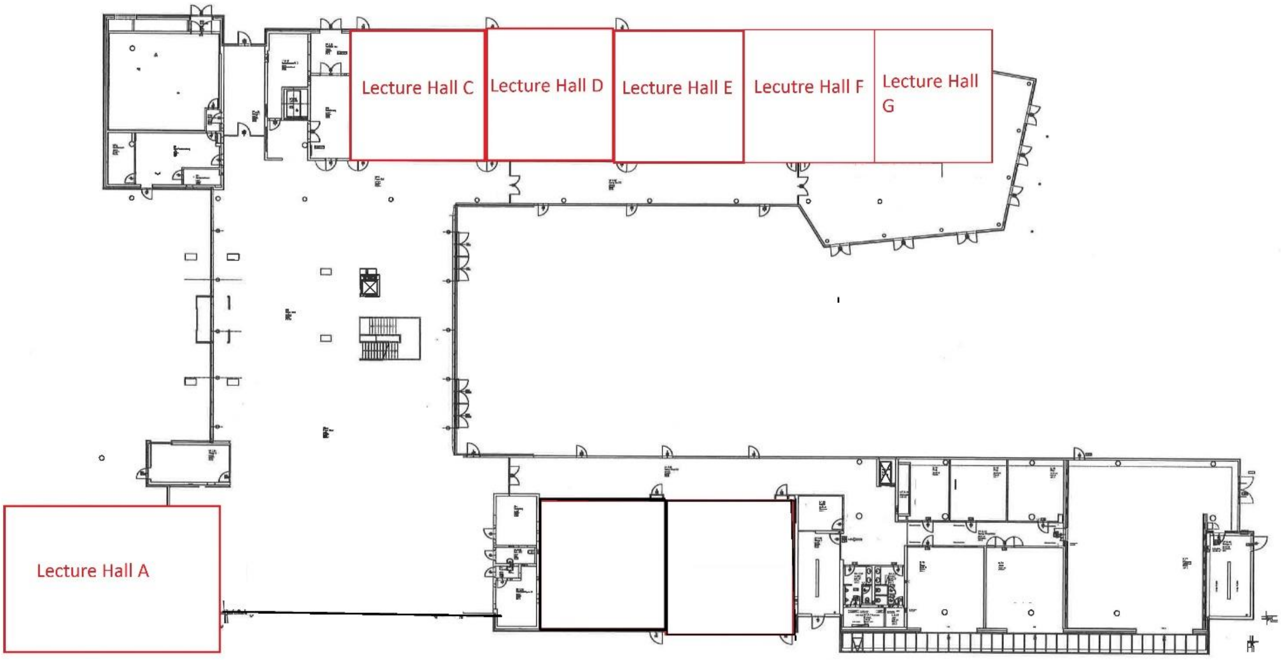
Campus – Main Entrance

Room Plans

Roomplan Ground Floor



Roomplan First Floor



Lunch Information & Menu

We will provide you with a catered lunch directly at the conference venue. There will be a joint lunch and coffee break area.

Here you can find the menu:

Wednesday, August 31, 2016
Braised beef with sour cherries, mashed potatoes and roasted onions **or** vegetable lasagne with mozzarella

Thursday, September 01, 2016
Milan style Schnitzel (chicken) with tomato-basil pasta **or** baked spinach cannelloni with cheese-corn crust

Friday, September 02, 2016
Asian chicken curry with basmati rice **or** penne "toscana" with antipasti vegetables and parmesan cheese

WIFI Information

There is WIFI available at the venue of ARES 2016:

WIFI name: ARES
Password: conference2016

Eduroam is also available.

Directions

Address of the Conference Venue:
Salzburg University of Applied Sciences
Campus Urstein Süd 1
5412 Puch
Austria

How to get from the airport to the city centre

1. Bus

Public buses go at regular intervals between Salzburg Airport, Salzburg main railway station and the city centre.
Public bus lines:

- The bus line **no 2** goes daily every 10/20 minutes between Salzburg main railway station and the airport. Sundays and public holidays every 20 min. Journey time approx. 20 min.
- The bus line **no 27** goes daily every 15/20 minutes from the airport via Wals/Viehhausen to the railway station. Journey time approx. 40 min.
- The bus line **no 10** (Mon-Sat) every 10 minutes from the airport via Salzburg city center (15 min) to Salzburg-Sam.

Costs: single ticket € 2.50, children € 1.30 (up to 15 years)
Tickets available at the "Newscorner" in the airport terminal, at the bus stop (ticket machine) or from the bus driver.

