ESORICS 2015

ESORICS 2015

Program Guide

ESORICS 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

Wednesday, Sept 23		
	LH C	LH D
08:00 - 17:00	REGISTRATION	
09:00 - 09:15	Opening Leture Hall A	
09:15 - 10:15	Keynote Session *Richard Clayton, University of Cambridge, UK* Lecture Hall A	
10:15 - 10:45	Break	
10:45 - 12:15	Session 1A: Network & Web Security	Session 1B: Cryptography I
12:15 - 13:00	Invited Talk *Afonso Ferreira, European Commission* Lecture Hall A	
13:00 - 14:30	Lunch	
14:30 - 16:00	Session 2A: System Security	Session 2B: Cryptography II
16:00 - 16:30	Break	
16:30 - 18:00	Session 3A: Risk Analysis	Session 3B: Cryptography III
18:00 - 22:00	Mayor's Reception	

Thursday, Sept 24		
	LH C	LH D
08:00 - 17:00	REGISTRATION	
09:00 - 10:00	Keynote Session *Sushil Jajodia, George Mason University Fairfax, US* Lecture Hall A	
10.00 - 10:30	Break	
10:30 - 12:00	Session 4A: Privacy I	Session 4B: Signatures
12:00 - 13:30	Lunch	
13:30 - 15:00	Session 5A: Privacy II	Session 5A: Applied Security I
15:00 - 15:30	Break	
15:30 - 17:00	Session 6A: Cloud Security	Session 6B: Protocols & ABE
17:00 - 23:00	Conference Dinner	

Friday, Sept 25			
	LH C	LH D	LH E
08:00 - 17:00	REGISTRATION		
09:00 - 10:30	Session 7A: Cloud Analysis & Side-Channels	Session 7B: Crypto Applications & Attacks	PhD Symposium
10:30 - 11:00	Break		
11:00 - 12:30	Session 8A: Authentication I	Session 8B: Policies	PhD Symposium
12:30 - 14:00	Lunch		
14:00 - 15:30	Session 9A: Authentication II	Session 9B: Detection & Monitoring	PhD Symposium
15:30 - 15:45	Break		
15:45 - 17:15	Session 10: Applied Security II		

Wednesday, 23rd September 2015

09.00-17.00 Registration

09.00 – 09.15 Opening

Lecture Hall A

09.15-10.15 Keynote Session

Session Chair: Peter Y A Ryan (University of Luxembourg, Luxembourg)

Lecture Hall A

Cybercrime data: Big, Biased and Beyond Review?

Richard Clayton (University of Camebridge, UK)

Abstract: I spend my academic life generating and processing data about cybercrime. These datasets are big and getting bigger. Some people say that's true of cybercrime as well, but I don't entirely agree! My datasets are also significantly biased, but once you accept that the bias is there it can lead one to find some really useful results. But perhaps the greatest problem that we all have with cybercrime data is an inability to reproduce each other's work — an essential technique for detecting inadvertent errors and improving analysis techniques. At Cambridge we have a new approach to cybercrime data sharing; and I'll be explaining how it is possible to get involved.

10.15-10.45 Coffee Break

10.45-12.15 Session 1A: Network & Web Security

Session Chair: Rolf Schillinger (Universität Regensburg, Germany)

Lecture Hall C

1. DNS-Scopy: Towards Security of Internet Naming Infrastructure

Haya Shulman and Michael Waidner (Technische Universität Darmstadt, Germany)

Abstract: We study the operational characteristics of the server-side of the Internet's naming infrastructure. Our findings discover common architectures whereby name servers are 'hidden' behind server-side caching DNS resolvers. We explore the extent and the scope of the name servers that use server-side caching resolvers, and find such configurations in at least 38% of the domains in a forward DNS tree, and higher percent's of the domains in a reverse DNS tree. We characterize the operators of the server-side caching resolvers and provide motivations, explaining their prevalence. Our experimental evaluation indicates that the caching infrastructures are typically run by third parties, and that the services, provided by the third parties, often do not deploy best practices, resulting in misconfigurations, vulnerabilities and degraded performance of the DNS servers in popular domains. 2. Waiting for CSP — Securing Legacy Web Applications with JSAgents.

