ESORICS 2015

ESORICS 2015

Program Guide

Workshop only

21 – 25 September 2015
Vienna, Austria

www.esorics2015.sba-research.org

Organized by…

SBA Research

Supported by…

HUAWEI

Contents

Welcome

It is our great pleasure to welcome you to the 20th European Symposium on Research in Computer Security (ESORICS 2015).

This year's symposium continues its tradition of establishing a European forum for bringing together researchers in the area of computer security, by promoting the exchange of ideas with system developers and by encouraging links with researchers in related areas.

The call for papers attracted 293 submissions – a record in the ESORICS series – from 41 countries. The papers went through a careful review process and were evaluated on the basis of their significance, novelty, technical quality, as well as on their practical impact and/or their level of advancement of the field's foundations. Each paper received at least three independent reviews, followed by extensive discussion. We finally selected 59 papers for the final program, resulting in an acceptance rate of 20 %.

The program was completed with keynote speeches by Sushil Jajodia, George Mason University Fairfax, USA and Richard Clayton, University of Cambridge, UK. Further, we are happy to welcome Afonso Ferreira, European Commission, who will give an invited talk. The co-located PhD Symposium will give nine PhD students the opportunity to present their current work and receive feedback from the community.

Putting together ESORICS 2015 was a 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 (more than 880 reviews were written) and providing feedback for authors. There is a long list of people who volunteered their time and energy to put together and organize the conference, and who deserve special thanks: the ESORICS Steering Committee, and its chair Pierangela Samarati in particular, for their support; Giovanni Livraga, for taking care of publicity; Javier Lopez, as workshop chair, and all workshop co-chairs, who organized workshops co-located with ESORICS; and Yvonne Poul for the local organization and the social events.

Finally, we would like to thank our sponsors, HUAWEI, for the financial support and SBA Research, for hosting and organizing ESORICS 2015.

A different country hosts the conference every year. ESORICS 2015 takes place in Vienna, Austria at the Vienna University of Technology. We are very happy to host the 20th edition of the symposium in Vienna and we tried to put together a special social program for you, giving you the opportunity to share ideas with other researchers and practitioners from institutions around the world and see all the beautiful sights of Vienna.

We hope that you find this program interesting and thought-provoking and that you enjoy ESORICS 2015 and Vienna.

Günther Pernul
ESORICS 2015 General Chair
Universität Regensburg, Germany

Peter Y A Ryan
ESORICS 2015 Program Chair
University of Luxembourg, Luxembourg

Edgar Weippl
ESORICS 2015 Program Chair
SBA Research, Austria

Program Overview

The detailed time slots for all workshops can be seen in the according workshop session.

	Monday, Sept 21				Tuesday, Sept 22			
	LH E	LH B	LH C		LH E	LH F	LH C	LH B
08:00 - 17:00	REGISTRATION			08:00 - 17:00	REGISTRATION			
09:00 - 10:30	STM I	SIoT I	QASA & DPM I	09:00 - 10:30	STM V	SHCIS I	CyberICS & WOS-CPS & DPM-QASA Lecture Hall C	
10:30 - 11:00	Break			10:30 - 11:00	Break			
11:00 - 12:30	STM II	SIoT II	QASA I	11:00 - 12:30	STM VI	SHCIS II	DPM IV	CyberICS I
12:30 - 14:00	Lunch			12:30 - 14:00	Lunch			
14:00 - 15:30	STM III	SIoT III	DPM II	14:00 - 15:30	STM VII (short papers)	SHCIS III	DPM V	WOC-CPS
15:30 - 16:00	Break			15:30 - 16:00	Break			
16:00 - 17:30	STM IV (ERCIM PhD Award) Business Meeting	SIoT IV	DPM III	16:00 - 17:30		SHCIS IV	DPM VI	Cyber-ICS II
18:00 - 22:30	Workshop Dinner							

Monday, 21st September 2015

08.00-17.00 Registration

09.00-10.30 STM I: Security metrics and classification

Session Chair: Riccardo De Masellis (FONDAZIONE BRUNO KESSLER, Italy)

Lecture Hall E

1. Digital Waste Sorting: A Goal-Based, Self-Learning Approach to Label Spam Email Campaigns

Mina Sheikhalishai (Université Laval, Canada), Andrea Saracino (Consiglio Nazionale delle ricerche, Italy), Mohamed Mejri, Nadia Tawbi and Fabio Martinelli (Université Laval, Canada)

Abstract: Fast analysis of correlated spam emails may be vital in the effort of finding and prosecuting spammers performing cybercrimes such as phishing and online frauds. This paper presents a self-learning framework to automatically divide and classify large amounts of spam emails in correlated labeled groups. Building on large datasets daily collected through honeypots, the emails are firstly divided into homogeneous groups of similar messages (campaigns), which can be related to a specific spammer. Each campaign is then associated to a class which specifies the goal of the spammer, i.e. phishing, advertisement, etc. The proposed framework exploits a categorical clustering algorithm to group similar emails, and a classifier to subsequently label each email group. The main advantage of the proposed framework is that it can be used on large spam emails datasets, for which no prior knowledge is provided. The approach has been tested on more than 3200 real and recent spam emails, divided in more than 60 campaigns, reporting a classification accuracy of 97% on the classified data.

2. Integrating Privacy and Safety Criteria into Planning Tasks

Anna Lavygina, Alessandra Russo and Naranker Dulay (Imperial College London, UK)

Abstract: In this paper we describe a new approach that uses multicriteria decision making and the analytic hierarchy process (AHP) for integrating privacy and safety criteria into planning tasks. We apply the approach to the journey planning using two criteria: (i) a willingness-toshare-data (WSD) metric to control data disclosure, and (ii) the number of unsatisfied safety preferences (USP) metric to mitigate risky journeys.

3. Security Metrics, Secure Elements, and Operational Measurement Trust in Cloud Environments

Teemu Kanstrén and Antti Evesti (VTT, Finland)

Abstract: Operational security assurance evaluation requires building security metrics models to express the expected security status of the system, and collecting data from the operational system to express the current state against these models. Many factors impact the confidence we can have in these metrics and their reported status. One major factor is the trust we can put in the provided measurement data. This paper describes the properties of a trusted measurement base, use of secure element functions and different probe form factors, and their impact on defining confidence levels for the measurement data. A way of quantifying this confidence level and using it as part of security metrics models is defined. Cloud computing is used as a domain to illustrate these concepts and the process of their application. The cloud environment is especially challenging for this type of assurance due to mixed ownership and potentially limited visibility into the infrastructure.

09.00-10.30 SIoT I: Security and Privacy

Lecture Hall B

1. Welcome message

2. Keynote: IoT Security Threats, Research Challenges, and Industrial Ecosystems

Dr. Tieyan Li and Dr. Guilin Wang, (Huawei, China)

09.15-10.30 QASA & DPM I: Quantitative Aspects of Security Assurance

Session Chair: Fabio Martinelli (Université Laval, Canada)

Lecture Hall C

1. General Welcome

2. Composable Bounds on Information Flow from Distribution Differences.

Megumi Ando and Joshua D. Guttman (The MITRE Corporation, USA)

Abstract: We define information leakage in terms of a “difference” between the a priori distribution over some remote behavior and the a posteriori distribution of the remote behavior conditioned on a local observation from a protocol run. Either a maximum or an average may be used. We identify a set of notions of “difference;” we show that they reduce our general

leakage notion to various definitions in the literature. We also prove general composability theorems analogous to the data processing inequality for mutual information, or cascading channels for channel capacities.

3. Quantitative Analysis of Network Security with Abstract Argumentation.

Artsiom Yautsiukhin (University of Perugia, Italy) and Francesco Santini (IIT-CNR, Italy)

Abstract: Abstract Argumentation Framework (AAF) is a useful technique for the analysis of arguments supporting or discouraging decisions (i.e., information can be in conflict). In particular, we apply Abstract Argumentation to support the administration of security in computer networks. Our approach captures the high-level topology of a system and helps to specify which and where security countermeasures are more appropriate. We apply a quantitative analysis on the Abstract Argumentation Framework that represents our knowledge, with the purpose to compare different decisions and select the most suitable ones.

10.30-11.00 Coffee Break

11.00-12.30 STM II: Data Protection

Lecture Hall E

1. A Declarative Framework for Specifying and Enforcing Purpose-aware Policies

Riccardo De Masellis (Trento RISE, Italy), Chiara Ghidini and Silvio Ranise (Bruno Kessler Foundation, Italy)

Abstract: Purpose is crucial for privacy protection as it makes users confident that their personal data are processed as intended. Available proposals for the specification and enforcement of purpose-aware policies are unsatisfactory for their ambiguous semantics of purposes and/or lack of support to the run-time enforcement of policies. In this paper, we propose a declarative framework based on a first order temporal logic that allows us to give a precise semantics to purpose aware policies and to reuse algorithms for the design of a run-time monitor enforcing purpose-aware policies. We also show the complexity of the generation and use of the monitor which, to the best of our knowledge, is the first such a result in literature on purpose-aware policies.

2. How to Trust the Re-Use of Data

Erisa Karafili, Hanne Riis Nielson and Flemming Nielson (Technical University of Denmark, Denmark)

Abstract: Research in natural sciences and life sciences involve carrying out experiments to collect data as well as carrying out analysis to interpret the data. Increasingly data is being made available to other scientists in big databases. The scientific process builds on the idea that research results can be independently validated by other researchers. However, the concern about the correct re-use of data is also increasing. As illustrated by a currently evolving case of alleged scientific mispractice there is a need to support a reliable re-use of data. To solve this challenge we introduce an enriched coordination language based on Klaim that can model the coordination of the re-use of data in the research community. We define the formal semantics of our language and develop a static analysis that can be used to check whether we have a trustable re-use of data.

3. Towards Balancing Privacy and Efficiency: A Principal-Agent Model of Data-Centric Business

Christian Zimmermann and Claus-Georg Nolte (University of Freiburg, Germany)

Abstract: Personal data has emerged as a crucial asset of the digital economy. However, unregulated markets for personal data severely threaten consumers' privacy. Based upon a commodity-centric notion of privacy, this paper takes a principal-agent perspective on data-centric business. Specifically, this paper presents an economic model of the privacy problem in data-centric business, in that drawing from contract theory. Building upon a critical analysis of the model, this paper analyzes how regulatory and technological instruments could balance efficiency of markets for personal data and data-subjects' right to informational self-determination.

11.00-12.40 SIoT II: Secure Protocols

Lecture Hall B

1. Smart Insiders: Exploring the Threat from Insiders using the Internet-of-Things

Jason Nurse, Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith and Sadie Creese (University of Oxford, UK)

Abstract: The Internet-of-Things (IoT) is set to be one of the most disruptive technology paradigms since the advent of the Internet itself. Market research company Gartner estimates that around 4.9 billion connected things will be in use in 2015, and around 25 billion by 2020. While there are substantial opportunities accompanying IoT, spanning from Healthcare to Energy, there are an equal number of concerns regarding the security and privacy of this plethora of ubiquitous devices. In this position paper we approach security and privacy in IoT from a different perspective to existing research, by considering the impact that IoT may have on the growing problem of insider threat within enterprises. Our specific aim is to explore the extent to which

IoT may exacerbate the insider-threat challenge for organizations and overview the range of new and adapted attack vectors. Here, we focus especially on (personal) devices which insiders bring and use within their employer's enterprise. As a start to addressing these issues, we outline a broad research agenda to encourage further research in this area.

2. BALSA: Bluetooth Low Energy Application Layer Security Add-on

Diego Ortiz-Yepes (Radbound University, Netherlands)

Abstract: Bluetooth Low Energy (BLE) is ideally suited to exchange information between mobile devices and Internet-of- Things (IoT) sensors. It is supported by most recent consumer mobile devices and can be integrated into sensors enabling them to exchange information in an energy-efficient manner. However, when BLE is used to access or modify sensitive sensor parameters, exchanged messages need to be suitably protected, which may not be possible with the security mechanisms defined in the BLE specification. Consequently we contribute BALSA, a set of cryptographic protocols, a BLE service and a suggested usage architecture aiming to provide a suitable level of security. In this paper we define and analyze these components and describe our proof-of-concept, which demonstrates the feasibility and benefits of BALSA.

3. Secure Association for the Internet of Things

Almog Benin, Sivan Toledo and Eran Tromer (Tel-Aviv University, Israel)

Abstract: Existing standards (ZigBee and Bluetooth Low Energy) for networked low-power wireless devices do not support secure association (or pairing) of new devices into a network: their association process is vulnerable to man-in-the-middle attacks. This paper addresses three essential aspects in attaining secure association for such devices. First, we define a user-interface primitive, oblivious comparison that allows users to approve authentic associations and abort compromised ones. This distills and generalizes several existing approve/abort mechanisms, and moreover we experimentally show that OC can be implemented using very little hardware: one LED and one switch. Second, we provide a new Message Recognition Protocol (MRP) that allows devices associated using oblivious comparison to exchange authenticated messages without the use of public key cryptography (which exceeds the capabilities of many IoT devices). This protocol improves upon previously proposed MRPs in several respects. Third, we propose a robust definition of security for MRPs that is based on universal composability, and show that our MRP protocol satisfies this definition.

4. REST-ful CoAP Message Authentication

Hoai Viet Nguyen and Luigi Lo Iacono (Cologne University of Applied Sciences, Germany)

Abstract: One core technology for implementing and integrating the architectural principles of REST into the Internet of Things (IoT) is CoAP, a REST-full application protocol for constrained networks and devices. Since CoAP defaults to UDP as transport protocol, the protection of CoAP-based systems is realized by the adoption of DTLS, a transport-oriented security protocol for datagrams. This is, however, in many cases not a sufficient safeguard, since messages in distributed systems—as obtained, e.g., by the adoption of REST—are commonly transported via multiple intermediate components. This induces the need for message-oriented protection means supplementing transport security for IoT scenarios with high security demands. This paper approaches an important part of this requirement by introducing a REST-ful CoAP message authentication scheme. The overarching goal of this work is, though, to establish a message-oriented security layer for CoAP. Here, specific challenges are stemming from the architectural style REST and the resource-restrictiveness of IoT networks and devices. The present contribution reaches this goal for authentication by proposing a REST-ful CoAP message signature generation and verification scheme.

11.00-12.50 QASA II: Security Assurance and Reputation

Session Chair: Joaquin Garcia-Alfaro (TELECOM SudParis, France)

Lecture Hall C

1. Security-Based Runtime Adaptation of Multi-Cloud Applications.

Kyriakos Kritikos (ICS-FORTH, Greece) and Philippe Massonet (CETIC, Belgium)

Abstract: Multi-cloud application management is promoted as an approach optimizing the provisioning of cloud-based applications for two main factors: exploit whole variety of services offered by cloud providers and avoid vendor lock-in. To enable such management, model-driven approaches promise to partially automating the provisioning process. However, such approaches tend to neglect security aspects and focus only on low-level infrastructure details or quality of service aspects. As such, our previous work proposed a particular security meta-model, bridging the gap between high- and low-level security requirements and capabilities, able to express security models exploited by a planning algorithm to derive an optimal

application deployment plan by considering both types of security requirements. This work goes one step further by focusing on runtime adaptation of multi-cloud applications based on security aspects. It advocates using adaptation rules, expressed in the event-condition-action form, which drive application adaptation behavior and enable assuring a more-or-less stable security level. Firing such rules relies on deploying security metrics and adaptation code in the cloud to continuously monitor rule event conditions and fire adaptation actions for applications when the need arises.

2.AdIDoS - Adaptive and Intelligent Fully-Automatic Detection of Denial-of-Service Weaknesses in Web Services.

Christian Altmeier (Software AG, Germany), Christian Mainka, Juraj Somorovsky and Jörg Schwenk (Ruhr University Bochum, Germany)

Abstract: Denial-of-Service (DoS) attacks aim to affect availability of applications. They can be executed using several techniques. Most of them are based upon a huge computing power that is used to send a large amount of messages to attacked applications, e.g. web services. Web services apply parsing technologies to process incoming XML messages. This enlarges the amount of attack vectors since attackers get new possibilities to abuse specific parser features and complex parsing techniques. Therefore, web service applications apply various countermeasures, including message length or XML element restrictions. These countermeasures make validations of web service robustness against DoS attacks complex and error prone. In this paper, we present a novel adaptive and intelligent approach for testing web services. Our algorithm systematically increases the attack strength and evaluates its impact on a given web service, using a black box approach based on server response times. This allows one to automatically detect message size limits or element count restrictions. We prove the practicability of our approach by implementing a new WS-Attacker plugin and detecting new DoS vulnerabilities in widely used web service implementations.