2. Taxi

A taxi stand can be found both directly in front of Salzburg main railway station and the airport terminal taking you directly to the check-in desks. Transfer airport-railway station approx. 15-20 minutes. An overview of available taxi services can be found here: http://www.salzburg-airport.com/en/passengers-visitors/arrival-parking/bus-train-taxi/taxi-transfer-service/

How to get from the airport to the Conference Venue

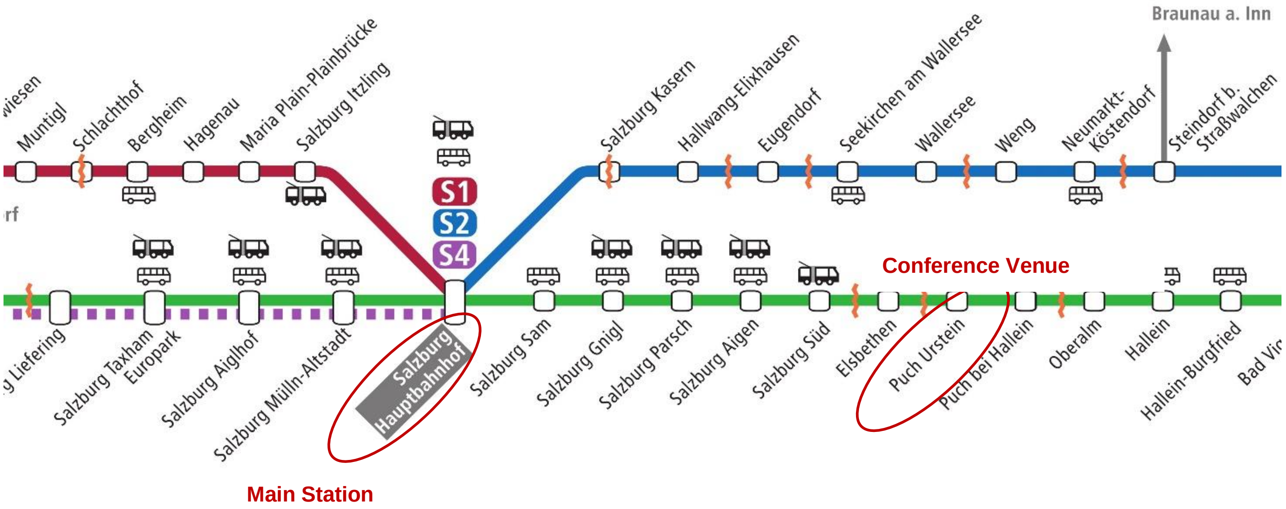
Take the bus line no 2 in direction “Salzburg Obergnigl”. Get out at “Salzburg Aiglhof S-Bahn” and change to the S-Bahn S3 in direction “Schwarzach-St.Veit Bahnhof”. Get out at the station “Puch Urstein (FH)”, from there it´s just 5 minutes´ walk to the venue.

How to get from the city to the Conference Venue:

1. Train

From Salzburg Central Station (“Salzburg Hauptbahnhof”), trains of the rapid transit line S3 in directions “Golling-Abtenau”, “Saalfelden” or “Schwarzach St. Veit” (you can take any of the trains S3 in these destinations) run every 30 minutes. Get off at the station “Puch Urstein” (see Map 3), which is located right next to the campus. Then follow the signs „Fachhochschule“ to get to the ARES 2016 Conference Venue (use the passage underground). Travel time is approx. 20 minutes. You can find a journey planner here: http://fahrplan.oebb.at/bin/query.exe/en

Below you can see an overview of the S-Bahn network in Salzburg. S3 is the green line.



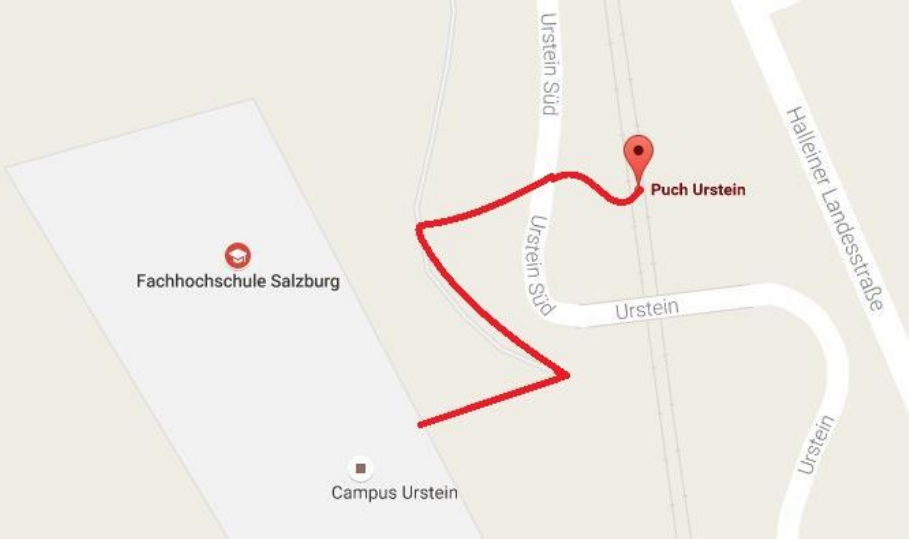
Map 3 Public Transportation Overview

Below you can find a timetable overview for S3:

From the City Center				To the City Center			
Stop	**First Train**	**Last Train**	**Intervals**	**Stop**	**First Train**	**Last Train**	**Intervals**
Salzburg HBF (main train station	6.21 am	0.21am	every 30 minutes (6.21, 6.51, 7.21,..)	**Puch Urstein**	5.54 am	23.23 pm	every 30 minutes (5.53, 6.23, 6.53,…)

Walking Distance from the stop “Puch Urstein (FH)” to the conference venue

Here you can see an overview how to get from the train stop “Puch Urstein (FH) to the conference venue.