2. Waiting for CSP - Securing Legacy Web Applications with JSAgents

Joerg Schwenk, Mario Heiderich and Marcus Niemietz (Ruhr-University Bochum, Germany)

Abstract: Markup Injection (MI) attacks, ranging from classical Cross- Site Scripting (XSS) and DOMXSS to Scriptless Attacks, pose a major threat for web applications, browser extensions, and mobile apps. To mitigate MI attacks, we propose JSAgents, a novel and flexible approach to defeat MI attacks using DOM meta-programming. Specifically, we enforce a security policy on the DOM of the browser at a place in the markup processing chain "just before" the rendering of the markup. This approach has many advantages: Obfuscation has already been removed from the markup when it enters the DOM, mXSS attack vectors are visible, and, last but not least, the (client-side) protection can be individually tailored to fit the needs of web applications. JSAgents policies look similar to CSP policies, and indeed large parts of CSP can be implemented with JSAgents. However, there are three main differences: (1) Contrary to CSP, the source code of legacy web applications needs not be modified; instead, the policy is adapted to the application. (2) Whereas CSP can only apply one policy to a complete HTML document, JSAgents is able, through a novel cascading enforcement, to apply different policies to each element in the DOM; this property is essential in dealing with JavaScript event handlers and URIs. (3) JSAgents enables novel features like coarse-grained access control: e.g. we may block read/write access to HTML form elements for all scripts, but human users can still insert data (which may be interesting for password and PIN fields).

3. Analyzing the BrowserID SSO System with Primary Identity Providers Using an Expressive Model of the Web

Daniel Fett, Ralf Kuesters and Guido Schmitz (University of Trier, Germany)

Abstract: BrowserID is a complex, real-world Single Sign-On (SSO) System for web applications recently developed by Mozilla. It employs new HTML5 features (such as web messaging and web storage) and cryptographic assertions to provide decentralized login, with the intent to respect users' privacy. It can operate in a primary and a secondary identity provider mode. While in the primary mode BrowserID runs with arbitrary identity providers, in the secondary mode there is one identity provider only, namely Mozilla's default identity provider. We recently proposed an expressive general model for the web infrastructure and, based on this web model, analyzed the security of the secondary identity provider mode of BrowserID. The analysis revealed several severe vulnerabilities, which have been fixed by Mozilla. In this paper, we complement our prior work by analyzing the even more complex primary identity provider mode of BrowserID. We do not only study authentication properties as before, but also privacy properties. During our analysis we discovered new and practical attacks that do not apply to the secondary mode: an identity injection attack, which violates a central authentication property of SSO systems, and attacks that break the privacy promise of BrowserID and which do not seem to be fixable without a major redesign of the system. Interestingly, some of our attacks on privacy make use of a browser side channel that, to the best of our knowledge, has not gained a lot of attention so far. For the authentication bug, we propose a fix and formally prove in a slight extension of our general web model that the fixed system satisfies all the authentication requirements we consider. This constitutes the most complex formal analysis of a web application based on an expressive model of the web infrastructure so far. As another contribution, we identify and prove important security properties of generic web features in the extended web model to facilitate future analysis efforts of web standards and web applications.

10.45-12.15: Session 1B: Cryptography I

Session Chair: Edgar Weippl (SBA Research, Austria)

Lecture Hall D

1. Computational Soundness for Interactive Primitives

Michael Backes, Esfandiar Mohammadi and Tim Ruffing (Saarland University, Germany)

Abstract: We present a generic computational soundness result for interactive cryptographic primitives. Our abstraction of interactive primitives leverages the Universal Composability (UC) framework, and thereby offers strong composability properties for our computational soundness result: given a computationally sound Dolev-Yao model for non-interactive primitives, and given UC-secure interactive primitives, we obtain computational soundness for the combined model that encompasses both the non-interactive and the interactive primitives. Our generic result is formulated in the CoSP framework for computational soundness proofs and supports any equivalence property expressible in CoSP such as strong secrecy and anonymity. In a case study, we extend an existing computational soundness result by UC-secure blind signatures. We obtain computational soundness for blind signatures in uniform bi-processes in the applied π-calculus. This enables us to verify the untraceability of Chaum's payment protocol in ProVerif in a computationally sound manner.