3. An integrated reward and reputation mechanism for MCS preserving users privacy

Cristian Tanas, Sergi Delgado-Segura and Jordi Herrera-Joancomartí (Universitat Autònoma de Barcelona, Spain)

Abstract: Mobile Crowd Sensing (MCS) presents numerous and unique research challenges most of them based on the fact that human participation is in the loop. In this paper we analyze three of the most important: user participation, data sensing quality and user anonymity. To solve them, we present PaySense, a general framework for user rewarding and reputation accountability that preserves users' privacy using cryptocurrencies. Furthermore, we detailed an implementable system using Bitcoins.

12.30-14.00 Lunch Break

14.00-15.30: STM III: Intrusion detection and software vulnerabilities

Session Chair: Andrea Saracino (IIT-CNR, Italy)

Lecture Hall E

1. The AC-Index: Fast Online Detection of Correlated Alerts

Andrea Pugliese, Antonino Rullo and Antonio Piccolo (University of Calabria, Italy)

Abstract: We propose an indexing technique for alert correlation that supports DFA-like patterns with user-defined correlation functions. Our *AC-Index* supports (i) the retrieval of the top-*k* (possibly noncontiguous) sub-sequences, ranked on the basis of an arbitrary user provided severity function, (ii) the concurrent retrieval of sub-sequences that match any pattern in a given set, (iii) the retrieval of partial occurrences of the patterns, and (iv) the online processing of streaming logs. The experimental results confirm that, although the supported model is very expressive, the AC-Index is able to guarantee a very high efficiency of the retrieval process.

2. Intrusion Detection System for Applications using Linux Containers

Amr Abed, Charles Clancy (Virginia Tech, USA) and David Levy (The MITRE Corporation, USA)

Abstract: Linux containers are gaining increasing traction in both individual and industrial use, and as these containers get integrated into mission-critical systems, real-time detection of malicious cyber-attacks becomes a critical operational requirement. This paper introduces a real-time host-based intrusion detection system that can be used to passively detect malfeasance against applications within Linux containers running in a standalone or in a cloud multi-tenancy environment. The demonstrated intrusion detection system uses bags of system calls monitored from the host kernel for learning the behavior of an application running within a Linux container and determining anomalous container behavior. Performance of the approach using a database application was measured and results are discussed.

3. SUDUTA: Script UAF Detection Using Taint Analysis

John Galea and Mark Vella (University of Malta, Malta)

Abstract: Use-after-free (UAF) vulnerabilities are caused by the use of dangling pointers. Their exploitation inside script engine-hosting applications, e.g. web browsers, can even bypass state-of-the-art countermeasures. This work proposes SUDUTA (**S**cript **U**AF **D**etection **U**sing **T**aint **A**nalysis), which aims at facilitating the diagnosis of UAF bugs during vulnerability analysis and improves an existent promising technique based on dynamic taint tracking. Firstly, precise taint analysis rules are presented in this work to clearly specify how SUDUTA manages the taint state. Moreover, it shifts its analysis to on-line, enabling instrumentation code to gain access to the program state of the application. Lastly, it handles the presence of custom memory allocators that are typically utilized in script-hosting applications. Results obtained using a benchmark dataset and vulnerable applications validate these three improvements.

14.00-15.30 Slot III: Users and Privacy

Lecture Hall B

1. Keynote: IOT Security and Data Integrity using 3GPP Authentication

Gustavo Tanoni (Ericsson, Canada)

2. Keynote: On Security Threats in IoT with Mobile Guard

Dr. Joerg Abendroth (Nokia, Germany)

14.00-15.30 DPM II and Invited Talk DPM-QASA

Session Chair: Fabio Martinelli (Université Laval, Canada)

Lecture Hall C

1. Stronger Security for Sanitizable Signatures.

Stephan Krenn (AIT Austrian Institute of Technology GmbH, Austria), Kai Samelin (IBM Research, Switzerland) and Dieter Sommer (Technical University of Darmstadt, Germany)

Abstract: Sanitizable signature schemes (SSS) enable a designated party (called the sanitizer) to alter admissible blocks of a signed message. This primitive can be used to remove or alter sensitive data from already signed messages without involvement of the original signer. Current state-of-the-art security definitions of SSSs only dene a \weak" form of security. Namely, the unforgeability, accountability and transparency definitions are not strong enough to be meaningful in certain use-cases. We identify some of these use-cases, close this gap by introducing stronger definitions and show how to alter an existing construction to meet our desired security level. Moreover, we clarify a small yet important detail in the state-of-the-art privacy definition. Our work allows to deploy this primitive in more and different scenarios.

2. Invited talk DPM-QASA: Data Security and Privacy in the Cloud

Pierangela Samarati (Università degli Studi di Milano, Italy)

Abstract: The rapid advancements in Information and Communication Technologies (ICTs) have enabled the emerging of the cloud as a successful paradigm for conveniently storing, accessing, processing, and sharing information. With its significant benefits of scalability and elasticity, the cloud paradigm has appealed companies and users, which are more and more resorting to the multitude of available providers for storing and processing data. Unfortunately, such a convenience comes at a price of loss of control over these data and consequent new security threats that can limit the potential widespread adoption and acceptance of the cloud computing paradigm. In this talk I will illustrate some security and privacy issues arising in the cloud scenario, focusing in particular on the problem of guaranteeing confidentiality and integrity of data stored or processed by external cloud providers.

15.30-16.00: Coffee Break

16.00-17.00: STM IV (ERCIM PhD Award) Business Meeting

Lecture Hall E

1. Preserving Privacy in Data Release

Giovanni Livraga (Università degli Studi di Milano, Italy)

16.00-17.45 SIoT IV: Security Attacks and Threats

Lecture Hall B

1. On the security and privacy of Internet of Things architectures and systems

Emmanouil Vasilomanolakis, Jörg Daubert (AGT International, Switzerland), Manisha Luthra (Technische Universität Darmstadt, Germany), Vangelis Gazis, Alexander Wiesmaier and Panagiotis Kikiras (AGT International, Switzerland)

Abstract: The Internet of Things (IoT) brings together a multitude of technologies, with a vision of creating an interconnected world. This will benefit both corporations as well as the end-users. However, a plethora of security and privacy challenges need to be addressed for the IoT to be fully realized. In this paper, we identify and discuss the properties that constitute the uniqueness of the IoT in terms of the upcoming security and privacy challenges. Furthermore, we construct requirements induced by the aforementioned properties. We survey the four most dominant IoT architectures and analyze their security and privacy components with respect to the requirements. Our analysis shows a mediocre coverage of security and privacy requirements. Finally, through our survey we identify a number of research gaps that constitute the steps ahead for future research.

2. Multiple Fault Attack on PRESENT with a Hardware Trojan Implementation in FPGA

Jakub Breier and Wei He (Nanyang Technological University, Singapore)

Abstract: Internet of Things connects lots of small constrained devices to the Internet. As in any other environment, communication security is important and cryptographic algorithms are one of many elements that we use in order to keep messages secure. It is necessary to use algorithms that do not require high computational power, lightweight ciphers are therefore an ideal candidate for this purpose. Since these devices work in various environments, it is necessary to test security of implementations of cryptographic algorithms. In this paper, we explore a possibility of attacking an ultra-lightweight cipher PRESENT by using a multiple fault attack. Utilizing the Differential Fault Analysis technique, we were able to recover the secret key with two faulty encryptions and an exhaustive search of 216 remaining key bits. Our attack aims at four nibbles in the penultimate round of the cipher, causing faulty output in all nibbles of the output. We also provide a practical attack scenario by exploiting Hardware Trojan (HT) technique for the proposed fault injection in a Xilinx Spartan-6 FPGA.

3. Characterizing and Comparing the Energy Consumption of Side Channel Attack Countermeasures and Lightweight Cryptography on Embedded Devices

David Mccann, Kerstin Eder and Elisabeth Oswald (University of Bristol, UK)

Abstract: This paper uses an Instruction Set Architecture (ISA) based statistical energy model of an ARM Cortex-M4 microprocessor to evaluate the energy consumption of an implementation of AES with different side channel attack (SCA) countermeasures and an implementation of lightweight ciphers PRESENT, KLEIN and ZORRO with and without Boolean first order masking. In this way, we assess the additional energy consumption of using different SCA countermeasures and using lightweight block ciphers on 32 bit embedded devices. In addition to this, we provide a methodology for developing an ISA based energy model for cryptographic software with an accuracy of _5%. In addition to providing our methodology for developing this model, we also show that using variations of instructions that reduce the size of code can reduce the energy consumption by as much as 30% 40% and that memory instructions reduce the predictability of our energy model.

4. Not so Smart: On Smart TV Apps

Marcus Niemietz, Juraj Somorovsky, Christian Mainka and Joerg Schwenk (Ruhr-University Bochum, Germany)

Abstract: One of the main characteristics of Smart TVs are apps. Apps extend the Smart TV behavior with various functionalities, ranging from usage of social networks or payed streaming services, to buying articles on Ebay. These actions demand usage of critical data like authentication tokens and passwords, and thus raise a question on new attack scenarios and general security of Smart TV apps. In this paper, we investigate attack models for Smart TVs and their apps, and systematically analyze security of Smart TV devices. We point out that some popular apps, including Facebook, Ebay or Watchever, send login data over unencrypted channels. Even worse, we show that an arbitrary app installed on devices of the market share leader Samsung can gain access to the credentials of a Samsung Single Sign-On account. Therefore, such an app can hijack a complete user account including all his devices like smartphones and tablets connected with it. Based on our findings, we provide recommendations that are of general importance and applicable to areas beyond Smart TVs.

5. Closing Remarks

16.00-17.50 DPM III: Monetization and Data Revocation

Session Chair: Guillermo Navarro Arribas (Universitat Autonoma de Barcelona, Spain)

Lecture Hall C

1. Some Remarks and Ideas about Monetization of Sensitive Data

Ania M. Piotrowska and Marek Klonowski (Wrocław University of Technology, Poland)

Abstract: One of the emerging problems on the border of privacy protection research and e-commerce is the monetization of sensitive data. More precisely, a client would like to obtain some statistical data about users' personal information in exchange for a reward. To satisfy both parties, a monetization protocol should ensure that users' privacy is not violated and the data utility is preserved at the same time. During ESORICS 2014 Bilogrevic et al. presented a novel and promising approach to monetization of aggregated sensitive data. In our paper, we point some flaws and shortcomings of the presented protocol. We also make some general methodological remarks to explain why some auspicious directions of data monetization might be futile. Finally, we propose a simple scheme for a secure data aggregation based on sharing trust between different non-collaborating parties.

2. A Novel Approach for Data Revocation on the Internet

Olga Kieselmann, Nils Kopal and Arno Wacker (University of Kassel, Germany)

Abstract: After publishing data on the Internet, the data publisher loses control over it. However, there are several situations where it is desirable to remove published information. To support this, the European Union proposed the General Data Protection Regulation (GDPR) which states that providers must remove the data when the corresponding owner requests it. However, the data might already have been copied by third parties. Therefore, Article 17 of the GDPR includes the regulation that the provider must also inform all third parties about the user's request. Hence, the providers would need to track every access, which is hard to achieve. This technical infeasibility is a gap between the legislation and the current technical possibilities. To close this gap, we propose a novel service which gives the data owner the possibility to inform simultaneously all providers about her removal request.

3.PerfectDedup: Secure Data Deduplication

Pasquale Puzio (SecludIT, France), Refik Molva, Melek Önen (EURECOM, France) and Sergio Loureiro (SecludIT, France)

Abstract: With the continuous increase of cloud storage adopters, data deduplication has become a necessity for cloud providers. By storing a unique copy of duplicate data, cloud providers greatly reduce their storage and data transfer costs. Unfortunately, deduplication introduces a number of new security challenges. We propose PerfectDedup, a novel scheme for secure data deduplication, which takes into account the popularity of the data segments and leverages the properties of Perfect Hashing in order to assure block-level deduplication and data confidentiality at the same time. We show that the client-side overhead is minimal and the main computational load is outsourced to the cloud storage provider.

18.00 Workshop Dinner & Sightseeing Tour

Meeting point: 18:00 in front of the Conference Venue

Walking tour: *Off the beaten track Vienna:* 18:00 – 19:30
Beside Empress Elisabeth, St. Stephen's Cathedral and Schönbrunn Palace, Vienna has lot more to offer: Let our guides show you the nicest walk through the Old Town of Vienna.

Workshop Dinner at Restaurant Schubert: 19:30 – 23:00

The walking tour will end at the location of the Workshop Dinner, Restaurant Schubert. Please note that there is no possibility to store your laptop / bag at the university or during the tour.

Address:
Restaurant Schubert
Schreyvogelgasse 6
1010 Vienna
(Metro stop U2 „Schottentor"– directions will be provided, no organized transport for returning)

Tuesday, 22nd September 2015

08.00-17.00 Registration

09.00-10.30 STM V: Cryptographic protocols

Session Chair: Naranker Dulay (Imperial College London, UK)

Lecture Hall E

1. Two-Factor Authentication for the Bitcoin Protocol

Christopher Mann and Daniel Loebenberger (University of Bonn, Germany)

Abstract: We show how to realize two-factor authentication for a Bitcoin wallet. To do so, we explain how to employ an ECDSA adaption of the two-party signature protocol by MacKenzie and Reiter (2004) in the context of Bitcoin and present a prototypic implementation of a Bitcoin wallet that offers both: two-factor authentication and verification over a separate channel. Since we use a smart phone as the second authentication factor, our solution can be used with hardware already available to most users and the user experience is quite similar to the existing online banking authentication methods.

2. Private Proximity Testing on Steroids: An NTRU-based protocol

Constantinos Patsakis, Panayiotis Kotzanikolaou (University of Piraeus, Greece) and Mélanie Bouroche (Trinity College, Ireland)

Abstract: Nowadays, most smartphones come pre-equipped with location (GPS) sensing capabilities, allowing developers to create a wide variety of location-aware applications and services. While location awareness provides novel features and functionality, it opens the door to many privacy nightmares. In many occasions, however, users do not need to share their actual location, but to determine whether they are in proximity to others, which is practically one bit of information. Private proximity protocols allow this functionality without any further information leakage. In this work we introduce a novel protocol which is far more efficient than the current state of the art and bases its security on lattice-based cryptography.

3. Selecting a New Key Derivation Function for Disk Encryption

Milan Broz and Vashek Matyas (Masaryk University, Czech Republic)

Abstract: Many full disk encryption applications rely on a strong password-based key derivation function to process a passphrase. This article defines requirements for key derivation functions and analyzes recently presented password hashing functions (second round finalists of the Password Hashing Competition) for their suitability for disk encryption.

09.15-10.30 SHCISI: Identity and Access Management

Lecture Hall F

1. Dynamic Trust-Based Recertifications in Identity and Access Management

Christian Richthammer, Michael Kunz, Johannes Sänger, Matthias Hummer, and Günther Pernul (University of Regensburg, Germany)

Abstract: Security compliance has become an important topic for medium- and large-sized companies in the recent years. In order to fulfill all requirements legally imposed, high quality identity management – particularly with respect to correct and Consistent access control – is essential. In this context, the concept of recertification has proven itself to maintain the quality and correctness of access rights over a long period of time. In this paper, we show how the traditional recertification concept can be notably enhanced through involving the notion of trust. We thereto propose a trust-based recertification model and demonstrate its benefits by means of a realistic use case. Our dynamic concept can help to better spread the recertification overhead compared to the traditional approach with fixed periods. Furthermore, it aids in the identification of risky employees.

2. Towards an Economic Approach to Identity and Access Management Systems Using Decision Theory

Eva Weishäupl, Michael Kunz, Emrah Yasasin, Gerit Wagner, Julian Prester, Guido Schryen, and Günther Pernul (University of Regensburg, Germany)

Abstract: Nowadays, providing employees with failure-free access to various systems, applications and services is a crucial factor for organizations' success as disturbances potentially inhibit smooth workflows and thereby harm productivity. However, It is a challenging task to assign access rights to employees' accounts within a satisfying time frame. In addition, the management of multiple accounts and identities can be very onerous and time consuming for the responsible administrator and therefore expensive for the organization. In order to meet these challenges, firms decide to invest in introducing an Identity and Access Management System (IAMS) that supports the organization by using policies to assign permissions to accounts, groups, and roles. In practice, since various versions of IAMSs exist, it is a challenging task to decide upon introduction of an IAMS. The following study proposes a first attempt of a decision support model for practitioners which considers four

alternatives: Introduction of an IAMS with Role-based Access Control (RBAC) or without and no introduction of IAMS again with or without RBAC. To underpin the practical applicability of the proposed model, we parametrize and operationalize it based on a real world use case using input from an expert interview.