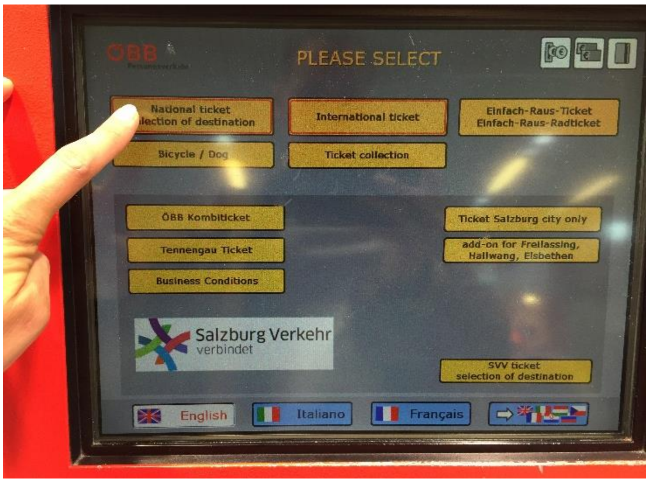
Map 4: Walking distance S-Bahn – Venue

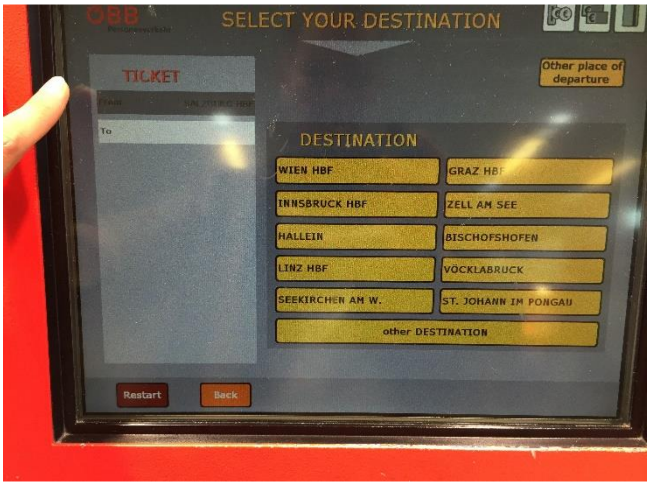
After getting out at the stop “Puch Urstein (FH) follow the signs „Fachhochschule“ to get to the ARES 2016 Conference Venue (use the passage underground) (see pictures below).

How to buy a ticket for the public transportation (using the rapid transit line S3)

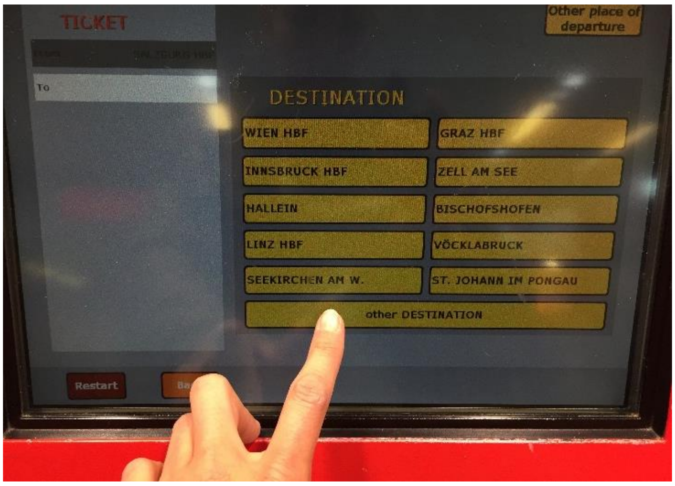
(in case you are not using the provided shuttle service)

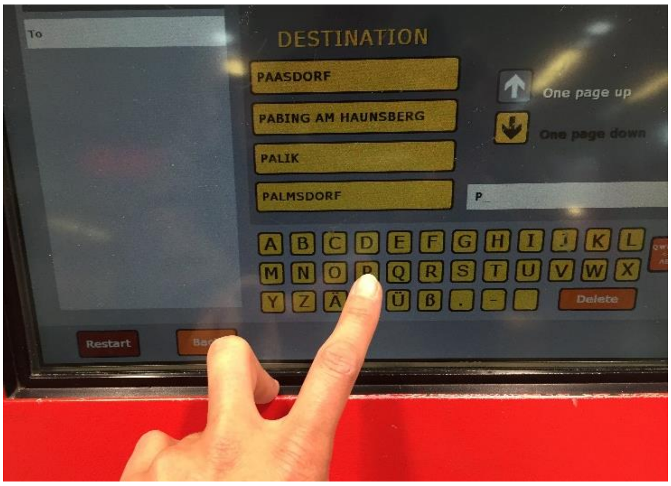
1. Select “national ticket”


ÖBB
PLEASE SELECT
National ticket selection of destination
International ticket
Einfach-Raus-Ticket Einfach-Raus-Radticket
Bicycle / Dog
Ticket collection
ÖBB Kombiticket
Tennengau Ticket
Business Conditions
Ticket Salzburg city only
add-on for Freilassing, Hallwang, Elsbethen
Salzburg Verkehr verbindet
SVV ticket selection of destination
English
Italiano
Français