2. Efficient Zero-Knowledge Proofs for Commitments from Learning With Errors over Rings

Fabrice Benhamouda (ENS, CNRS, INRIA, and PSL, France), Stephan Krenn (AIT Austrian Institute of Technology GmbH, Austria) , Vadim Lyubashevsky (ENS, INRIA, France) and Krzysztof Pietrzak (IST Austria, Austria)

Abstract: We extend a commitment scheme based on the learning with errors over rings (RLWE) problem, and present efficient companion zero knowledge proofs of knowledge. Our scheme maps elements from the ring (or equivalently, n elements from Fq) to a small constant number of ring elements. We then construct Σ-protocols for proving, in a zero-knowledge manner, knowledge of the message contained in a commitment. We are able to further extend our basic protocol to allow us to prove additive and multiplicative relations among committed values. Our protocols have a communication complexity of O(Mnlog q) and achieve a negligible knowledge error in one run. Here M is the constant from a rejection sampling technique that we employ, and can be set close to 1 by adjusting other parameters. Previously known Σ-protocols for LWE-related languages only achieved a noticeable or even constant knowledge error (thus requiring many repetitions of the protocol), or relied on "smudging" out the error (which necessitates working over large fields, resulting in poor efficiency).

3. Interleaving Cryptanalytic Time-memory Trade-offs on Non-Uniform Distributions

Gildas Avoine (Institut Universitaire de France, France), Xavier Carpent (Universit´e Catholique de Louvain, Belgium) and Cédric Lauradoux (INRIA, France)

Abstract: Cryptanalytic time-memory trade-offs (TMTO) are famous tools available in any security expert toolbox. They have been used to break ciphers such as A5/1, but their efficiency to crack passwords made them even more popular in the security community. While symmetric keys are generated randomly according to a uniform distribution, passwords chosen by users are in practice far from being random, as confirmed by recent leakage of databases. Unfortunately, the technique used to build TMTOs is not appropriate to deal with non-uniform distributions. In this paper, we introduce an efficient construction that consists in partitioning the search set into subsets of close densities, and a strategy to explore the TMTOs associated to the subsets based on an interleaved traversal. This approach results in a significant improvement compared to currently used TMTOs. We experimented our approach on a classical problem, namely cracking 7-character NTLM Hash passwords using an

alphabet with 34 special characters. This resulted in speedups ranging from 16 to 76 (depending on the input distribution) over rainbow tables, which are considered as the most efficient variant of time-memory trade-offs.

12.15 – 13.00 Invited Talk

Lecture Hall A

The European Strategic Agenda for Research and Innovation in Cybersecurity

Afonso Ferreira (Trust & Security Unit, European Commission, Belgium)

Abstract: This talk will present the European Strategic Research and Innovation Agenda (SRA) for cybersecurity as it is being released by the Working Group on Secure ICT Research and Innovation (aka WG3) of the Network and Information Security Platform, which is a public-private partnership put in place by the European Commission in 2013. Members of WG3 are close to two hundred. They address issues related to cybersecurity research and innovation in the context of the EU Strategy for Cyber Security and of the Network and Information Security Platform. WG3 identified the key challenges and corresponding desired outcomes in terms of innovation-focused, applied but also basic research in cybersecurity, privacy, and trust. The European SRA for cybersecurity designed by WG3 serves as main input for the drafting of Horizon 2020 Work Programmes by the European Commission and is source of inspiration for the coordination of, and collaboration between, research agendas across Europe, including industry research roadmaps and national research and innovation programmes of the Member States.

13.00-14.30 Lunch Break

14.30-16.00 Session 2A: System Security

Session Chair: Rolf Schillinger (Universität Regensburg, Germany)

Lecture Hall C

1. A Practical Approach for Adaptive Data Structure Layout Randomization

Ping Chen, Jun Xu, (The Pennsylvania State University, USA) Zhiqiang Lin (University of Texas at Dallas, USA), Dongyan Xu (Purdue University, USA), Bing Mao (Nanjing University, China) and Peng Liu (The Pennsylvania State University, USA)