09.15-10.30: CyberICS & WOS-CPS & DPM-QASA

Lecture Hall C

1. Welcome

2. Invited speaker: Industrial Control Systems Security – From SCADA Security to Adversarial Control Theory

Dieter Gollman (Technische Universität Hamburg, Germany)

Abstract: We describe an approach for analyzing and attacking the physical part (a process) of a cyber-physical system. The stages of this approach are demonstrated in a case study, a simulation of a vinyl acetate monomer plant. We want to demonstrate in particular where security has to rely on expert knowledge in the domain of the physical components and processes of a system and that there are major challenges for converting cyber-attacks into successful cyber-physical attacks.

10.30-11.00 Coffee Break

11.00-12.30 STM VI: Controlling data release

Session Chair: Ken Barker (University of Calgary, Canada)

Lecture Hall E

1. It's My Privilege: Controlling Downgrading in DC-Labels

Lucas Waye (Harvard University, USA), Pablo Buiras (Chalmers University of Technology, Sweden), Daniel King, Stephen Chong (Harvard University, USA) and Alejandro Russo (Chalmers University of Technology, Sweden)

Abstract: Disjunction Category Labels (DC-labels) are an expressive label format used to classify the sensitivity of data in information-flow control systems. DC-labels use capability-like *privileges* to downgrade information. Inappropriate use of privileges can compromise security, but DC-labels provide no mechanism to ensure appropriate use. We extend DC-labels with the novel notions of *bounded privileges* and *robust privileges*. Bounded privileges specify and enforce upper and lower bounds On the labels of data that may be downgraded. Bounded privileges are simple and intuitive, yet can express a rich set of desirable security policies. Robust privileges can be used only in downgrading operations that are *robust*, i.e., the code exercising privileges cannot be abused to release or certify more information than intended. Surprisingly, robust downgrades can be expressed in DC-labels as downgrading operations using a weakened privilege. We provide *sound and complete* run-time security checks to ensure downgrading operations are robust. We illustrate the applicability of bounded and robust privileges in a case study as well as by identifying a vulnerability in an existing DC-label-based application.

2. Obligations in PTaCL

Conrad Williams and Jason Crampton (Royal Holloway, University of London, UK)

Abstract: Obligations play an increasingly important role in authorization systems and are supported by languages such as XACML. However, our understanding of how to handle obligations in languages such as XACML, particularly in exceptional circumstances, is hampered by a lack of formality and rigor in the existing literature, including the XACML standard. PTaCL is an attribute-based policy language that makes use of tree-structured policies and targets, like XACML. However, PTaCL is more general than XACML and has rigorous operational semantics for request evaluation, from which a policy decision point can be implemented. In this paper, we enhance PTaCL by extending the policy syntax to include obligations and defining the obligations that should be associated with an authorization decision. Our final contribution is to extend our analysis to cases where policy evaluation may return an indeterminate value. We demonstrate that obligation semantics for PTaCL coincide with those of XACML when there is no indeterminacy. More importantly, we show that our obligation semantics provide a principled method for determining obligations for any policy-combining algorithm and the set of possible obligations in the presence of indeterminacy, thereby providing considerable advantages over existing approaches.

3. Content and Key Management to Trace Traitors in Broadcasting Services

Kazuto Ogawa (Japan Broadcasting Corporation, Japan), Goichiro Hanaoka (National Institute of Advanced Industrial Science and Technology, Japan) and Hideki Imai (The University of Tokyo, Japan)

Abstract: Traitor tracing encryption schemes are a type of broadcasting encryption and have been developed for broadcasting services. There are multiple distinct decryption keys for each encryption key, and each service subscriber is given a unique decryption key. Any subscriber that redistributes his or her decryption key to a third party or who uses it to make a pirate receiver (*PR*) can be identified using the schemes. However, almost all previous schemes are effective against only those *PR*s

with only one decryption key. We first discuss an attack (*content comparison attack*) against the above encryption schemes. The attack involves multiple distinct decryption keys and content-data comparison mechanism. We have developed a *content and key management method* (*CKM*) that makes traitor tracing schemes secure against the content comparison attack. Its use makes it impossible for *PR*s to distinguish ordinary content data from test data and makes traitor tracing schemes effective against all *PR*s. The CKM makes the broadcasting services secure.

11.00-12.30 SHCIS II: Security in the Clouds

Lecture Hall F

1. Virtual Machine Introspection with Xen on ARM

Tamas K. Lengyel, Thomas Kittel, and Claudia Eckert (Technische Universität München, Germany)

Abstract: In the recent years, virtual machine introspection has become a valuable technique for developing security applications for virtualized environments. With the increasing popularity of the ARM architecture and the recent addition of hardware virtualization extensions there is a growing need for porting existing tools to this new platform. Porting these applications requires proper hypervisor support, which we have been exploring and developing for the upcoming Xen 4.6 release. In this paper we explore using ARM's two-stage paging mechanisms with Xen to enable stealthy, efficient tracing of guest operating systems for security purposes.

2. Analysing Malware Attacks in the Cloud: A Use Case for the TLSInspector Toolkit

Benjamin Taubmann, Dominik Dusold, Christoph Frädrich, and Hans P. Reiser (University of Passau, Germany)

Abstract: Nowadays, malicious attacks in the Internet often use encrypted communication channels. Thus, an attacker might exploit a vulnerability in a web service using the HTTPS protocol. If network intrusion detection systems (NIDS) are unable to decrypt this communication, they cannot observe the contents of such attacks. If the NIDS is operated independently of the web services, it is impractical to directly provide decryption keys to it. This is, for example, the case if a cloud provider operates the NIDS, while a cloud customer manages the web service within a virtual machine. Additionally, malware often encrypts the communication to a command and control server. The encryption keys used for that communication channel are fully under the control of the malware and thus it is even more difficult to provide them to the NIDS. This paper discusses both use cases in a common cloud scenario and describes a VMI based prototype that is able to decrypt TLS encrypted communication of a virtual machine. The decryption is achieved by taking a memory snapshot and extracting the cryptographic key that is required to decrypt a network flow. We experimentally evaluate the overhead caused by taking the memory snapshots and the performance of extracting the encryption key from the snapshot.

3. QoS-Aware Secure Live Migration of Virtual Machines

Waseem Mandarawi, Andreas Fischer, Hermann de Meer (University of Passau, Germany) and Eva Weishaeupl (University of Regensburg, Germany)

Abstract: The live migration of Virtual Machines (VMs) is a key technology in server virtualization solutions used to deploy Infrastructure-as-a-Service (IaaS) clouds. This process, on one hand, increases the elasticity, fault tolerance, and maintainability in the virtual environment. On the other hand, it increases the security challenges in cloud environments, especially when the migration is performed between different data centers. Secure live migration mechanisms are required to keep the security requirements of both cloud customers and providers satisfied. These mechanisms are known to increase the migration downtime of the VMs, which plays a significant role in the compliance to Service Level Agreements (SLAs). This paper discusses the main threats caused by live migration and the main approaches for securing the migration. The requirements of a comprehensive Quality of Service (QoS)-aware secure live migration solution that keeps both security and QoS requirements satisfied are defined.

11.00-12.20 DPM IV: Short Papers

Session Chair: Isaac Agudo (NICS Lab, Spain)

Lecture Hall C

1. User-centric privacy-preserving collection and analysis of trajectory data (Short Paper).

Cristina Romero-Tris and David Megías (Universitat Oberta de Catalunya (UOC), Spain)

Abstract: Due to the increasing use of location-aware devices such as smartphones, there is a large amount of available trajectory data whose improper use or publication can threaten users' privacy. Since trajectory information contains personal mobility data, it may reveal sensitive details like habits of behavior, religious beliefs, and sexual preferences. Current solutions focus on anonymizing data before its publication. Nevertheless, we argue that this approach gives the user no control about the information she shares. For this reason, we propose a novel approach that works inside users' mobile devices, where users can decide and configure the quantity and accuracy of shared data.

2. Can You Really Anonymize the Donors of Genomic Data in Today's Digital World? (Short Paper).

Mohammed Alser, Nour Almadhoun, Azita Nouri, Can Alkan and Erman Ayday (Bilkent University, Turkey)

Abstract: The rapid progress in genome sequencing technologies leads to availability of high amounts of genomic data. Accelerating the pace of biomedical breakthroughs and discoveries necessitates not only collecting millions of genetic samples but also granting open access to genetic databases. However, one growing concern is the ability to protect the privacy of sensitive information and its owner. In this work, we survey a wide spectrum of cross-layer privacy breaching strategies to human genomic data (using both public genomic databases and other public non-genomic data). We outline the principles and outcomes of each technique, and assess its technological complexity and maturation. We then review potential privacy-preserving countermeasure mechanisms for each threat.

3. The leaking battery: A privacy analysis of the HTML5 Battery Status API (Short Paper).

Lukasz Olejnik (INRIA Privatics, France), Gunes Acar, Claude Castelluccia (KU Leuven, Belgium) and Claudia Diaz (INRIA Privatics, France)

Abstract: We highlight privacy risks associated with the HTML5 Battery Status API. We put special focus on its implementation in the Firefox browser. Our study shows that websites can discover the capacity of users' batteries by exploiting the high precision readouts provided by Firefox on Linux. The capacity of the battery, as well as its level, expose a finger printable surface that can be used to track web users in short time intervals. Our analysis shows that the risk is much higher for old or used batteries with reduced capacities, as the battery capacity may potentially serve as a tracking identifier. The finger printable surface of the API could be drastically reduced without any loss in the API's functionality by reducing the precision of the readings. We propose minor modifications to Battery Status API and its implementation in the Firefox browser to address the privacy issues presented in the study. Our bug report for Firefox was accepted and a fix is deployed.

4. Secure Refactoring with Java Information Flow (Short Paper).

Steffen Helke (Brandenburgische Technische Universität Cottbus-Senftenberg, Germany), Florian Kammueller (Middlesex University, UK) and Christian W. Probst (Technical University of Denmark, Denmark)

Abstract: Refactoring means that a program is changed without changing its behavior from an observer's point of view. Does the change of behavior also imply that the security of the program is not affected by the changes? Using Myers and Liskov's distributed information flow control model DLM and its Java implementation Jif, we explore this question practically on common patterns of Refactoring as known from Fowler. We first illustrate on an example the \Extract method" refactoring and how it can endanger confidentiality. We then show how to construct a secure version of this major refactoring pattern by employing Jif to control information flows. Finally, we can show that security leaks as encountered at the outset are not possible anymore.

11.00-12.30: CyberICS I

Lecture Hall B

1. The economics of cybersecurity, from the public good to the revenge of the industry

Danilo Delia (University of Paris VIII Vincennes-Saint Denis, France)

Abstract: In the aftermath of Edward Snowden’s intelligence revelations, many governments around the world are increasingly elaborating so-called « digital sovereignty » policies. The declared aim is to develop trusted technologies to protect the more sensitive networks. The ambition of this article is to turn over the complex- and often contrasting- motivations and interests behind the industrial policy movements, explain how the dominant representation of cybersecurity as public good is impacting the public policy and analyze the dynamics between private and public players

2. Teaching Industrial Control System Security UsingCollaborative Projects

Thuy Nguyen, Mark Gondree (Naval Postgraduate School, USA) and David Reed (Ship Systems Engineering Station (NSWCCD-SSES), USA)

Abstract: In this work, we discuss lessons learned over the past three years while supporting a graduate capstone course centered on research projects in industrial control system (ICS) security. Our course considers real-world problems in shipboard ICS posed by external stakeholders: a system-owner and related subject matter experts. We describe the course objectives, format, expectations and outcomes. While our experiences are generally positive, we remark on opportunities for curricula improvement relevant to those considering incorporating realistic ICS topics into their classroom, or those working with an external SME.

3. Trust Establishment in Cooperating Cyber-Physical System.

Andre Rein (Fraunhofer Institute SIT, Germany), Roland Rieke (Philipps-Universität Marburg, Germany), Michael Jäger (Technische Hochschule Mittelhessen, Germany), Nicolai Kuntze (Fraunhofer Institute SIT, Germany) and Luigi Coppolino (Universita degli Studi di Napoli "Parthenope", Italy)

Abstract: Cooperating systems are systems of systems that collaborate for a common purpose. In this work, we consider networked cooperating systems that base important decisions on data gathered from external sensors and use external actuators to enforce safety critical actions. Typical examples of cooperating cyber physical systems are critical infrastructure process control systems. Such systems must not only be secure, they must be demonstrably so. Using the example of a hydroelectric power plant control system, this paper analyzes security threats for networked cooperating systems, where sensors providing decision critical data are placed in non-protected areas and thus are exposed to various kinds of attacks. We propose a concept for trust establishment in cyber-physical cooperating systems. Using trusted event reporting for critical event sources, the authenticity of the security related events can be verified. Based on measurements obtained with a prototypical realization, we evaluate and analyze the amount of overhead data transmission between event source and data verification system needed for trust establishment. We propose an efficient synchronization scheme for system integrity data, reducing network traffic as well as verification effort.

4. Forensics in Industrial Control System: A Case Study (short paper)

Pieter Van Vliet (Ministry of Infrastructure and the Environment, Netherlands), M-T. Kechadi and Nhien An Le Khac (University College Dublin, Ireland)

Abstract. Industrial Control Systems (ICS) are used worldwide in critical infrastructures. An ICS system can be a single embedded system working standalone for controlling a simple process or ICS can also be a very complex Distributed Control System (DCS) connected to Supervisory Control And Data Acquisition (SCADA) system(s) in a nuclear power plant. Although ICS are widely used today, there are very little research on the forensic acquisition and analyze ICS's artefacts. In this paper we present a case study of forensics in ICS where we describe a method of safeguarding important volatile artefacts from an embedded industrial control system and several other sources.

12.30-14.00 Lunch Break

14.00-15.30 STM VII (short papers): Security Analysis, Risk Management, and Usability

Session Chair: Erisa Karafili (Technical University of Denmark, Denmark)

Lecture Hall E

1. In Cyber-Space, no one can hear you S.CREAM: A Root Cause Analysis technique for Socio-Technical Security

Ana Ferreira (University of Porto, Portugal), Jean-Louis Huynen, Vincent Koenig and Gabriele Lenzini (University of Luxembourg, Luxembourg)

Abstract: Inspired by the root cause analysis techniques that in the field of safety research and practice help investigators understand the reasons of an incident, this paper investigates the use of root cause analysis in security. We aim at providing a systematic method for the security analyst to identify the socio-technical attack modes that can potentially endanger a system's security.

2. A Socio-Technical Investigation into Smartphone Security

Melanie Volkamer (Technische Universität Darmstadt, Germany), Karen Renaud (University of Glasgow, UK), Oksana Kulyk, and Sinem Emeroz (Technische Universität Darmstadt, Germany)

Abstract: Many people do not deliberately act to protect the data on their Smartphones. The most obvious explanation for a failure to behave securely is that the appropriate mechanisms are unusable. Does this mean usable mechanisms will automatically be adopted? Probably not! Poor usability certainly plays a role, but other factors also contribute to nonadaptation of precautionary mechanisms and behaviors. We carried out a series of interviews to determine justifications for non-adoption of security precautions, specifically in the smartphone context, and developed a model of Smartphone precaution non-adoption. We propose that future work should investigate the use of media campaigns in raising awareness of these issues.

3. A Game Theoretic Framework for Modeling Adversarial Cyber Security Game among Attackers, Defenders, and Users

Tatyana Ryutov, Michael Orosz, Detlof von Winterfeldt (USC Information Sciences Institute, USA) and Jim Blythe (USC, USA)

Abstract: This paper models interactions in the cyber environment as a three-way security game between attacker, defender, and user. The paper focuses on understanding and modeling the roles, motivations and conflicting objectives of the players.

Unlike most research in cyber security, this paper studies not only technological but also psychosocial aspects of the interactions. The paper develops recommendations for selecting games that have relevant features for representing cyber security interactions and outlines directions for future research.