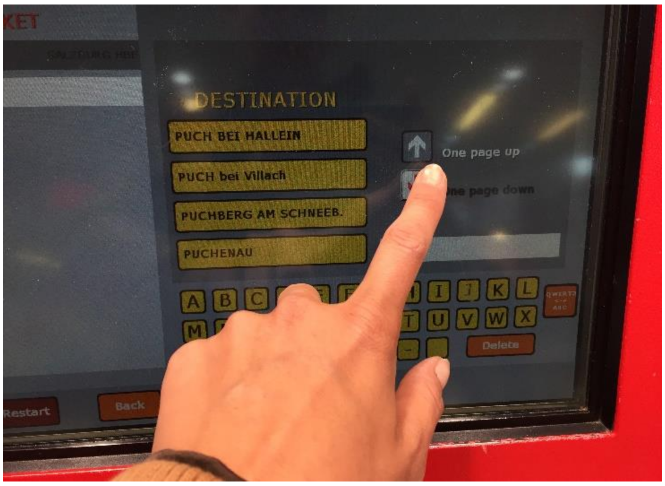


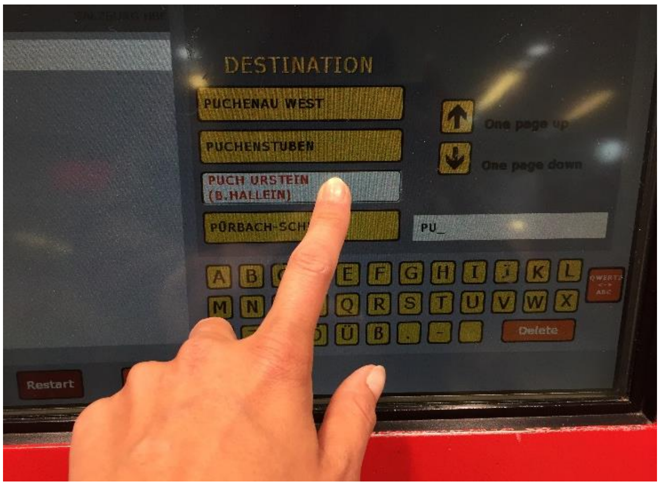
2. Select “other destination” and type in “Puch” (if you buy a ticket from the University back to Salzburg City Center type in here: “Salzburg HBF”)



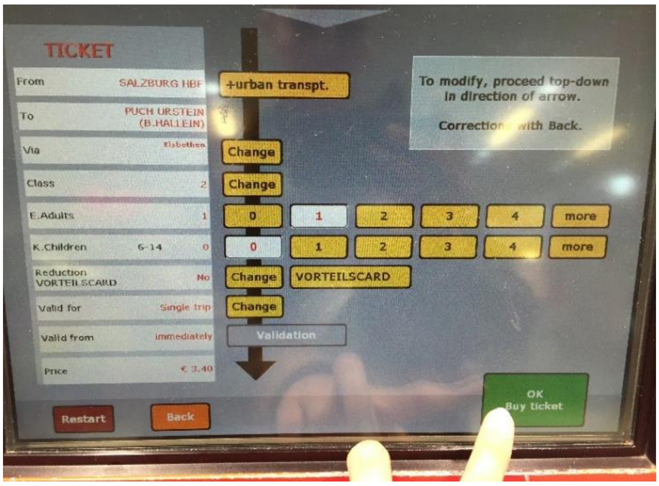


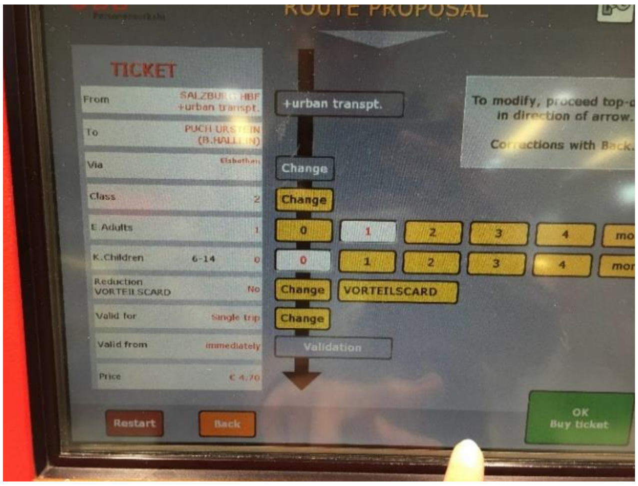
3. Click “one page down”, select “Puch Urstein (B. Hallein)”





4. A one-way ticket costs 3,40 €, If you select “+ urban transport” (transport you can use in the whole city center) a ticket costs 4,70 €