Abstract: Attackers often corrupt data structures to compromise software systems. As a countermeasure, data structure layout randomization has been proposed. Unfortunately, existing techniques require manual designation of randomize-able data structures without guaranteeing the correctness and keep the layout unchanged at runtime. We present a system, called SALADS, that automatically translates a program to a DSSR (Data Structure Self-Randomizing) program. At runtime, a DSSR program dynamically randomizes the layout of each security-sensitive data structure by itself autonomously. DSSR programs regularly re-randomize a data structure when it has been accessed several times after last randomization. More importantly, DSSR programs automatically determine the randomizability of instances and randomize each instance independently. We have implemented SALADS based on gcc-4.5.0 and generated DSSR user-level applications, OS kernels, and hypervisors. Our experiments show that the DSSR programs can defeat a wide range of attacks with reasonable performance overhead.

2. Trustworthy prevention of code injection in Linux on embedded devices

Hind Chfouka (University of Pisa, Italy), Hamed Nemati, Roberto Guanciale, Mads Dam (KTH Royal Institute of Technology, Sweden) and Patrik Ekdahl (Ericsson AB, Sweden)

Abstract: We present MProsper, a trustworthy system to prevent code injection in Linux on embedded devices. MProsper is a formally verified run-time monitor, which forces an untrusted Linux to obey the executable space protection policy; a memory area can be either executable or writable, but cannot be both. The executable space protection allows the MProsper's monitor to intercept every change to the executable code performed by a user application or by the Linux kernel. On top of this infrastructure, we use standard code signing to prevent code injection. MProsper is deployed on top of the Prosper hypervisor and is implemented as an isolated guest. Thus MProsper inherits the security property verified for the hypervisor: (i) Its code and data cannot be tampered by the untrusted Linux guest and (ii) all changes to the memory layout is intercepted, thus enabling MProsper to completely mediate every operation that can violate the desired security property. The verification of the monitor has been performed using the HOL4 theorem prover and by extending the existing formal model of the hypervisor with the formal specification of the high level model of the monitor.

3. Practical Memory Deduplication Attacks in Sandboxed Javascript

Daniel Gruss, David Bidner and Stefan Mangard (Graz University of Technology, Austria)

Abstract: Page deduplication is a mechanism to reduce the memory footprint of a system. Identical physical pages are identified across borders of virtual machines and programs and merged by the operating system or the hypervisor. However,

this enables side-channel information leakage through cache or memory access time. Therefore, it is considered harmful in public clouds today, but it is still considered safe to use in a private environment, i.e., private clouds, personal computers, and smartphones. We present the first memory-disclosure attack in sandboxed Javascript which exploits page deduplication. Unlike previous attacks, our attack does not require the victim to execute an adversary's program, but simply to open a website which contains the adversary's Javascript code. We are not only able to determine which applications are running, but also specific user activities, for instance, whether the user has specific websites currently opened. The attack works on servers, personal computers and smartphones, and across the borders of virtual machines.

14.30-16.00 Session 2B: Cryptography II

Session Chair: Stefan Katzenbeisser (TU Darmstadt, Germany)

Lecture Hall D

1. Efficient Message Authentication Codes with Combinatorial Group Testing

Kazuhiko Minematsu (NEC Corporation, Japan)

Abstract: Message authentication code, MAC for short, is a symmetrickey cryptographic function for authenticity. A standard MAC verification only tells whether the message is valid or invalid, and thus we cannot identify which part is corrupted in case of invalid message. In this paper we study a class of MAC functions that enables to identify the part of corruption, which we call group testing MAC (GTM). This can be seen as an application of a classical (non-adaptive) combinatorial group testing to MAC. Although the basic concept of GTM (or its keyless variant) has been proposed in various application areas, such as data forensics and computer virus testing, they rather treat the underlying MAC function as a black box, and exact computation cost for GTM seems to be overlooked. In this paper, we study the computational aspect of GTM, and show that a simple yet non-trivial extension of parallelizable MAC (PMAC) enables O (m + t) computation for my data items and t tests, irrespective of the underlying test matrix we use, under a natural security model. This greatly improves efficiency from naively applying a black-box MAC for each test, which requires O (mt) time. Based on existing group testing methods, we also present experimental results of our proposal and observe that ours runs as fast as taking single MAC tag, with speed-up from the conventional method by factor around 8 to 15 for m = 104 to 105 items.