4. Design, Demonstration, and Evaluation of An Information Security Contract and Trading Mechanism to Hedge Information Security Risks

Pankaj Pandey (Gjovik University College, Norway) and Steven De Haes (University of Antwerp, Belgium)

Abstract: Cyber-insurance products are the only financial instrument available as a risk-transfer mechanism in the information security domain. Furthermore, cyber-insurance markets are unable or unwilling to facilitate the transfer of risks, particularly those with a high probability and high intensity of loss. Thus, there is a need for a new mechanism to address the variety of information security risks. This article addresses the shortcomings in the existing information security risk hedging market. The article presents a financial instrument and a corresponding trading mechanism to be used for risk hedging in an information security prediction market. Also, the article uses an imaginary case to demonstrate the application of the contract. Furthermore, an evaluation of the contract and trading mechanism in its usefulness in hedging the underlying risks is presented. In our analysis, we found that information security contracts can be a solution (at least to some extent) to the problems in the existing risk hedging mechanisms in the information security domain.

14.00-15.30 SHCIS III: (Mobile) Malware I

Lecture Hall F

1. Social Network Analysis of Mobile Malware Initiating SMS Messages

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

Abstract: The largest part of mobile malware today spreads via malicious applications. It is common practice that malware is analyzed either statically by reverse-engineering of malicious samples or dynamically by observing the traffic generated by the samples. The static approach is extremely time consuming and the number of apps added to app stores on a daily basis is very high. It is therefore crucial to carefully select the apps to analyze before starting the static inspection. We believe that by visualizing the structure of the mobile malware ecosystem, the manual reverse-engineering process can be better targeted. In this paper, we propose heuristics to determine the similarity and authorship of Android malware initiating short messages by looking at phone numbers and keywords used in short messages. Specifically, we show that social network analysis is a valuable tool to simplify the selection of suspicious samples for the further malware analysis process. We validate our statement on authorship of Android malware. From the resulting social graph we estimate the number of mobile malware authors based on the language character set used in the decompiled source code.

2. Google Verify Apps: The Illusion of Security?

Jennifer Naumann, Mykola Protsenko, and Tilo Müller (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany)

Abstract: In this paper we analyze Verify Apps, which is the standard anti-virus software for Android offered by Google. Verify Apps should protect the user from malicious apps which are installed from other sources than Google's Play Store. To get more information about the internals of Verify Apps, we tested it with 6103 malware apps, each modified with four different obfuscation techniques. In addition, we examined its functionality in detail by reverse engineering. Verify Apps recognized about 42 percent of the original malware samples, but even such a simple transformation as re-zipping the app, which only affects the hash signatures of a file, resulted in detection rate dropping to less than 3 percent. After the application of static obfuscation techniques, none of the samples could be detected. Moreover, we experienced practical problems with Verify Apps: It stops working after identifying eleven apps as malware, and the verification of already installed apps, which is one of its new features according to Google, could not be observed.

3. Automated Malware Analysis for Android: A Comparative Evaluation

Marcel Busch, Mykola Protsenko, and Tilo Müller (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany)

Abstract: In this paper, we show to what extent automatically generated reports for Android apps can help analyzing potentially malicious behavior. We generated reports using three well known analysis platforms for eleven malware and six goodware samples. Using the analysis reports generated by Andrubis, Mobile-Sandbox and SandDroid, we firstly evaluate each platform's ability to express information about an app's maliciousness. It turns out that no appropriate classification in goodware and malware can be performed by the assessed frameworks without relying on third party mostly signature based detection engines. Secondly, we discuss the contents presented within the generated malware reports and take them as a basis for comparing the frameworks. This comparison leads to the conclusion that among the assessed frameworks no truly superior solution exists.

14.00-15.20 DPM V: Position and Short Papers

Session Chair: Jordi Herrera Joancomartí (Universitat Autònoma de Barcelona, Spain)

Lecture Hall C

1. Privacy Threats in E-Shopping (Position Paper).

Jesus Diaz (Universidad Autónoma de Madrid, Spain), Seung Geol Choi (United States Naval Academy, USA), David Arroyo (Universidad Autónoma de Madrid, Spain), Angelos Keromytis (Columbia University, USA), Francisco Rodriguez (Universidad Autónoma de Madrid, Spain) and Moti Yung (Columbia University, USA)

Abstract: E-shopping has grown considerably in the last years, providing customers with convenience, merchants with increased sales, and financial entities with an additional source of income. However, it may also be the source of serious threats to privacy. In this paper, we review the e-shopping process, discussing attacks or threats that have been analyzed in the literature for each of its stages. By showing that there exist threats to privacy in each of them, we argue our following position: "It is not enough to protect a single independent stage, as is usually done in privacy respectful proposals in this context. Rather, a complete solution is necessary spanning the overall process, dealing also with the required interconnections between stages." Our overview also reflects the diverse types of information that e-shopping manages, and the benefits (e.g., such as loyalty programs and fraud prevention) that system providers extract from them. This also endorses the need for solutions that, while privacy preserving, do not limit or remove these benefits, if we want prevent all the participating entities from rejecting it.

2. Comparison-based Privacy: Nudging Privacy in Social Media (Position Paper).

Jan Henrik Ziegeldorf, Martin Henze, Rene Hummen and Klaus Wehrle (RWTH Aachen University, Germany)

Abstract: Social media continues to lead imprudent users into oversharing, exposing them to various privacy threats. Recent research thus focusses on nudging the user into the 'right' direction. In this paper, we propose Comparison-based Privacy (CbP), a design paradigm for privacy nudges that overcomes the limitations and challenges of existing approaches. CbP is based on the observation that comparison is a natural human behavior. With CbP, we transfer this observation to Decision-making processes in the digital world by enabling the user to compare herself along privacy-relevant metrics to user-selected comparison groups. In doing so, our approach provides a framework for the integration of existing nudges under a self-adaptive, user-centric norm of privacy. Thus, we expect CbP not only to provide technical improvements, but to also increase user acceptance of privacy nudges. We also show how CbP can be implemented and present preliminary results.

3. You never surf alone. Ubiquitous tracking of users' browsing habits (Short Paper).

Silvia Puglisi, David Rebollo-Monedero and Jordi Forné (Universitat Politècnica de Catalunya (UPC), Spain)

Abstract: In the early age of the internet users enjoyed a large level of anonymity. At the time web pages were just hypertext documents; almost no personalization of the user experience was offered. The Web today has evolved as a world-wide distributed system following specific architectural paradigms. On the web now, an enormous quantity of user generated data is shared and consumed by a network of applications and services, reasoning upon users expressed preferences and their social and physical connections. Advertising networks follow users' browsing habits while they surf the web, continuously collecting their traces and surfing patterns. We analyze how users tracking happens on the web by measuring their online footprint and estimating how quickly advertising networks are able to profile users by their browsing habits.

4. LockPic: Privacy Preserving Photo Sharing in Social Networks (Short Paper).

Carlos Pares-Pulido and Isaac Agudo (University of Malaga, Spain)

Abstract: There are many privacy concerns related to the use of social networks, in particular the posting of pictures and controlling who has access to them. In this paper we introduce a solution for the distribution of personal or sensitive pictures. Our aim is to provide a method for secure and privacy friendly picture sharing through social networks, that allows users to encrypt sensitive regions in pictures (particularly, faces) in a reversible, non-intrusive way, leaving the rest of the picture unaltered. This way, any image can be freely published and distributed on any social network, and viewed by as many users as the platform allows, while the protected parts are only accessible with the corresponding key. Once the key for a particular region has been acquired, the receiver of the picture can decrypt this region without downloading any additional information. The core of our proposal is a C library, which efficiently integrates an encryption/decryption algorithm with the encoding/decoding process. We have also released an Android application, LockPic, and a companion key server that showcase all the functionality mentioned in this work.

14.00-15.30: WOC-CPS

Lecture Hall B

1. LiMon: Lightweight Authentication for Tire Pressure Monitoring Sensors

Bogdan Groza and Cristina Solomon (Politehnica University of Timisoara, Romania)

Abstract: Modern vehicles offer a raw territory for designing security solutions as the over-increasing design complexity demanded massive advances in electronics in the absence of a crisp vision over the adversary model. The vehicle Tire Pressure Monitoring System (TPMS) is a sub-system that recently triggered some attention in the light of several reported attacks. In this work we start from analyzing existing proposals and reckon some shortcomings, e.g., academic proposals are not yet tested on real-world components while a patented security solution from the industry (likely deployed in practice) is completely insecure. Motivated by these, we design a new solution and deploy it on real-world components that are used in the automotive industry. Designing security for this subsystem proves to be especially relevant as the computational resources for TPM systems are somewhat at the minimum to be found in automotive embedded devices. Our solution is deployed on Infineon SP37 sensors and takes advantage of some recently proposed light-weight cryptographic designs, e.g., SPECK and PRESENT.

2. Umbra: Embedded Web Security through Application- Layer Firewalls

Travis Finkenauer and J. Alex Halderman (University of Michigan, USA)

Abstract: Embedded devices with web interfaces are prevalent, but, due to memory and processing constraints, implementations typically make use of Common Gateway Interface (CGI) binaries written in low-level, memory-unsafe languages. This creates the possibility of memory corruption attacks as well as traditional web attacks. We present Umbra, an application-layer firewall specifically designed for protecting web interfaces in embedded devices. By acting as a “friendly man-in-the-middle,” Umbra can protect against attacks such as cross-site request forgery (CSRF), information leaks, and authentication bypass vulnerabilities. We evaluate Umbra’s security by analyzing recent vulnerabilities listed in the CVE database from several embedded vendors and find that it would have prevented half of the vulnerabilities. We also show that Umbra comfortably runs within the constraints of an embedded system while incurring minimal performance overhead.

3. Towards Standardising Firewall Reporting

Dinesha Ranathunga, Matthew Roughan (University of Adelaide, Australia), Phil Kernick (CQR Consulting, Australia) and Nickolas Falkner (University of Adelaide, Australia)

Abstract: Rubin and Greer stated that \The single most important factor of your firewall's security is how you configure it. “However, firewall configuration is known to be difficult to get right. In particular domains, such as SCADA networks, while there are best practice standards that help, an overlooked component is the specification of firewall reporting policies. Our research tackles this question from first principles: we ask what the uses of firewall reports are, and we allow these to guide how reporting should be performed. We approach the problem by formalizing the notion of scope and granularity of a report across several dimensions: time, network elements, policies, etc.

15.30-16.00 Coffee Break

16.00-17.30 SHCIS IV: (Mobile) Malware II

Lecture Hall F

1. Leveraging Deep Learning for Malware Detection and Classification

Bojan Kolosnjaji and Claudia Eckert (Technische Universität München, Germany)

Abstract: As signature-based malware detection systems are unable to cope with the increasing number and variety of malware samples, machine learning has been proposed as a robust alternative. Neural networks have been used in numerous research efforts as a machine learning-based method for the detection and classification of malware, for the purpose of both network-based and host-based intrusion detection. The most used configuration of neural network in these efforts was a perceptron with one hidden layer. However, recent years have brought a significant advancement in neural networks, with new training methods and improved configuration possibilities for neural network units. The advancement is centered around the paradigm of deep learning. This paper contains a description of these new approaches and discusses the possibilities of their application to malware detection and classification problems. A novel malware detection architecture is presented that leverages these advancements for classifying malware based on inputs from static and dynamic analysis results.

2. Approximating Optimal Software Obfuscation for Android Applications

Yan Zhuang and Felix C. Freiling (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany)

Abstract: In the context of software protection, we study the problem of automatically obfuscating a given program to a given target level of "difficulty". We measure difficulty by utilizing software complexity metrics. We formalize the search problem and argue that current informed search algorithms cannot be used for our purpose, because the number of evaluated search candidates should be minimal and their actual complexities cannot be predicted with certainty. Within a framework for program obfuscation for Android APKs, we empirically evaluate two different algorithms that search for an obfuscated version satisfying a conjunction of target complexity metrics. We show that a first algorithm whose predictions rely on mean values is outperformed by a second algorithm based on Bayes theorem. Keywords: software complexity metric, obfuscation, software quality, optimized obfuscation, Android applications

16.00-17.45 DPM VI: Biometrics and Privacy Preservation

Session Chair: Joaquin Garcia-Alfaro (TELECOM SudParis, France)

Lecture Hall C

1. Privacy-Preserving Biometric Authentication and Matching via Lattice-Based Encryption.

Constantinos Patsakis (University of Piraeus, Greece), Jeroen van Rest (TNO, The Netherlands), Michal Choras (University of Science and Technology, Poland) and Mélanie Bouroche (Trinity College, Ireland)

Abstract: The continuous dependence on electronic media has radically changed our interactions, many of which are now performed online. In many occasions users need to authenticate to remote machines, but the hostile environment of the Internet may severely expose users and service providers. To counter these shortcomings, strong authentication is pushed forward. As a means to authenticate individuals, biometric authentication is gradually gaining more and more ground. While the use of biometric data enables many useful applications, these data are very sensitive. For this reason, it is essential to handle them with the least user exposure. In this work we propose a very efficient protocol for privacy-preserving biometric authentication using lattice-based encryption. More precisely, we exploit the homomorphic properties of NTRU to provide a robust and secure solution and provide experimental results which illustrate the efficacy of our proposal.

2. Comprehensive and Improved Secure Biometric System using Homomorphic Encryption.

Avradip Mandal, Arnab Roy (Fujitsu Laboratories of America, USA) and Masaya Yasuda (Kyushu University, Japan)

Abstract: With the widespread development of biometric systems, concerns about security and privacy are increasing. An active area of research is template protection technology, which aims to protect registered biometric data. We focus on a homomorphic encryption approach, which enables building a \cryptographically-secure" system. In DPM 2013, Yasuda et al. proposed an efficient template protection system, using the homomorphic encryption scheme proposed by Brakerski and Vaikuntanathan. In this work, we improve and fortify their system to withstand impersonation attacks such as replay and spoofing attacks. We introduce a challenge-response authentication mechanism in their system and design a practical distributed architecture where computation and authentication are segregated. Our comprehensive system would be useful to build a large-scale and secure biometric system such as secure remote authentication over public networks.

3. On the Privacy of Horizontally Partitioned Binary Data-based Privacy-Preserving Collaborative Filtering.

Murat Okkalioglu (Yalova University, Turkey), Mehmet Koc (Seyh Edebali University, Turkey) and Huseyin Polat (Anadolu University, Turkey)

Abstract: Collaborative filtering systems provide recommendations for their users. Privacy is not a primary concern in these systems; however, it is an important element for the true user participation. Privacy-preserving collaborative filtering techniques aim to offer privacy measures without neglecting the recommendation accuracy. In general, these systems rely on the data residing on a central server. Studies show that privacy is not protected as much as believed. On the other hand, many e-companies emerge with the advent of the Internet, and these companies might collaborate to offer better recommendations by sharing their data. Thus, partitioned data-based privacy-persevering collaborative filtering schemes have been proposed. In this study, we explore possible attacks on two-party binary privacy-preserving collaborative filtering schemes and evaluate them with respect to privacy performance.

4. Farewell

16.00-17.30: CyberICS II

Lecture Hall B

1. Security Monitoring for Industrial Control Systems

Alessio Coletta and Alessandro Armando (Fondazione Bruno Kessler, Italy)

Abstract: An Industrial Control System (ICS) is a system of physical entities whose functioning heavily relies on information and communication technology components and infrastructures. ICS are ubiquitous and can be found in a number of safety-critical areas including energy, chemical processes, health-care, aerospace, manufacturing, and transportation. While originally isolated and inherently secure, ICS are recently becoming more and more exposed to cyber-attacks (e.g. Stuxnet). Many existing ICS do not feature cyber security protection, with liability issues and high costs in case of incidents. Since existing ICS are normally based on components and protocols that cannot be modified nor updated, redesign is usually not feasible. In this paper we propose a monitoring framework for the run-time verification of ICS. The framework is based on a formal language that supports the precise specification of high-level safety requirements as well as of the relevant threat model, and on a passive monitoring technique that detects and notifies if the system state is close to a critical state.

2. Wireless HART NetSIM: aWireless HART SCADA-Based Wireless Sensor Networks simulator

Lyes Bayou (Télécom Bretagne-LabSTICC, France), David Espes (University of Western Brittany, France), Nora Cuppens and Frédéric Cuppens (Télécom Bretagne-LabSTICC, France)

Abstract: The security of SCADA systems is a major concern. Indeed, these systems are used to manage important infrastructures. However, conducting security analyzes on these systems is almost impossible. Therefore, using simulators is the best way to do that. In this paper, we describe our simulator for WirelessHART SCADA-based systems. It implements the whole protocol stack and both field devices and the Network Manager including routing and scheduling algorithms. The simulator is specially tailored to assess WirelessHART security mechanisms and to test attacks and countermeasures. It includes scenarios for testing several kinds of attacks such as sybil and denial of service (DoS) attacks. Also, new scenarios can easily be added to test other kinds of attacks.