2. ARES 2016 shuttle service:

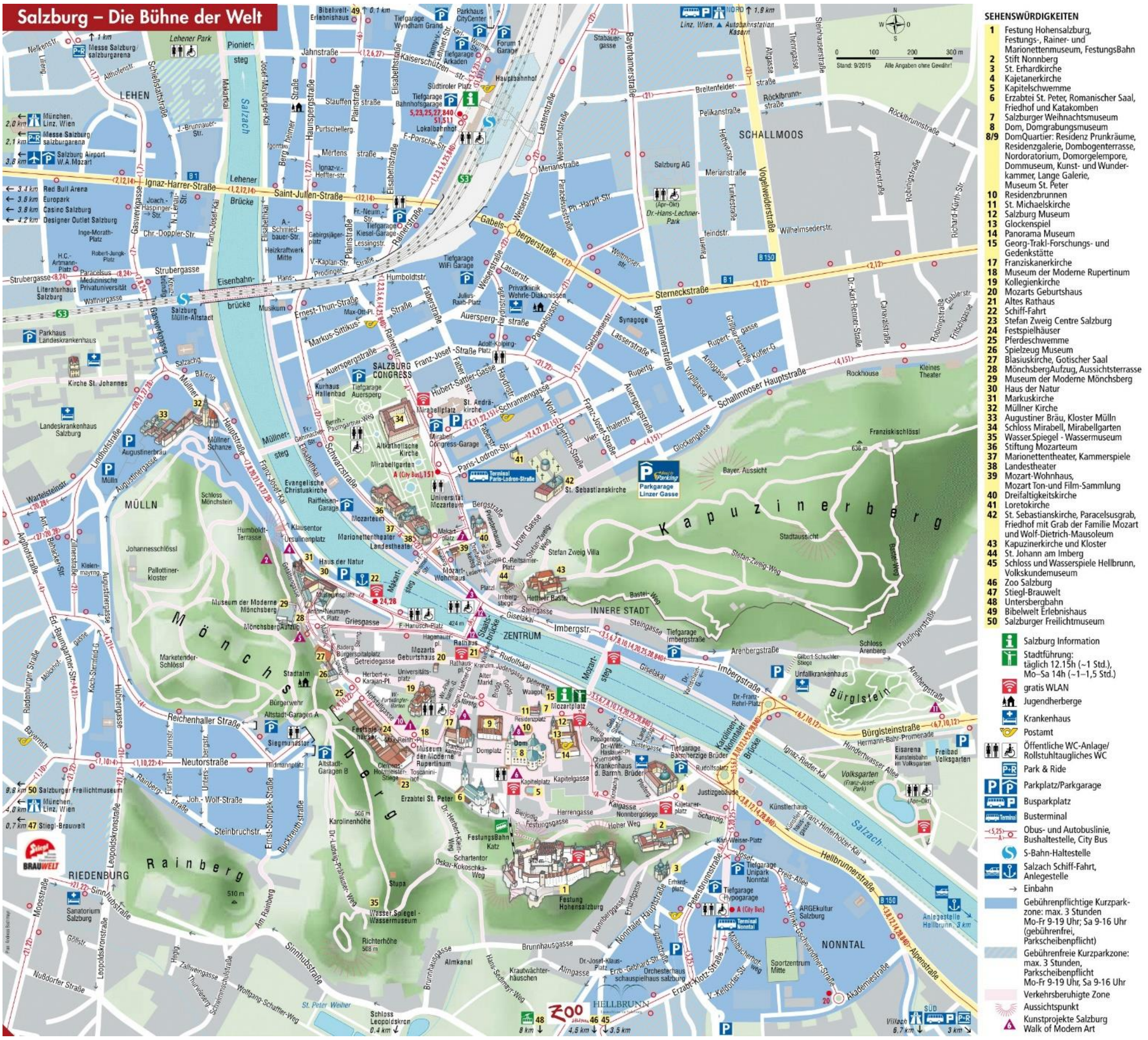
As the conference will take place at the Salzburg University of Applied Sciences, which is not located directly in the city center of Salzburg, ARES 2016 will provide a shuttle service, which is free of charge. Please note that it is necessary to sign up, if you want to use the shuttle service, to do so please **contact us.**

There will be three shuttles operating each morning between the City Center and the Conference location. The participants will be picked up between 7.50 am to 8.30 am on Wednesday, August 31, 2016 and 8.15 am to 9.00 am on Thursday September 01, 2016 as well as on Friday, September 03, 2016. The detailed timetable for the ARES 2016 shuttle service will be published on the website and it will available at the registration. Below you can find an overview with the shuttle stops and to which stop you should go if you stay at a different hotel.