2. A Symmetric-Key Based Proofs of Retrievability Supporting Public Verification

Chaowen Guan, Kui Ren, Fangguo Zhang (University at Buffalo, USA), Florian Kerschbaum (SAP, Germany) and Jia Yu (University at Buffalo, USA)

Abstract: Proofs-of-Retrievability enables a client to store his data on a cloud server so that he executes an efficient auditing protocol to check that the server possesses all of his data in the future. During an audit, the server must maintain full knowledge of the client's data to pass, even though only a few blocks of the data need to be accessed. Since the first work by Juels and Kaliski, many PoR schemes have been proposed and some of them can support dynamic updates. However, all the existing works that achieve public verifiability are built upon traditional publickey cryptosystems which imposes a relatively high computational burden on low-power clients (e.g., mobile devices). In this work we explore indistinguishability obfuscation for building a roof-of-Retrievability scheme that provides public verification while the encryption is based on symmetric key primitives. The resulting scheme offers light-weight storing and proving at the expense of longer verification. This could be useful in apations where outsourcing files is usually done by low-power client and verifications can be done by well equipped machines (e.g., a third party server). We also show that the proposed scheme can support dynamic updates. At last, for better assessing our proposed scheme, we give a performance analysis of our scheme and a comparison with several other existing schemes which demonstrates that our scheme achieves better performance on the data owner side and the server side

3. DTLS-HIMMO: Achieving DTLS certificate security with symmetric key overhead

Oscar Garcia-Morchon, Ronald Rietman, Sahil Sharma, Ludo Tolhuizen and Jose-Luis Torre-Arce (Philips Group Innovation, Netherlands)

Abstract: Billions of devices are being connected to the Internet creating the Internet of Things (IoT). The IoT not only requires strong security, like current Internet applications, but also efficient operation. The recently introduced HIMMO scheme enables lightweight and collusion resistant identity-based key sharing in a non-interactive way, so that any pair of Internet-connected devices can securely communicate. This paper firstly reviews the HIMMO scheme and introduces two extensions that e.g. enable implicit credential verification without the need of traditional digital certificates. Then, we show how HIMMO can be efficiently implemented even in resource-constrained devices, enabling combined key agreement and credential verification more efficiently than using ECDH-ECDSA. We further explain how HIMMO helps to secure the Internet and IoT by introducing the DTLS-HIMMO operation mode. DTLS, the datagram version of TLS, is becoming the standard security protocol in the IoT, although it is very frequently discussed that it does not offer the right performance for IoT scenarios. Our design, implementation, and evaluation show that DTLS-HIMMO operation mode achieves the security properties of the DTLS-Certificate security suite while exhibiting the overhead of symmetric-key primitives without requiring changes in the DTLS standard.

16.00-16.30 Coffee Break

16.30-18.00 Session 3A: Risk Analysis

Session Chair: Nora Cuppens (Telecom Bretagne, France)

Lecture Hall C

1. Should Cyber-Insurance Providers Invest in Software Security?

Aron Laszka (Vanderbilt University, USA) and Jens Grossklags (Pennsylvania State University, USA)

Abstract: Insurance is based on the diversifiability of individual risks: if an insurance provider maintains a large portfolio of customers, the probability of an event involving a large portion of the customers is negligible. However, in the case of cyber-insurance, not all risks are diversifiable due to software monocultures. If a vulnerability is discovered in a widely used software product, it can be used to compromise a multitude of targets until it is eventually patched, leading to a catastrophic event for the insurance provider. To lower their exposure to non-diversifiable risks, insurance providers may try to influence the security of widely used software products in their customer population, for example, through vulnerability reward programs. We explore the proposal that insurance providers should take a proactive role in improving software security, and provide evidence that this approach is viable for a monopolistic provider. We develop a model which captures the supply and demand sides of insurance, provide computational complexity results on the provider's investment decisions, and propose different heuristic investment strategies. We demonstrate that investments can reduce non-diversifiable risks and can lead to a more profitable cyber-insurance market. Finally, we detail the relative merits of the different heuristic strategies with numerical results.