3. Remote Attestation for Embedded Systems

Markku Kylänpää and Aarne Rantala (VTT Technical Research Centre of Finland, Finland)

Abstract. Large distributed systems, like Industrial Control Systems, should be able to verify that devices that are connected to trusted entities are real authorized network nodes running unmodified firmware. Remote attestation is a mechanism that can provide limited confidence of device identity and integrity. Remote attestation allows a remote verifier, e.g. a service provider, to verify integrity of the connecting system before providing a service. The current standard practice in remote attestation, defined by the Trusted Computing Group (TCG), is based on integrity measurements whose results are stored into an isolated trusted component called Trusted Platform Module (TPM) inside the system to be attested. The proof-of-concept scenario implementing similar functionality using an ARM processor secure environment is discussed. The implementation is done using ARM processor emulator which includes emulation for ARM TrustZone Trusted Execution Environment (TEE) providing isolated trusted component functionality. Challenges and security issues of the chosen approach are discussed.

4. An Attack Execution Model for Industrial Control Systems Security Assessment (short paper)

Ziad Ismail (EDF R&D, France), Jean Leneutre (Telecom ParisTech, France) and Alia Fourati (EDF R&D, France)

Abstract: The improved communication and remote control capabilities of industrial control systems equipment have increased their attack surface. As a result, managing the security risk became a challenging task. The consequences of attacks in an industrial control system can go beyond targeted equipment to impact services in the industrial process. In addition, the success likelihood of an attack is highly correlated to the attacker profile and his knowledge of the architecture of the system. In this paper, we present the Attack Execution Model (AEM), which is an attack graph representing the evolution of the adversary's state in the system after each attack step. We are interested in assessing the risk of cyber-attacks on an industrial control system before the next maintenance period. Given a specific attacker profile, we generate all potential attacker actions that could be executed in the system. Our tool outputs the probability and the time needed to compromise a target equipment or services in the system.

Social Events

Monday, 21st September 2015 – Workshop Dinner

Sightseeing Walking Tour & Workshop Dinner

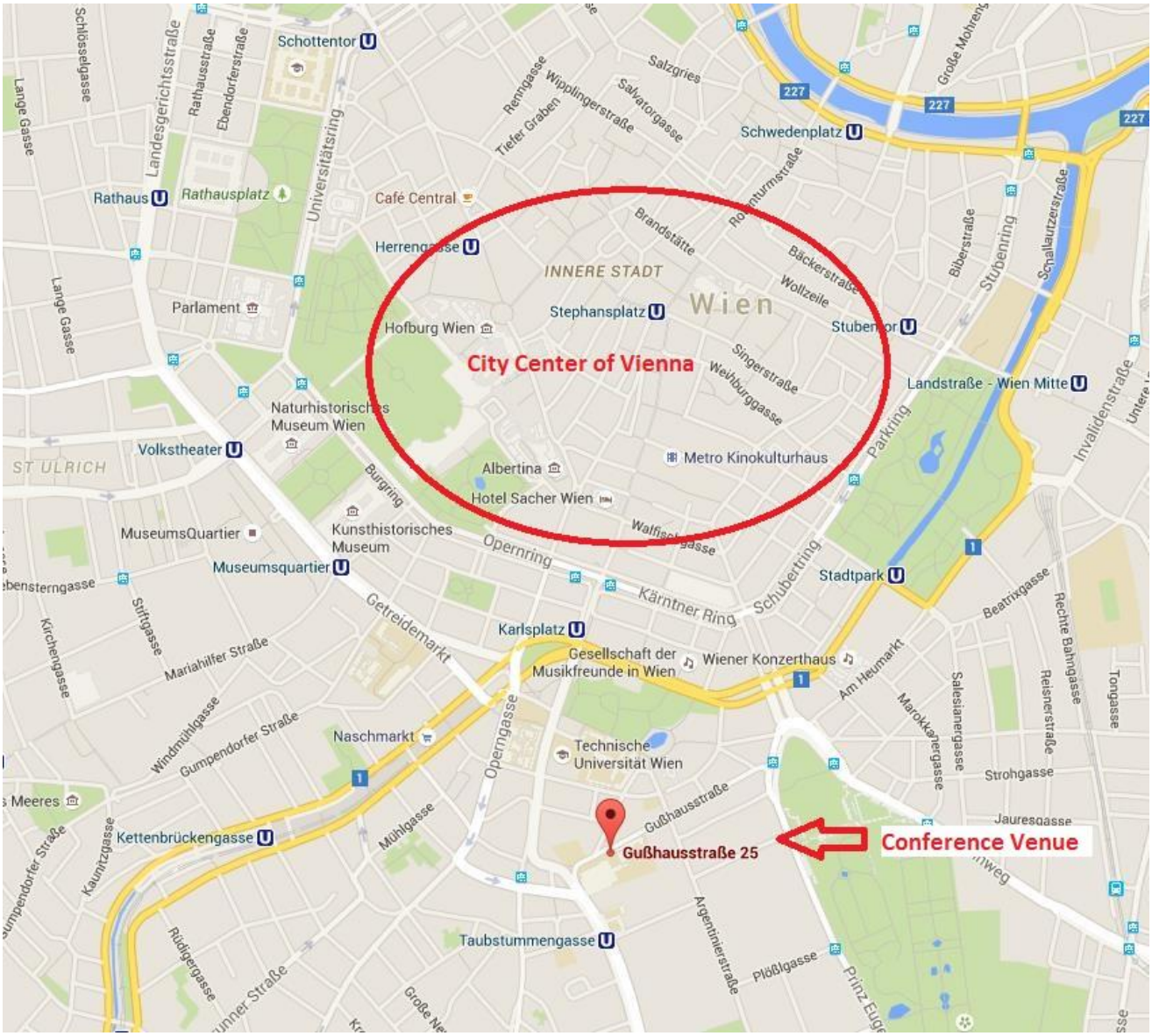
We have organized a walking tour "Off the beaten path" in Vienna. Afterwards we will have our workshop dinner at the Restaurant Schubert. The tour will take about 1.5 hours and will end directly at the restaurant.

Meeting point: 18:00 in front of the Conference Venue
Walking tour "Off the beaten track Vienna": 18:00 – 19:30
Beside Empress Elisabeth, St. Stephen's Cathedral and Schönbrunn Palace, Vienna has lot more to offer: Let our guides show you the nicest walk through the Old Town of Vienna.
Workshop Dinner at Restaurant Schubert: 19:30 – 23:00

Please note that there is no possibility to store your laptop / bag at the university or during the tour.

Address:
Restaurant Schubert
Schreyvogelgasse 6
1010 Vienna
(Metro stop U2 „Schottentor"- directions will be provided, no organized transport for returning)

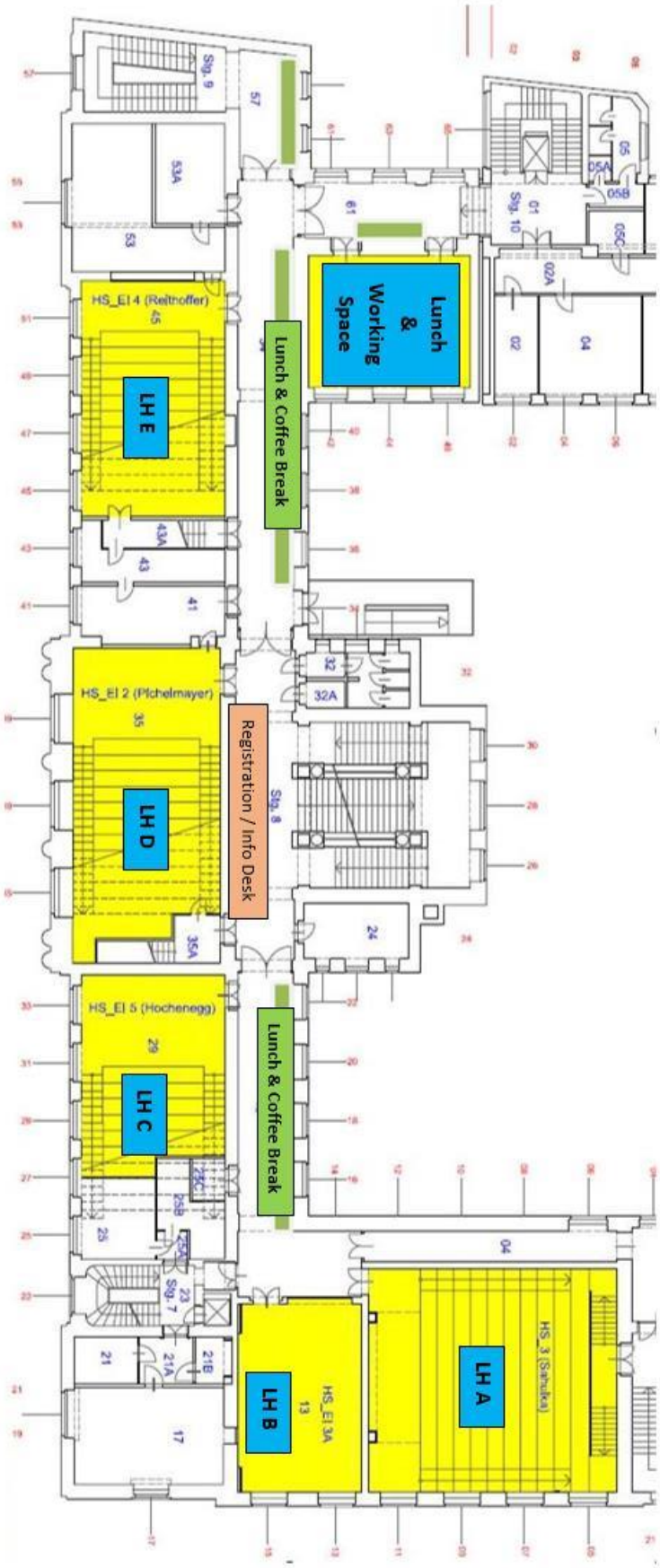
Venue Overview



Conference Venue

Map 1: Conference Venue Overview

Room Plan


Lunch & Working Space
Lunch & Coffee Break
HS_EI 4 (Reithoffer)
LH E
HS_EI 2 (Pichelmayer)
LH D
Registration / Info Desk
Lunch & Coffee Break
HS_EI 5 (Hochenegg)
LH C
LH B
HS_EI 3A
LH A
HS_3 (Schulka)

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. During the lunch break the working room will serve as lunch break area where you can also enjoy your lunch as a seated lunch.

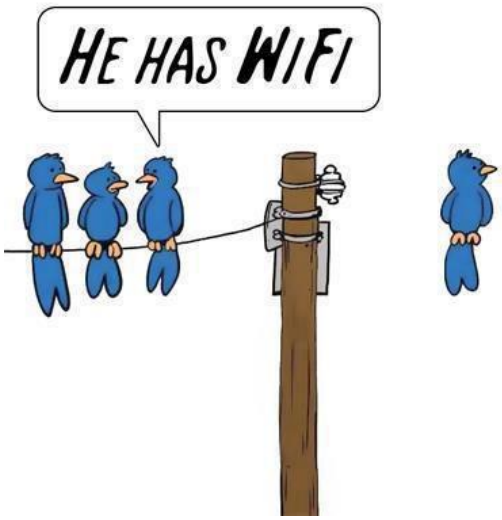
Here you can find the menu:

Monday, September 21st 2015
Salted sponge mixture into a clear vegetable soup
Chickenragout with fresh vegetables and noodles **or** Tortellini filled with spinach on herbal sauce

Tuesday, September 22nd 2015
Potato cream soup
Fried escalope of turkey with pea's rice **or** vegetables lasagne on tomato sauce with grana Padano

WIFI Information

The SSID of the wireless LAN is *Tunetguest*. All participants receive an own user and password. Your personal WIFI information is printed on your badge. Eduroam is also available.



Directions

How to get from the airport to the city centre

The Vienna International Airport (VIE) in Schwechat is about 20 km away in the southeast of Vienna. Train lines S7 and S2 (suburban railway "S-Bahn"), ICE as well as the City Airport Train (CAT) connect the city center with the airport.

You can also take a taxi for your convenience, a taxi fare is at about 30 Euro. We recommend a pre-booked taxi with airportdriver.at. It can be booked online: http://www.airportdriver.at/en/airport-transfe. After the baggage claim, take the left exit and walk left. The driver will wait for you there.

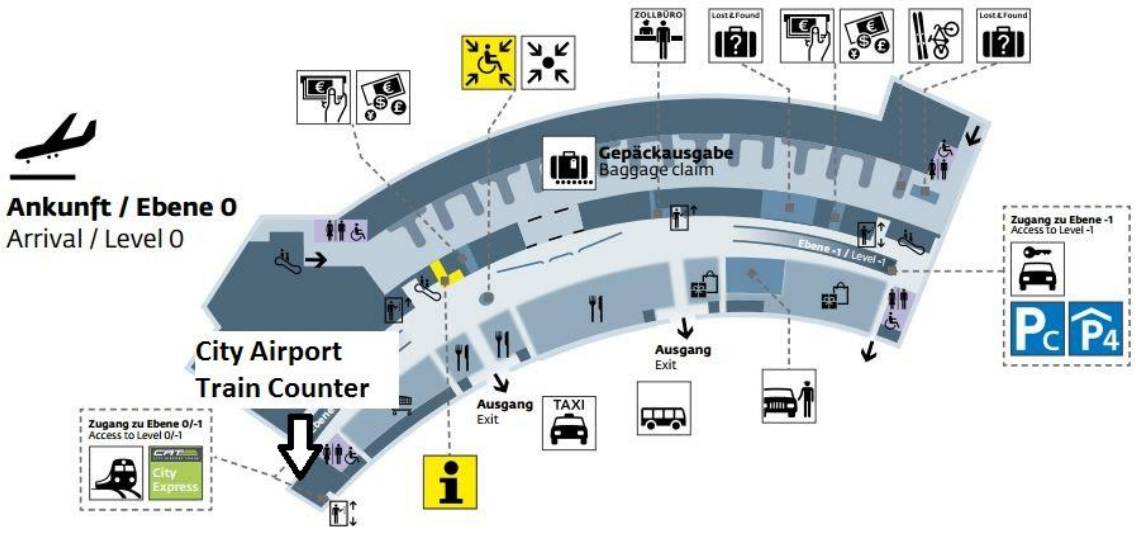
1. City Airport Train / CAT

The CAT takes just 16 minutes nonstop to get from central Vienna to the airport and vice versa. The City Airport Train operates daily from 05.36 a.m. to 23.36 p.m. The City Air Terminal is just 10 minutes from St. Stephan's Cathedral at "Landstraße - Wien Mitte" station, which can be reached easily by tram, underground, bus or taxi. The price for a single fair is €11.00, the exact timetable and more information can be found here: http://www.cityairporttrain.com/

Overview departure time CAT

Departure	Arrival	First train (departure)	Last train (departure)	Duration
Wien Mitte	Vienna Airport	05:36 (then 06 & 36 min. past the hour)	23.06	16 min
Vienna Airport	Wien Mitte	06:06 (then 06 & 36 min. past the hour)	23.36	16 min

Vienna Airport Map



Map 2: Vienna Airport Map

2. S-Bahn / suburban railway

The Schnellbahn (S-Bahn) is a low-priced way of getting from Vienna to the airport and back. Price: from € 4.40 (including travel on Vienna public transport). Ticket machines are on the platforms at the airport and at Wien Mitte.

The following table gives a summary of the S-Bahn timetable between "Landstraße - Wien Mitte" and Vienna Airport. To get to the city center you need to take the S-Bahn line "S7" in direction "Floridsdorf".

Departure	Arrival	First suburban railway (departure)	Last suburban railway (departure)	Duration
Wien Mitte	Vienna Airport	04:30 (then apprx. Every 30 min)	23:45	25 min
Vienna Airport	Wien Mitte	04:56 (then apprx. Every 30 min))	00:17	25 min

3. ICE/ long-distance train

The ICE departs every 2 hours from Vienna to the airport or from the Airport to Vienna. In Vienna it stops at two train stations "Wien-Hauptbahnhof" and "Wien Meidling". From "Wien Hauptbahnhof" you can take the red undergoundline (U1) direction "Leopoldau" and get out at the stop "Karlsplatz" or "Stephansplatz".