Shuttle Stops ARES	
the bus will stop at these hotels to pick you up	
Name of the hotel	**Address**
Hotel am Mirabellenplatz (Austrotel)	Paris-Lodron-Straße 1, 5020 Salzburg
Meininger Hotel Salzburg City Center	Fürbergstraße 18-20, 5020 Salzburg
Mercure Salzburg Central	Sterneckstrasse 20, 5020 Salzburg
Mercure Salzburg City	Bayerhamerstraße 14A, 5020 Salzburg
Motel One Salzburg Süd	Alpenstraße 92, 5020 Salzburg
NH Salzburg City	Franz-Josef-Straße 26, 5020 Salzburg
Sheraton Salzburg Hotel	Auerspergstraße 4, 5020 Salzburg
Wyndham Grand Salzburg Conference Center	Fanny-von-Lehnert-Straße 7, 5020 Salzburg
Which stop to use if you stay at a different hotel	
Name of the hotel you stay in	**Shuttle stop to use for your convenience**
AirBnB (Poschingerstraße 10)	Meininger Hotel Salzburg City Center
AllYouNeed Hotel Salzburg	NH Salzburg City
Altstadt Hotel Hofwirt Salzburg	NH Salzburg City
Bergland Hotel	Mercure Salzburg Central
BEST WESTERN PLUS Amedia Art Salzburg	Meininger Hotel Salzburg City Center
Crown Plaza	Sheraton Salzburg Hotel
Gasthaus Adlerhof	Wyndham Grand Salzburg Conference Center
Gasthaus im Priesterseminar Salzburg	Hotel am Mirabellenplatz (Austrotel)
Holiday Inn Salzburg City	Mercure Salzburg Central
Hotel Ibis Salzburg Nord	Mercure Salzburg Central
Hotel Markus Sittikus	Sheraton Salzburg Hotel
Hotel Mozart	NH Salzburg City
JUFA Hotel Salzburg City	Motel One Salzburg Süd
Motel One Salzburg Mirabell	Sheraton Salzburg Hotel
Ramada Hotel Salzburg City Centre	Wyndham Grand Salzburg Conference Center
Star Inn Hotel Salzburg Zentrum	Hotel am Mirabellenplatz (Austrotel)

If you stay at a different hotel you can go to one of the hotels listed above and take the shuttle from there No shuttle service is provided in the evenings as all participants will be picked up every day from the conference venue to get to the social event locations. All social events will end it the city center (either by bus or the social event is in the city center anyway).

City Map Salzburg


Salzburg – Die Bühne der Welt
SEHENSWÜRDIGKEITEN
1 Festung Hohensalzburg, Festungs-, Rainer- und Marionettenmuseum, FestungsBahn
2 Stift Nonnberg
3 St. Erhardkirche
4 Kajetanerkirche
5 Kapitelschwemme
6 Erzabtei St. Peter, Romanischer Saal, Friedhof und Katakomben
7 Salzburger Weihnachtsmuseum
8 Dom, Domgrabungsmuseum
8/9 DomQuartier: Residenz Prunkräume, Residenzgalerie, Dombogenterrasse, Nordoratorium, Domorgelempore, Dommuseum, Kunst- und Wunderkammer, Lange Galerie, Museum St. Peter
10 Residenzbrunnen
11 St. Michaelskirche
12 Salzburg Museum
13 Glockenspiel
14 Panorama Museum
15 Georg-Trakl-Forschungs- und Gedenkstätte
17 Franziskanerkirche
18 Museum der Moderne Rupertinum
19 Kollegienkirche
20 Mozarts Geburtshaus
21 Altes Rathaus
22 Schiff-Fahrt
23 Stefan Zweig Centre Salzburg
24 Festspielhäuser
25 Pferdeschwemme
26 Spielzeug Museum
27 Blasiuskirche, Gotischer Saal
28 MönchsbergAufzug, Aussichtsterrasse
29 Museum der Moderne Mönchsberg
30 Haus der Natur
31 Markuskirche
32 Müllner Kirche
33 Augustiner Bräu, Kloster Mülln
34 Schloss Mirabell, Mirabellgarten
35 Wasser.Spiegel - Wassermuseum
36 Stiftung Mozarteum
37 Marionettentheater, Kammerspiele
38 Landestheater
39 Mozart-Wohnhaus, Mozart Ton-und Film-Sammlung
40 Dreifaltigkeitskirche
41 Loretokirche
42 St. Sebastianskirche, Paracelsusgrab, Friedhof mit Grab der Familie Mozart und Wolf-Dietrich-Mausoleum
43 Kapuzinerkirche und Kloster
44 St. Johann am Imberg
45 Schloss und Wasserspiele Hellbrunn, Volkskundemuseum
46 Zoo Salzburg
47 Stiegl-Brauwelt
48 Untersbergbahn
49 Bibelwelt Erlebnishaus
50 Salzburger Freilichtmuseum
Salzburg Information
Stadtführung: täglich 12.15h (~1 Std.), Mo–Sa 14h (~1–1,5 Std.)
gratis WLAN
Jugendherberge
Krankenhaus
Postamt
Öffentliche WC-Anlage/ Rollstuhltaugliches WC
Park & Ride
Parkplatz/Parkgarage
Busparkplatz
Busterminal
Obus- und Autobuslinie, Bushaltestelle, City Bus
S-Bahn-Haltestelle
Salzach Schiff-Fahrt, Anlegestelle
Einbahn
Gebührenpflichtige Kurzparkzone: max. 3 Stunden Mo-Fr 9-19 Uhr; Sa 9-16 Uhr (gebührenfrei, Parkscheibenpflicht)
Gebührenfreie Kurzparkzone: max. 3 Stunden, Parkscheibenpflicht Mo-Fr 9-19 Uhr, Sa 9-16 Uhr
Verkehrsberuhigte Zone
Aussichtspunkt
Kunstprojekte Salzburg Walk of Modern Art
Stand: 9/2015
Alle Angaben ohne Gewähr!
LEHEN
SCHALLMOOS
MÜLLN
ZENTRUM
INNERE STADT
NONNTAL
RIEDENBURG
Kapuzinerberg
Mönchsberg
Rainberg
Salzach

Map 5: City Map Salzburg

Welcome to Salzburg!

Useful Information

Tourist Information

Tourist Info – Mozartplatz
Mozartplatz 5
5020 Salzburg
Austria

Opening Hours:
August: daily 9am-7pm
September (01-8): daily 9am - 6.30pm

Emergency Numbers	
Fire service	122
Police	133
Ambulance/ rescue	144
European emergency	112

Drinking Water

It is perfectly safe to drink the tap water in Austria. However only drink water from public water dispensers if it is mentioned there that the water is drinkable.

Opening hours shops in Salzburg

Shops are usually open Mon - Fri from 9.00 am - 6.30 pm, Sat until 5.00 pm or 6.00 pm; some shopping centres are open until 8.00 pm or 9.00 from Mon-Fri. Shopping is available on Sundays and holidays at the large railway stations, at the airport and in the museum shops.

Drugstores are open from Monday to Friday from 8.00 am - 6.00 pm, usually without a lunch break, and on Saturday from 8.00 am - 12.00 noon. Outside of these times, a 24-hour drugstore standby service is available throughout the city. Details of the nearest open drugstore are posted at every drugstore. For telephone information, call the number 1455.

Public Transport Information

Ticket Prices:

Ticket Type	Price Central Zone	Price from City Centre to ARES	Additional Information
Single Ticket	1.8 €/2.6 €*	3.5 €	
5 Trips by person	9 €		
09/17 Ticket	1.5 €		Valid in one direction between 9pm to 5am
Day Pass	3.7€/ 5.7€ *	7 €	Unlimited trips during 1 day
*Price if bought from Conductor/Bus driver			

Night service

A number of buses (lines 1-7 & 24) leave from Rathaus, Hanuschplatz and Theatergasse in all directions at 11:15 pm, 11:45 pm, 00:15 am and 00:45 am.

Bus line 3 guarantees connection to Salzburg's local train service (night trains: leaving at midnight and at 2:00 am). A Bus Taxi service from Hanuschplatz and Theatergasse is also available from Sunday through Thursday, every 30 minutes - starting at 11:30 pm

Where to buy your ticket

- Automatic Ticket Dispenser
- On board from the bus driver
- From certain approved retailers (Tobacconists) in the metropolitan area

Connections

The tickets allow you to travel on any S-Bahn, tram or bus. **Attention**: making a return journey on the same line, or recommencing your journey on the same line, will be considered as 2 separate journeys.

Tipping:

Tipping in restaurants in Austria is the norm - but there is no fixed rate. A normal tip in Austria will amount up to 10% of the bill, normally rounded up to a convenient number.

About Salzburg

Salzburg is storybook Austria. Standing beside the fast-flowing Salzach River, your gaze is raised inch by inch to the Altstadt's mosaic of graceful domes and spires, the formidable clifftop fortress and the mountains beyond. It's a view that never palls. It's a backdrop that once did the lordly prince-archbishops and home-grown genius Mozart proud.

Salzburg is located in a very pretty part of Austria, where the Alps meet the flatter hill region to their north, with lots of lakes within easy reach in the Salzkammergut and the Salzburger Seenland. The city itself is situated by the river Salzach and at an altitude of approximately 430 metres; it is shaped by several hills. The exceptionally well-preserved Medieval and Baroque old town (city center) is testimony to the wealth of the former city-state. This was primarily due to salt and gold mining in the south of Salzburg. The heyday of the principality was in the 17th century, when Salzburg was among the richest areas in Europe.

As tempting as it is to spend every minute in the Unesco-listed Altstadt, drifting from one baroque church and monumental square to the next in a daze of grandeur, Salzburg rewards those who venture further. Give Getreidegasse's throngs the slip, meander side streets where classical music wafts from open windows, linger decadently over coffee and cake, and let Salzburg slowly, slowly work its magic.

Beyond Salzburg's two biggest money-spinners – Mozart and The Sound of Music – hides a city with a burgeoning arts scene, wonderful food, manicured parks and concert halls that uphold musical tradition 365 days a year. Everywhere you go, the scenery, the skyline, the music and the history send your spirits soaring higher than Julie Andrews' octave-leaping vocals.

Most of the sights can be seen on a stroll through Salzburg's historic city center: the Residence, the Carillon, the Cathedral, the Franciscan Church, Mozart Square, the Horse Pond, Hofstallgasse, St. Peter's Monastery. The spirit of days gone past can be felt at every turn: the ages have left their mark on the churches, towers, façades, balustrades and galleries. Even the street names commemorate the people and events that shaped its history.

A number of palaces in the city and its vicinity beckon invitingly: Mirabell Palace, whose Marble Hall is used for wedding ceremonies, and the Mirabell Gardens, one of the most spectacular photo scenes in Salzburg. Hellbrunn Palace to the south of the city is known for its wondrous trick fountains in the summer and its charming Christmas market in the winter. Klessheim Palace in Wals, Leopoldskron Palace and Aigen Palace and its park are worth a trip into the countryside.

A host of outstanding galleries and museums such as the Museum of Modern Art, the Rupertinum, Mozart's Birthplace, the Mozart Residence, Salzburg Museum, the Cathedral Museum, the Baroque Museum and the Toy Museum invite visitors to a lazy afternoon of browsing. Precious objects of art, modern works of art and the occasional bizarre exhibit are there to admire and appreciate.