The following table gives an overview of the timetable.

	From the Airport			To the Airport		
	Vienna Airport	**Wien Hauptbahnhof**	**Wien Meidling**	**Wien Meidling**	**Wien Hauptbahnhof**	**Vienna Airport**
First train	6:25 (then every 2 hours)	06:41 (then every 2 hours)	06:49 (then every 2 hours	07:27 (then every 2 hours)	07:38 (then every 2 hours)	07:56 (then every 2 hours)
Last train	22:00	22:16	22:24	21:07	21:15	21:32

How to get from the airport directly to the Conference Venue

Address of the Conference Venue:
Vienna University of Technology
„Altes Elektrotechnik Institut“
Gusshaustraße 25
1040 Vienna
Austria

Choose a connection from before, either the CAT or the S-Bahn (see information before) to get from the airport to the venue. The closest underground stops are “Karlsplatz” (U1/U4/U2) or “Taubstummengasse” (U1).

If you decide to take the CAT to get to the Conference Venue:

The last stop is “Landstraße - Wien Mitte” (1). Get out there and take the green underground line (U4) in direction “Karlsplatz”. (2) Then you can either walk to the conference venue (exit “Resselpark”) or change to the red underground line (U1), direction “Reumanplatz” and get out at “Taubstummengasse” (3) then follow the signs to the exit “Floragasse” from there it is just a 3 minutes’ walk to the venue. See map 3.

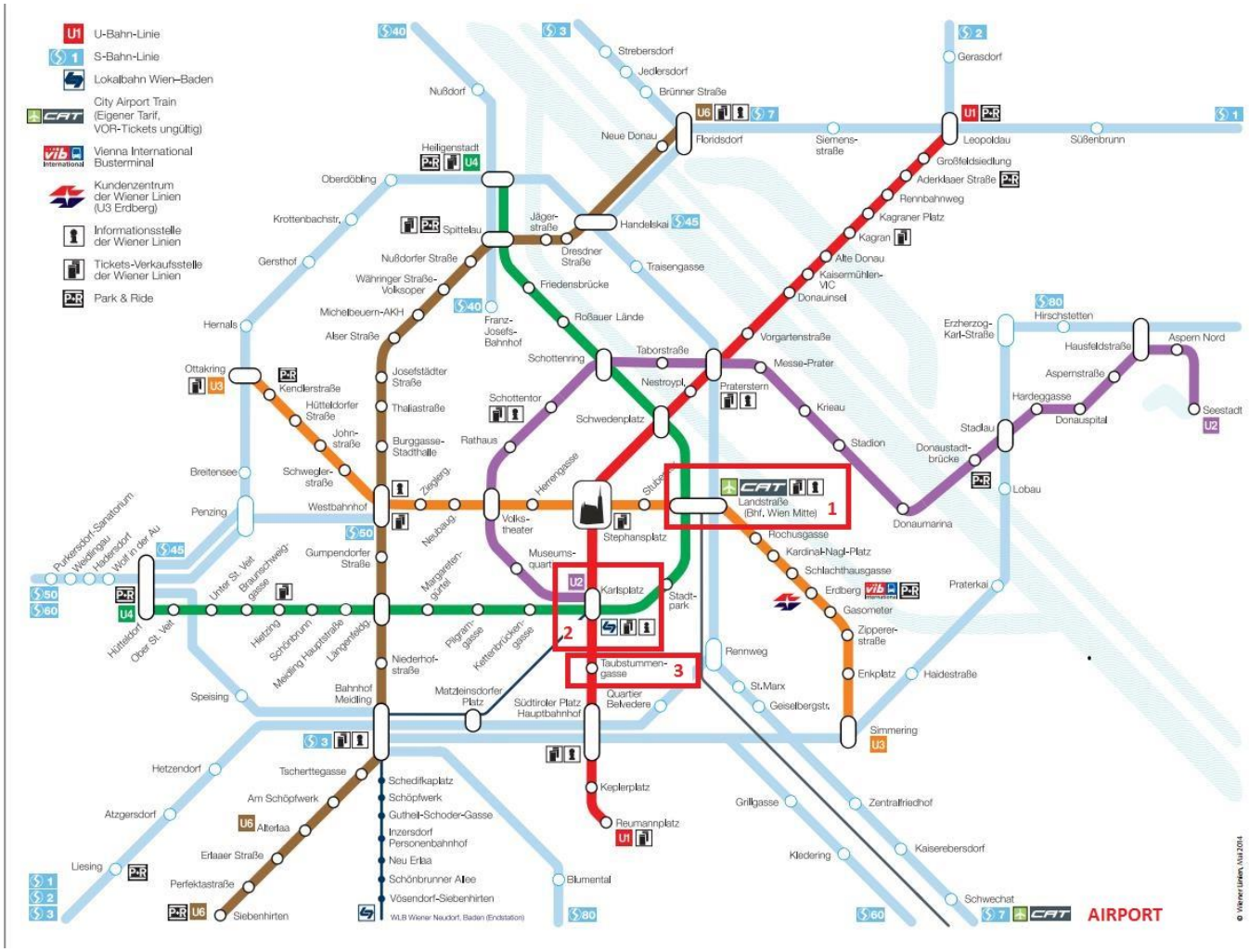
If you decide to take the S-Bahn to get to the Conference Venue:

Get out at the stop “Praterstern” (1) and take the red underground line (U1) in direction “Reumanplatz”. Get out at “Taubstummengasse” (2) then follow the signs to the exit “Floragasse” from there it is just a 3 minutes’ walk to the venue. See map 6.

If you decide to take the ICE to get to the Conference Venue:

Get out at “Wien Hauptbahnhof” (1) and take the red underground line (U1) direction “Leopolau” and get out at the stop “Taubstummengasse” (2) then follow the signs to the exit “Floragasse” from there it is just a 3 minutes’ walk to the venue. See map 7.

Underground Map CAT



Map 3: CAT: Airport - Conference Venue

1 Get out at “Landstraße - Wien Mitte” and change to U4 (“Hütteldorf”)

2 Get out at “Karlsplatz” and walk or change to U1 (“Reumanplatz”)

3 Get out at “Taubstummengasse”

Walking Distances

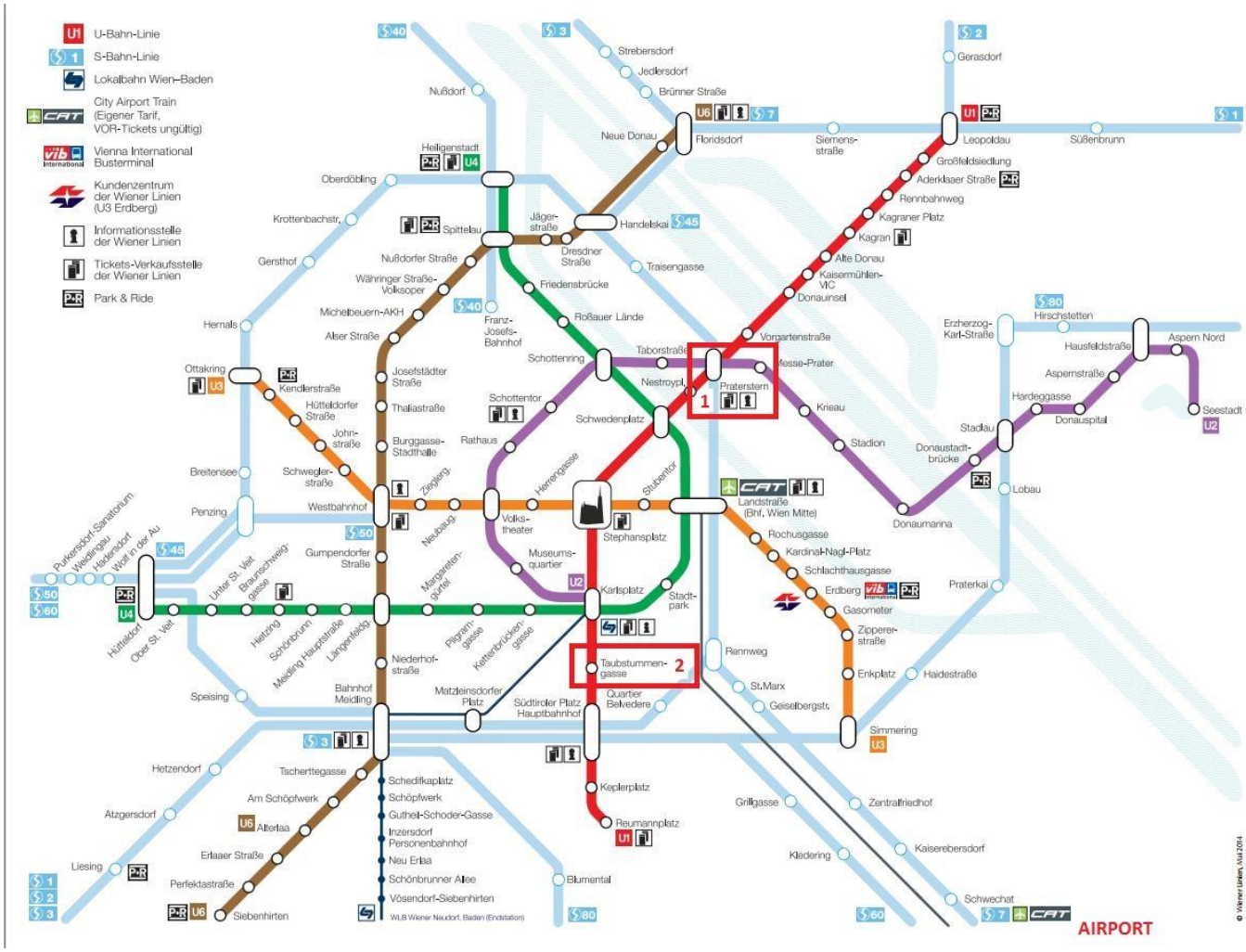
Stop „Taubstummengasse“ to the conference venue:

Map 4: Taubstummengasse (U1) to Conference Venue

Stop “Karlsplatz” to the conference venue:

Map 5: Karlsplatz (U1/U4/U2) to Conference Venue

Underground Map S-Bahn

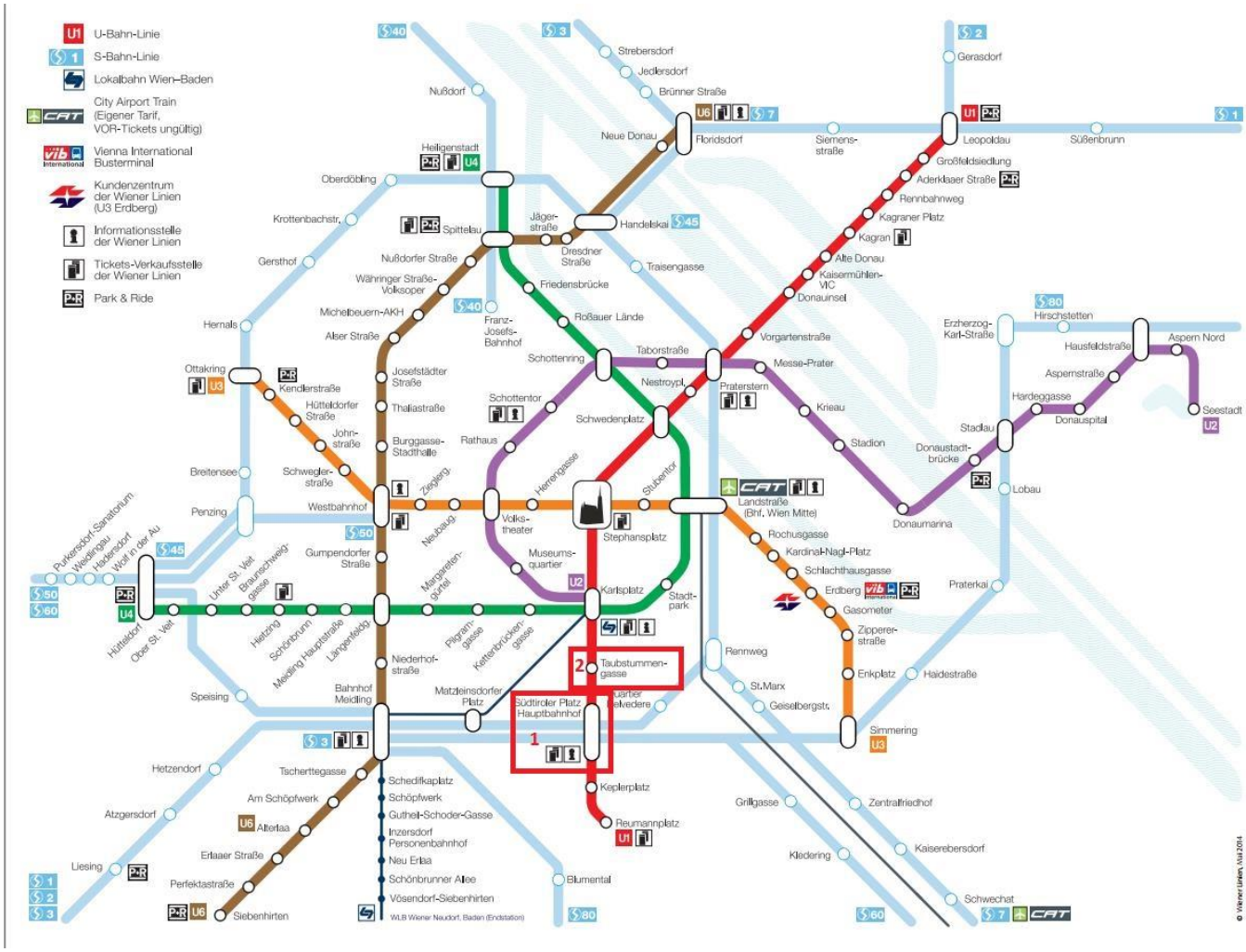


Map 6: S-Bahn: Airport -> Conference Venue

1 Get out at “Praterstern” and change to U1 (“Karlsplatz”)

2 Get out at “Taubstummengasse”

Underground MAP ICE

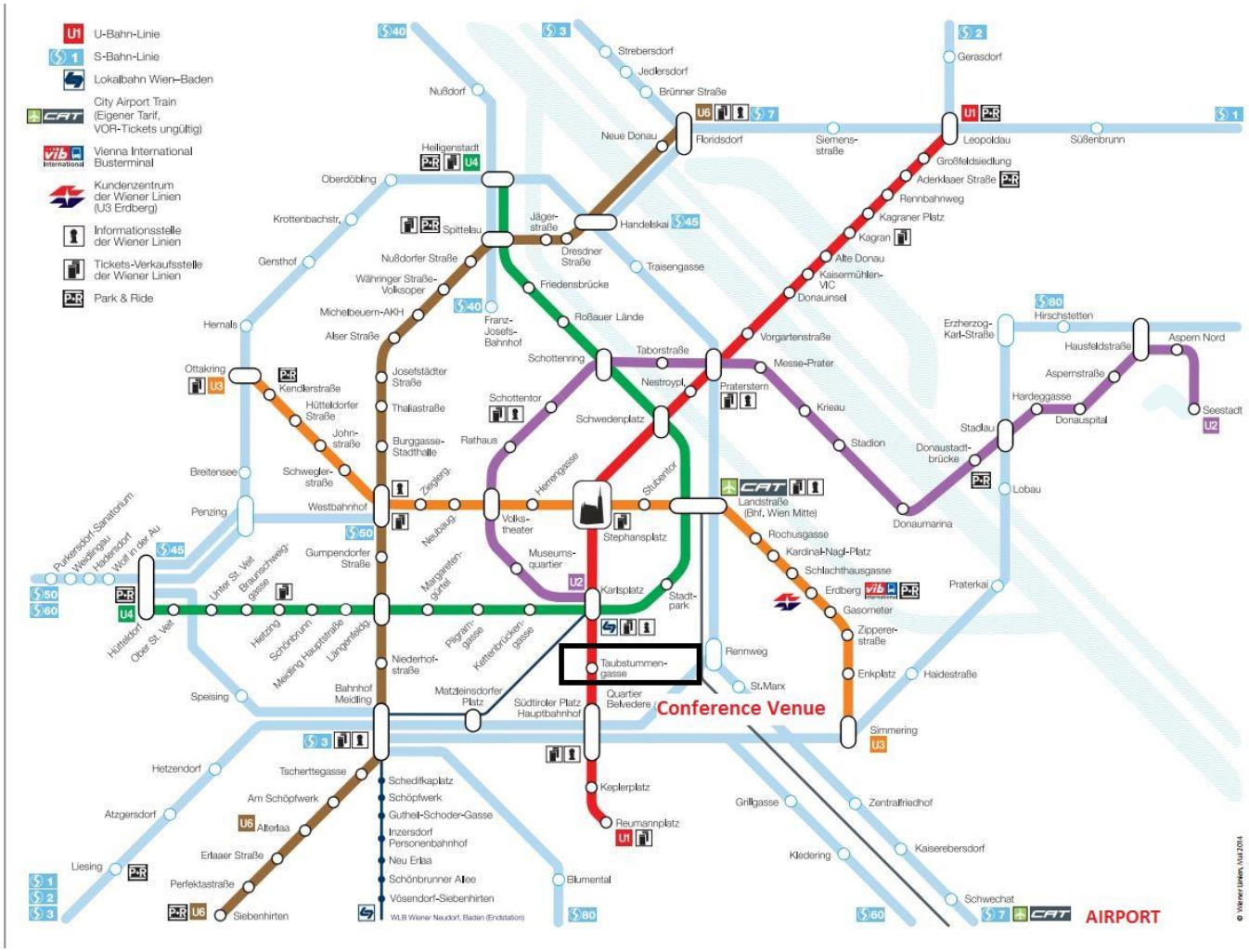


Map 7: ICE Airport -> Conference Venue

1 Get out at “Wien Hauptbahnhof” and change to U1 (“Karlsplatz”)

2 Get out at “Taubstummengasse”

Public Transport



Map 8: Public Transport Vienna

The underground trains (U-Bahn) run from about 5.00 am in the morning to about midnight. The underground trains run around the clock on Friday and Saturday and on the eve of public holidays!

Welcome to Vienna!

Useful Information

Tourist Information
1st district, city centre Albertinaplatz, corner of Maysedergasse Daily from 9.00 am to 7.00 pm Vienna International Airport, Schwechat Arrival hall Daily from 7.00 am to 10.00 pm

Emergency Numbers	
Fire service	122
Police	133
Ambulance/ rescue	144
Emergency doctor	141
European emergency	112

Opening hours shops in Vienna

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.

WIFI in Public Transport

In Vienna there are 10 WIFI Hotspots available in the public transportation systems. These are set up near the information offices in the following metro stations:

- Südtiroler Platz/Hauptbahnhof (U1, red line)
- Karlsplatz (U1, red line/U2, purple line/ U4, green line)
- Stephansplatz (U1, red line/ U3, orange line)
- Praterstern (U1, red line/U2, purple line)
- Schottentor (U2, purple line)
- Westbahnhof (U6, brown line/ U3, orange line)
- Landstraße (U3, orange line/ U4, green line)
- Erdberg (U3, orange line)
- Meidling (U6, brown line)
- Floridsdorf (U6, brown line)

Public Transport Tickets

24-, 48- & 72-hour-ticket

24-hour-ticket € 7.60
48-hour-ticket € 13.30
72-hour-ticket € 16.50

About

- ticket is valid for 24, 48 or 72 hours from validation
- valid on all public transport services in Vienna

Vienna Weekly Ticket

Weekly ticket (Monday-Sunday) € 16.20

About

- ticket is valid for one week, from Monday to Sunday during this week it can be used for as many rides as you want

Single Trip

Single Trip € 2.20

About

- can be used to travel once in one direction and are valid from the time they are punched in a validating machine
- you may change between tram, bus and underground as often as you like, but without interrupting travel

Tickets are available

- at the Vienna transport Authority´s ticket offices
- ticket machines
- tobacconists
- online: https://shop.wienerlinien.at/

About Vienna

Vienna is old, Vienna is new – and so diverse: from the magnificent Baroque buildings to “golden” Art Nouveau or the latest architecture. Vienna is packed with imperial history; at the same time it has exciting contemporary museums, lively eating and a vibrating nightlife, but also many quiet corners to explore.

Few cities can boast the imperial grandeur of Vienna, once the centre of the powerful Habsburg monarchy. Lipizzaner stallions performing elegant equine ballet, the angelic tones of the Vienna Boys' Choir drifting across a courtyard and, outrageously opulent palaces.

Walk in the footsteps of the Habsburgs, visit the splendid baroque Schönbrunn or Belvedere Palaces, or stroll along the magnificent Ring Boulevard to take a look at the heart of the former vast Habsburg Empire, the Imperial Palace. Get a sense of the luster and glory of the old empire by visiting St. Stephen’s Cathedral, the Spanish Riding School, and the Giant Ferris Wheel at the Prater, as well as the sarcophagi in the Imperial Vault.

Visit Empress Sisi’s former summer residence. This baroque complex contains an enchanting park, the Palm House,

Schloss Schönbrunn

the Gloriette and a zoo. Spend an entire day at Schönbrunn: visit the show rooms with a "Grand Tour with Audio Guide," admire the splendid Bergl Rooms, and stroll through the “Labyrinth.” Schönbrunn Zoo in Vienna is the oldest existing zoo in the world and has been named Europe's best on three occasions. Each year more than two million visitors come to see the panda baby, new-born elephants and many other rare animals.

Beautiful and celebrated Empress Elisabeth has long since become a cult figure. The Sisi Museum in the Imperial Apartments of the Imperial Palace compares the myth and the facts. Among the highlights are numerous personal objects once owned by Elisabeth as well as the most famous portraits of the beautiful empress.
The Spanish Riding School in only a few steps away from the Sisi Museum and will be celebrating the 450th anniversary of its first written mention with gala performances on Heldenplatz in 2015.

Emperor Franz Joseph officially opened Vienna's Ringstrasse on May 1, 1865. Vienna is celebrating its 150th birthday in 2015 with numerous events and exhibitions. The most beautiful boulevard in the world not only rich in sights, it also has large parks, important monuments, and much more. About 800 buildings line the boulevard today. Additional sights on the Ringstrasse, aside from the many opulent buildings, include the black-gold lattice fence in front of the Hofburg, the world’s longest fence from the age of Historicism, the 5.5-meter-tall Pallas Athene statue in front of the Parliament, and the “Rathausmann”, a statue of a man on the tower of City Hall.

Vienna State Opera

The University of Vienna is the second oldest German-speaking University in the world. The building on the Ring was erected in the style of the Italian High Renaissance. The first university in Vienna had already be founded in 1365, but elsewhere in the city. That's why the 650th birthday of the most important educational institution in the country will be celebrated in 2015.

Vienna is one the most musical cities in the world. This is partly due to the vast number of great composers and musicians who were born here or lived and worked here. Visiting Austria's capital therefore means experiencing the works of Mozart, Haydn, Schubert, Beethoven, Johann Strauss and many others in venues like the Staatsoper and Musikverein. The music of Bach and Händel continues to be performed in Vienna's historic churches today, and Vienna's Collection of Ancient Musical Instruments, paired with a visit to the Haus der Musik, takes you deeper into the texture of music and how it is created. Venues for classical music are augmented by some great clubs and live rock and jazz places.

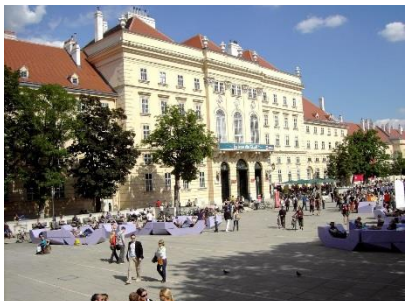

Volksgarten

The Mercer Study has chosen Vienna as the world's number one most liveable city for the sixth time in a row in 2015. More than half of the metropolitan area is made up of green spaces. 280 imperial parks and gardens enrich the cityscape. In spring, 400 species of rose bloom in the Volksgarten alone. The nearby recreation areas of Prater, Vienna Woods and Lobau invite visitors to go on walks, day trips, hikes and bicycle tours. Vienna has a total of 2,000 parks.

St. Stephen's Cathedral is the symbol of Vienna. Construction commenced in the 12th century. Today, it is one of the most important Gothic structures in Austria. Stephen's Cathedral is located directly in the city centre, at the religious and geographical heart of Vienna. It´s giant Pummerin bell features on television as it rings in the New Year.

It's hard to imagine a more liveable city than Vienna. This is a metropolis where regulars sit in cosy coffee houses and offer credible solutions to the worlds chaos over the noble bean; where Beisln (bistro pubs) serve delicious brews, wines and traditional food; where talented chefs are taking the capital in new culinary directions; and where an efficient transport system will ferry you across town from a restaurant to a post-dinner drink in no time at all. It's safe, it has lots of bicycle tracks and it even has its own droll sense of humour.

Vienna is a city where postmodernist and contemporary architectural designs contrast and fuse with the monumental and historic. The MuseumsQuartier is a perfect example, with modern museum architecture integrated into a public space created around former stables for the Habsburgs' horses.


Museumsquartier

Twentieth-century designs are little short of inspiring, while contemporary Vienna is constantly being given new and exciting infrastructural designs such as the new Twin City Liners boat landing and the enormous Hauptbahnhof.

Vienna also hosts several international events such as the famous opera ball that takes place every year in February, which is taking place in the Vienna State Opera. The Life Ball, one of the biggest AIDS charity events worldwide also takes place in Vienna and is held in front of the city hall. Each Life Ball is attended by stars, designers and politicians from all over the world such as Bill Clinton, Katy Perry and Charlize Theron and Jean Paul Gaultier. In 2015 Vienna is celebrating not only one but three anniversaries; 150 years Ringstrasse, 450 years of the Spanish Riding School and 650 years University Vienna. Furthermore Vienna hosted the 60th Eurovision Song Contest in May 2015.

Eurovision Song Contest 2015

Sources: Vienna Info, Lonely Planet

Tips from a Local

Here you can find some restaurant tips from a local!
Watch out because some of them are very crowded places, so it may be a good idea to reserve a table before you go there.

Restaurants

- **Flatschers**: The best steak in town. Steaks starting at € 25 without side dishes. Super-professional personnel. http://www.flatschers.at/, Kaiserstraße 121, 1070 Vienna
- **Brickmakers**: Smoked barbecue, Cider and one of the best beer collections I know in Vienna. Meat is smoked 13 hours before serving. http://www.brickmakers.at/, Zieglergasse 42, 1070 Vienna
- **Toma tu Tiempo**: Spanish tapas just as good (or even better) than in Spain. Good collection of Spanish wines. http://www.tomatutiempo.at/, Zieglergasse 44, 1070 Vienna
- **Grünspan**: Restaurant with classic Austrian dishes of very high quality, but not as expensive as the other restaurants in the first district. http://www.plachutta.at/de/gruenspan/, Ottakringer Straße 266, 1160 Vienna
- **Schweizerhaus**: Restaurant where they have the famous "Stelze" (part of the pig's leg). They also have drought Budweiser beer. Awesome beer garden. http://www.schweizerhaus.at/, Prater 116, 1020 Vienna
- **Wratschko:** Viennese atmosphere, delicious Viennese food. (no website) Neustiftgasse 51, 1070 Vienna

Cocktail Bars

- **Ebert's Cocktail Bar:** In my opinion, the best cocktails in town. They also have a cocktail school where you can learn how to mix awesome cocktails yourself. http://www.eberts.at/, Gumpendorfer Straße 51, 1060 Vienna
- **The Sign**: Equal in quality, but way better-looking cocktails than in Ebert's. http://www.thesignlounge.at/, Liechtensteinstraße 104-106, 1090 Vienna
- **Dino's American Bar**: One of the old and classic American cocktail bars in Vienna. Awesome cocktails (try the Whiskey Sour with white of egg). http://www.dinos.at/, Salzgries 19, 1010 Vienna
- **Barfly's**: Another old and classic American cocktail bar. It is inside a hotel. Huge collection of Whiskey and Rum. http://www.castillo.at/en/, Esterzahygasse 33, 1060 Vienna (Hotel Fürst Metternich)

Bars and Pubs

- **Känguruh**: Awesome bar that has a collection of about 300 beers (mostly Belgian, German and Austrian). http://www.kaenguruh-pub.at/, Bürgerspitalgasse 20, 1060 Vienna
- **Wein & Co**: Elegant bar, great opportunity to taste a huge collection of Austrian and international wines. Dress up elegant if you go there. https://www.weinco.at/filiale/wien-mariahilfer-strasse-9321, Mariahilfer Straße 36, 1070 Vienna
- **Hawidere**: (Hawidere = an Austrian way of greeting a good friend), extremely cozy and friendly Austrian pub in the 15th district. Good selection of beers, also Burgers and other things to eat. http://www.hawidere.at/, Ullmannstraße 31, 1150 Vienna

Cafés

- **Café Josefine**: Young, fresh and small café in the 8th district of Vienna. Awesome coffee, breakfast and small things to eat. http://cafejosefine.at/, Laudongasse 10, 1080 Vienna
- **Café Sperl:** Traditional Austrian café with a nice garden. http://www.cafesperl.at/, Gumpendorfer Straße 11, 1060 Vienna

Cultural Program

Taking place from September 21-27, 2015

Here you can find concerts, exhibitions and sightseeing trips taking place during your stay in Vienna.

Tourism Information Vienna:

Here are some websites that provide further information and suggestions for you stay in Vienna:
http://www.wien.info/en
http://www.lonelyplanet.com/austria/vienna
https://www.viennasightseeing.at/en/
http://www.viennaticketoffice.com/home_en.php

If you need any assistance concerning the booking of sightseeing tours, concerts or exhibitions please do not hesitate to contact the conference office.

Cafe Concerts, Heurigen & Dinner Shows

1st Viennese Heurigen Show

A successful blend of Viennese Waltz and Operetta with traditional Viennese Heurigen Culture is presented by the first Wiener Heurigen Show at the famous "Wine Tavern Wolff". The rustic ambient of this genuine wine tavern (in family possession since 1602), provides an ideal setting for an authentic experience of Viennese music, cuisine and wine culture. Dressed in colourful costumes, the talented musicians of the 1st Wiener Heurigen Show, supported by 2 singers and 2 charming dancers, entertain their audience with a selection of famous waltz melodies, polkas and romantic arias & duets from operettas.

Date:	Wed. 23rd September 2015, 8:15 p.m.
Venue:	Wolff Wine Tavern, Rathstrasse 44-46 1190 Vienna
Price:	25-48€
Contact information:	+43 1 524 74 78 tickets@heuriger.com www.heuriger.com

Austrian Dinner Show

A musical and culinary journey through Austria.

A musical journey from the mountains of Tirol, the charming lakes of the Salzkammergut, and from the romantic Danube Valley to imperial Vienna awaits the visitors of the “Austrian Dinner Show". Traditional folklore tunes and colorful dances, a spirited “Landler“ from the Alps, romantic arias from Salzburg and famous Waltzes and Operettas from Vienna, the highly talented musicians of the ensemble, excellent vocal soloists and spirited dancers will enchant with their performance of the musical treasures of Austria. Between each dinner course, the visitors experience an exciting program divided into 3 entertaining show scenes. During dinner, typical Viennese music will be played live.

Date:	Mon. 21st September 2015, 8 p.m. Wed. 23rd September 2015, 8 p.m., Fri. 25th September 2015
Venue:	Wiener Rathauskeller Rathausplatz 1 1010 Wien
Price:	58€
Contact information:	+43-1-274 90 46 office@dinnershow.at www.austriandinnershow.at

Exhibitions

Monet to Picasso. The Batliner Collection

Claude Monet
View of Vétheuil, 1881

Under the title “Monet to Picasso”, the Albertina exhibits its vast holdings of paintings from the period of Modernism, which are primarily made up of works from the Batliner Collection. The epochs covered by this reinstallation of the museum’s permanent collection range from Impressionism and Fauvism to German Expressionism, the Bauhaus, and the Russian avant-garde; the presentation concludes with works by Picasso.

Lee Miller

Lee Miller (1907-1977) is considered one of the most fascinating artists of the 20th century. In over five decades, she produced a body of photographic work of a range that remains unparalleled, and that unites the most divergent genres. Miller’s oeuvre extends from surrealistic images to photography in the fields of fashion, travelling, portraiture and even war correspondence; the Albertina presents a survey of the work in its breadth and depth, with the aid of 90 selected pieces.