Whether you decide to explore Salzburg on foot, by horse-drawn carriage, on a cruise, by bike, by bus or alone – the city reveals its beauty from many different perspectives. Climb the Kapuzinerberg or Mönchsberg for a stunning view of the city on the river with its characteristic architecture, colorful façades and tin roofs and beyond to the Gaisberg and Untersberg. Explore the surrounding towns and countryside on one of the many sightseeing tours.

Sources: Lonely Planet, Salzburg Info

Salzburger Mozartkugeln

A box of Salzburger Mozartkugeln by Mirabell combines the best Austria has to offer: history, music and tradition.

In 1890 Salzburg confectioner PAUL FÜRST created the “Original Salzburger Mozartkugel”, known today around the world. His delicious treat made from marzipan and pistachio surrounded by nougat and dark chocolate quickly became the city’s most famous confection.

Long after Wolfgang Amadeus Mozart died, Salzburg's master confectioner Paul Fürst started to produce little Marzipan balls, rolled them in a walnut-nougat crème, and put them on little sticks. He then dunked them into warm chocolate until they became evenly round. The original Mozartkugel was born. He chose the name Mozartkugel to pay his respects to Salzburg’s own Wolfgang Amadeus Mozart, who at the time was actually not very popular. It was the new speciality’s quality and its delicate taste that made the Mozartkugel such a great success. The original Fürst bakery is still producing the delicious Mozartkugeln by hand. Their authentic chocolate balls are sold at Alter Markt, Mirabellplatz Ritzerbogen and Getreidegasse.

Nowadays there are several companies making Mozartkugeln however the original ones are only available in shops of the Fürst bakery in the city of Salzburg and online.

Tourism Information Salzburg:

Here are some websites that provide further information and suggestions for your stay in Salzburg:
http://www.salzburg.info/en
http://www.visit-salzburg.net/
http://www.austria.info/uk/where-to-go/cities/salzburg
https://www.lonelyplanet.com/austria/salzburg

Survive in Austria… ☺

How are you? (informal)	Wie geht's?	*Vee-gates?*
How are you? (formal)	Wie geht es Ihnen?	*Vee gate ess eenen?*
Do you speak English?	Sprechen Sie Englisch?	*Sprecken zee English?*
Hello (in person)	Guten Tag	*Gutten Targ*
Good evening	Guten Abend	*Gutten Arbend*
I understand	Ich verstehe	*Ich fer-stay*
I don't understand	Ich verstehe das nicht	*Ich fer-stay dass nicht*
I don't know	Ich weiß es nicht	*Ich vice ess nicht*
Help!	Hilfe!	*Hill-fer!*
Thank you	Dankeschön	*Danker-shern*
Thank you very much	Vielen Dank!	*Feelen Dank!*
Where is....?	Wo ist...?	*Voh ist...?*
The Train station	Der Bahnhof	*Derr Barn-hoff*
Restroom	Toilette/WC	*Toilet/Vay-See*
The Airport	Der Flughafen	*Derr Floog-harfen*
The Post Office	Der Post	*Derr Posst*
I'm looking for...	Ich suche...	*Ich soo-kerr...*
I would like...please	ich möchte...bitte	*Ich muk-ter...bi-tuh*
a glass of water	ein Glas Wasser	*ayn glahs vah-ser*
"check" please (I would like to pay, please)	Zahlen, bitte	*S(t)ah-len, bit-tuh*
How do you say...in German?	Wie sagt man...auf Deutsch?	*Vee sakt mahn...of Doitsch?*
What is.......?	Was ist......?	*Vass ist...?*
Who is......?	Wer ist......?	*Verr ist...?*
When is......?	Wann ist......?	*Van ist...?*
Why is......?	Warum ist......?	*Varrum ist...?*
Cell phone/Mobile	Handy	*Handy*

Conference Office / Contact

If you need any support, please do not hesitate to contact us.

Yvonne Poul
ypoul@sba-research.org
Tel: +43 699 100 41 066

Bettina Bauer
bbauer@sba-research.org
Tel: +43 664 254 03 14

Wien Works & GWS – two companies with a social cause

Sustainability and supporting social responsible projects/ companies is very important for us. This year ARES is starting its cooperation with two new companies; Wien Works (printing company which printed the program for ARES 2016) and GWS (integrative company that produced the conference bags for ARES 2016).

Wien Works

Wien Work is an innovative non-profit, multi-faceted social economy organisation charged with creating and finding jobs for people with disabilities and persons experiencing disadvantages on the labour market. People with disadvantages, chronic conditions or long-term unemployed persons get the chance to take part in the economic and social process. Currently, about 600 people are employed at Wien Work. Two thirds of the employees and apprentices have physical or sensorial disabilities, learning disabilities or have been long-term unemployed.

GWS

GWS is an integrative company that integrates disabled people (that cannot work in conventional companies due to the type and degree of their handicaps) into working processes. The company has 480 employees of whom 80% are handicapped. GWS has three difference business areas: Merchandise & Souvenirs, Industrial Assembly and Clean Room Assembly.