Drawing Now: 2015

Tornado Amarillo Doble, Thyssen-Bornemisza Art

Forty years after Drawing Now, the legendary exhibition mounted jointly with the MoMA in New York, 2015 will see the Albertina once again attempt to take stock of what drawing means or can mean today. In the present showing, selected works by 36 international artists and artist groups turn the spotlight on relevant movements of the past ten years.

Drawing Now: 2015 illustrates the broad spectrum of present-day tendencies of drawing in art: its range of featured works runs from the abstract to the figurative and from sketches to large-scale projects planned in great detail. In terms of content, the artists devote their works to private experiences, simple everyday observations, and political events. They also reflect on the medium of drawing itself, examining the conditions and possibilities of such works’ production while also making a theme of appropriated drawing and drawing as a performative or collaborative act.

Date:	daily, 10 a.m. - 6 p.m.
Venue:	Albertina Albertinaplatz 1 1010 Wien
Contact information:	+43 1 534 83 0 info@albertina.at www.albertina.at

Sightseeing

Vienna Ring Tram

You can get to know Vienna's wonderful boulevard, the Ringstrasse around the Old City, in comfort from the Vienna Ring Tram – all year round, daily from 10.00 am to 5.30 pm.

Inside the wagons (31 seats), LCD screens inform you about the highlights along the route, supplemented with information in several languages over the headphones. Duration: 25 minutes; tickets can be purchased on board the tram and at the advance sales outlets of Wiener Linien Boarding and alighting point on Schwedenplatz

Date: daily from 10.00 am to 5.30 pm on the hour and half hour
Venue: Schwedenplatz
1010 Wien
Contact information: http://www.wienerlinien.at
Ticket price: 8€

Vienna at First Glance - Guided Walk

Comprehensive introduction to the most important sights of Vienna's historical center.

Meeting point: Tourist-Info, 1., Albertinaplatz / Ecke Maysedergasse

As of 3 people, irrespective of weather conditions, duration: 1 1/2-2 h, excluding admission fees, no booking required.

Date: daily, 2 p.m.
Contact information: +43 1 489 96 74
d.office@wienguide.at
www.wienguide.at
Ticket price: 15€

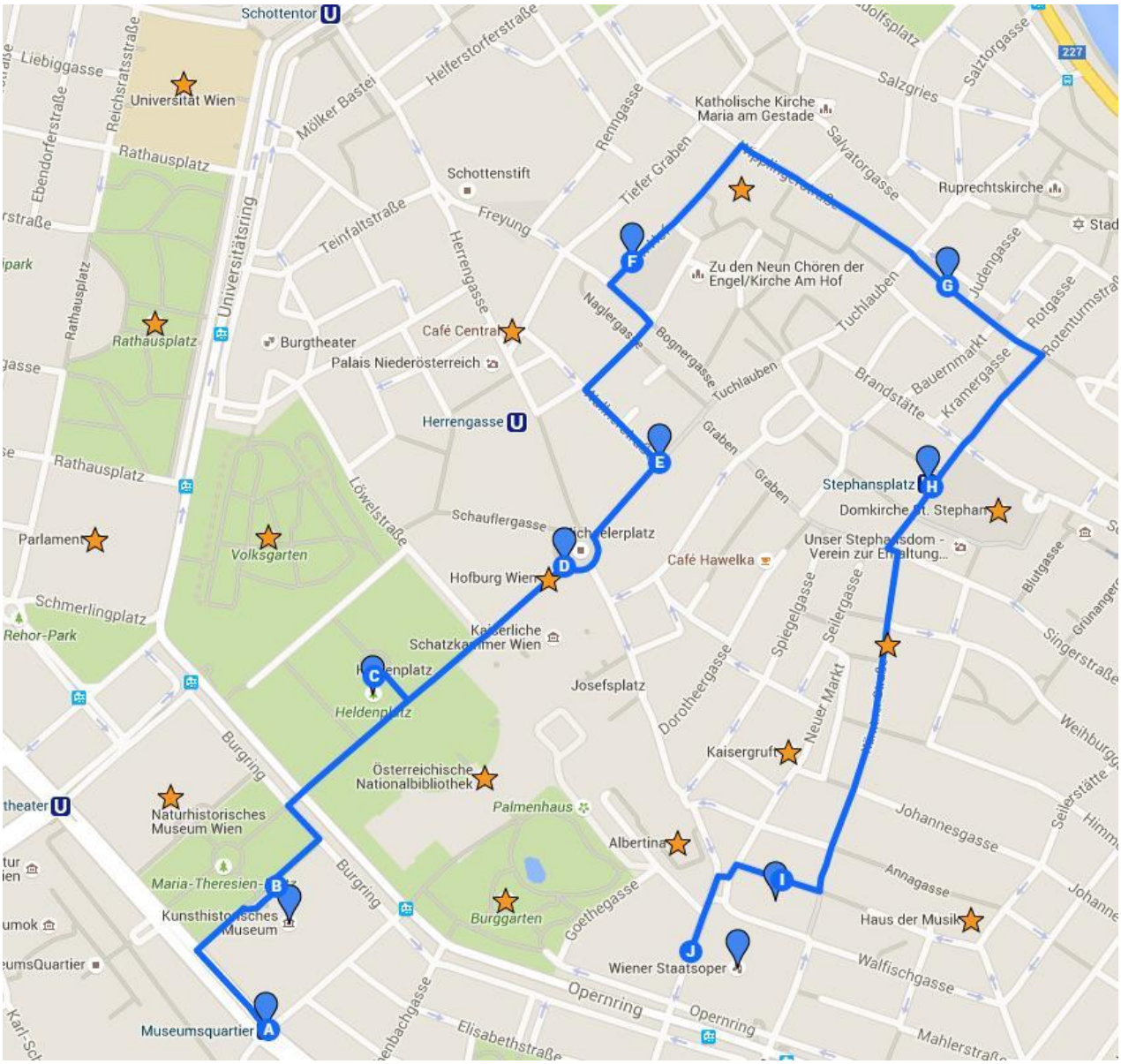
Guided Tours Spanish Horse Riding School

including Stables

A unique tour of the Spanish Riding School takes you to the different "stations" which account for the special charm of this institution. The Winter Riding School, a gem of baroque architecture; the Summer Riding School, one of Vienna's quietest and unexpected spots; the Stallburg, Vienna's most significant Renaissance building with the stables of the Lipizzaners.

Date: Monday – Sunday at 2, 3 and 4 p.m.
Venue: Spanish Riding Scool (Spanische Hofreitschule)
Michaelerplatz 1 (Besucherzentrum)
1010 Wien
Contact information: +43-1-533 90 32
www.srs.at
office@srs.at
Ticket price: 16€

Exploring Vienna by yourself – Vienna´s Inner City



A) Museumsquartier
B) Kunsthistorisches Museum (Museum of Art History)
C) Heldenplatz
D) Michaelerplatz
E) Kohlmarkt
F) Am Hof
G) Hoher Marks
H) Stephansplatz (St. Stephens Square)
I) Hotel Sacher Wien
J) Wiener Staatsoper (Vienna State Opera)

A detailed “Exploring Vienna by yourself” guide including information on the sights will be available at the registration.

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

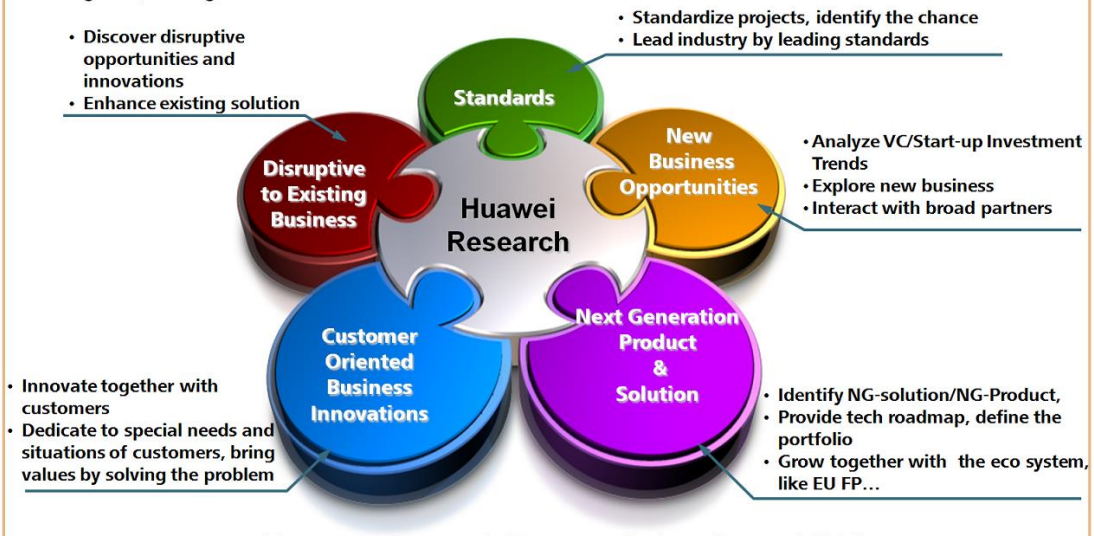
Bettina Bauer
bbauer@sba-research.org
Tel: +43 664 254 03 14

Sponsors / Supporters introduce themselves

HUAWEI

Huawei CRI Vision: Innovating the Future

Huawei **Central Research Institute (CRI)** currently has 1000+ researchers , and it is globally located in US, Germany, Singapore, Canada, Sweden, Russia ,Hong Kong and Shenzhen, Beijing, Shanghai, Hangzhou, Chengdu in China.



Huawei Central Research Institute (CRI)

Shield Lab of CRI: Research on ICT Security

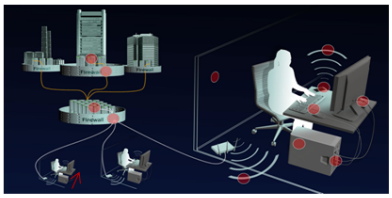
Shield Lab has four branches distributed in Singapore, Beijing, Shenzhen and Paris, and is focusing on the security technologies for the forthcoming ICT, including but not limited to:

- 5G Security
- Mobile Security and Advanced Defense Technologies
- Cloud Infrastructure and Virtualization Security
- IoT Security and Privacy
- Cryptography and Its Applications

Our Mission: To create defending technologies against attacks and misbehaviors in the ICT domain for the era of blending physical and digital worlds.

HUAWEI

Data Center



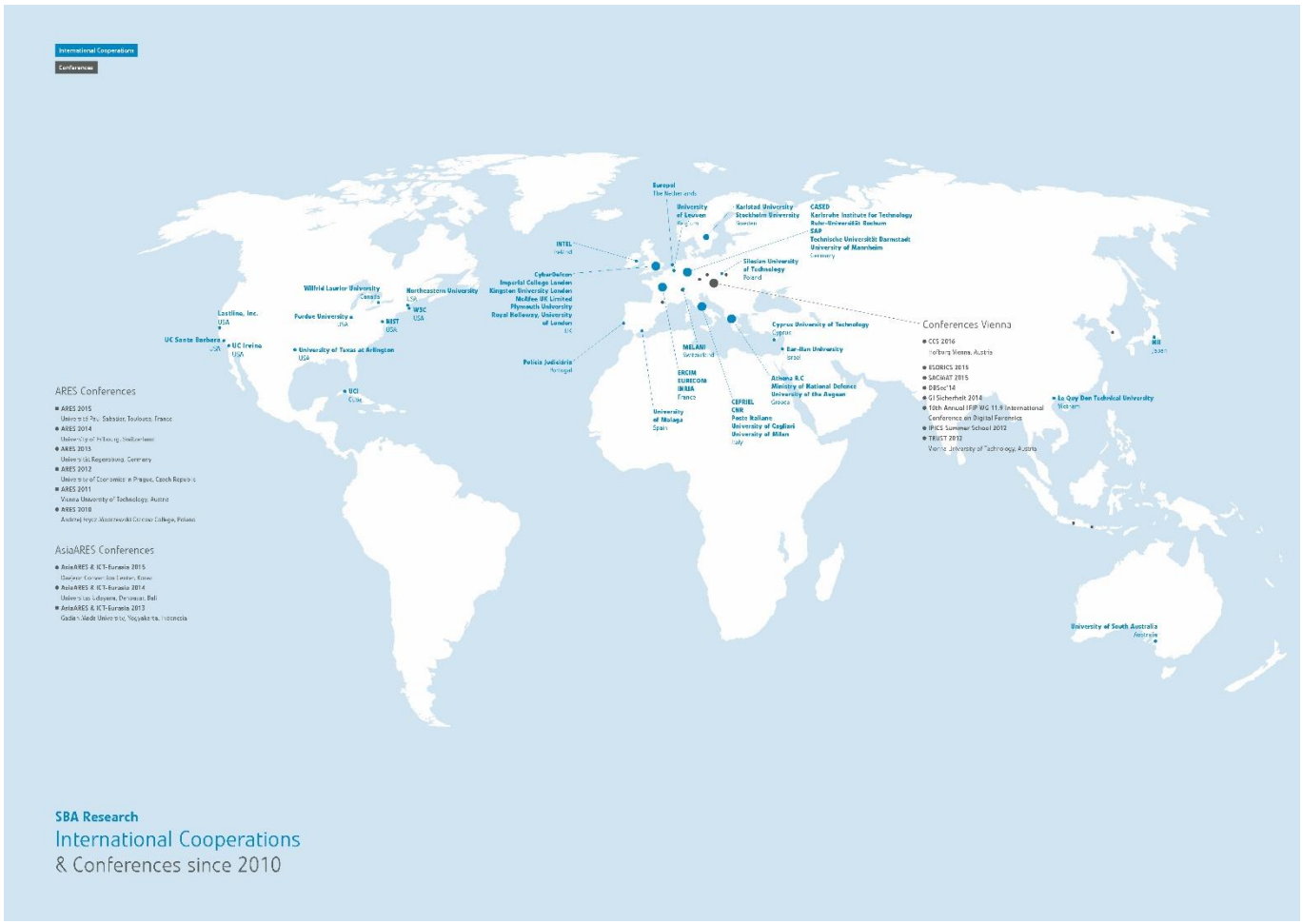
Communication Network Terminal

SBA Research

SBA Research is the research center for information security in Austria

SBA Research was founded in 2006 as the first Austrian research center for information security by the TU Wien, the Graz University of Technology and the University of Vienna. In recent years, the Vienna University of Economics and Business, the AIT Austrian Institute of Technology and the University of Applied Sciences St. Pölten joined as academic partners. Through scientific research of information security we develop practical and applicable solutions, while focusing on current issues like cyber security. SBA Research employs approx. 100 people and is by now the largest research center in Austria which exclusively addresses information security. The center is part of the Austrian COMET excellence program (COMET – Competence Centers for Excellent Technologies).

SBA Research researches and develops solutions in information security. Information security protects IT infrastructure and data against damages done by persons or events. Thereby the results of fundamental research are the basis for applied research and development.
The four research areas of SBA Research allow a comprehensive consideration of information security: AREA 1 addresses organisational security issues and the security of business processes; AREA 2 deals with data security and the protection of privacy for people, institutions and companies; AREA 3 is dedicated to software security and the prevention of cyber-attacks; AREA 4 covers the security of hardware and infrastructure.



www.sba-research.org

	Monday, Sept 21				Tuesday, Sept 22			
	LH E	LH B	LH C		LH E	LH F	LH C	LH B
08:00 - 17:00	REGISTRATION			08:00 - 17:00	REGISTRATION			
09:00 - 10:30	STM I	SIoT I	QASA & DPM I	09:00 - 10:30	STM V	SHCIS I	CyberICS & WOS-CPS & DPM-QASA Lecture Hall C	
10:30 - 11:00	Break			10:30 - 11:00	Break			
11:00 - 12:30	STM II	SIoT II	QASA I	11:00 - 12:30	STM VI	SHCIS II	DPM IV	CyberICS I
12:30 - 14:00	Lunch			12:30 - 14:00	Lunch			
14:00 - 15:30	STM III	SIoT III	DPM II	14:00 - 15:30	STM VII (short papers)	SHCIS III	DPM V	WOC-CPS
15:30 - 16:00	Break			15:30 - 16:00	Break			
16:00 - 17:30	STM IV (ERCIM PhD Award) Business Meeting	SIoT IV	DPM III	16:00 - 17:30		SHCIS IV	DPM VI	Cyber-ICS II
18:00 - 22:30	Workshop Dinner							