2. Lightweight and Flexible Trust Assessment Modules for the Internet of Things

Jan Tobias Muehlberg, Job Noorman and Frank Piessens (KU Leuven, Belgium)

Abstract: In this paper we describe a novel approach to securely obtain measurements with respect to the integrity of software running on a lowcost and low-power computing node autonomously or on request. We propose to use these measurements as an indication of the trustworthiness of that node. Our approach is based on recent developments in Program Counter Based Access Control. Specifically, we employ Sancus, a light-weight hardware-only Trusted Computing Base and Protected Module Architecture, to integrate trust assessment modules into an untrusted embedded OS without using a hypervisor. Sancus ensures by means of hardware extensions that code and data of a protected module cannot be tampered with, and that the module's data remains confidential. Sancus further provides cryptographic primitives that are employed by our approach to enable the trust management system to verify that the obtained trust metrics are authentic and fresh. Thereby, our trust assessment modules can inspect the OS or application code and securely report reliable trust metrics to an external trust management system. We evaluate a prototypic implementation of our approach that integrates Sancus-protected trust assessment modules with the Contiki OS running on a Sancus-enabled TI MSP430 microcontroller.

3. Confidence analysis for nuclear arms control: SMT abstractions of Bayesian Belief Networks

Paul Beaumont (Imperial College London, UK), Neil Evans (AWE Aldermaston, UK), Michael Huth (Imperial College London, UK) and Tom Plant (AWE Aldermaston, UK)

Abstract: How to reduce, in principle, arms in a verifiable manner that is trusted by two or more parties is a hard but important problem. Nations and organizations that wish to engage in such arms control verification activities need to be able to design procedures and control mechanisms that capture their trust assumptions and let them compute pertinent degrees of belief. Crucially, they also will need methods for reliably assessing their confidence in such computed degrees of belief in situations with little or no contextual data. We model an arms control verification scenario with what we call constrained Bayesian Belief Networks (cBBN). A cBBN represents a set of Bayesian Belief Networks by symbolically expressing uncertainty about probabilities and scenario specific constraints that are not represented by a BBN. We show that this abstraction of BBNs can mitigate well against the lack of prior data. Specifically, we describe how cBBNs have faithful representations within a Satisfiability Modulo Theory (SMT) solver, and that these representations open up new ways of automatically assessing the confidence that we may have in the degrees of belief represented by cBBNs. Furthermore, we show how to perform symbolic sensitivity analyses of cBBNs, and how to compute global optima of under-specified probabilities of particular interest to decision making. SMT solving also enables us to assess the relative confidence we have in two cBBNs of the same scenario, where these models may share some information but express some aspects of the scenario at different levels of abstraction.

16.30-18.00 Session 3B: Cryptography III

Session Chair: Peter Y A Ryan (University of Luxembourg, Luxembourg)

Lecture Hall D

1. Practical Invalid Curve Attacks on TLS-ECDH

Tibor Jager, Jörg Schwenk and Juraj Somorovsky (Ruhr University Bochum, Germany)

Abstract: Elliptic Curve Cryptography (ECC) is based on cyclic groups, where group elements are represented as points in a finite plane. All ECC cryptosystems implicitly assume that only valid group elements will be processed by the different cryptographic algorithms. It is well-known that a check for group membership of given points in the plane should be performed before processing. However, in several widely used cryptographic libraries we analyzed, this check was missing, in particular in the popular ECC implementations of Oracle and Bouncy Castle. We analyze the effect of this missing check on Oracle's default Java TLS implementation (JSSE with a SunEC provider) and TLS servers using the Bouncy Castle library. It turns out that the effect on the security of TLS-ECDH is devastating. We describe an attack that allows to extract the long-term private key from a TLS server that uses such a vulnerable library. This allows an attacker to impersonate the legitimate server to any communication partner, after performing the attack only once.

2. Making any Identity Based Encryption Accountable, Efficiently

Aggelos Kiayias (National and Kapodistrian University of Athens, Greece) and Qiang Tang (University of Connecticut, USA)

Abstract: Identity-Based Encryption (IBE) provides a compelling solution to the PKI management problem, however it comes with the serious privacy consideration that a trusted party (called the PKG) is required to generate (and hence also know) the secret keys of all users. This inherent key escrow problem is considered to be one of the major reasons hindering the wider utilization of IBE systems. In order to address this problem, Goyal [20] introduced the notion of accountable authority IBE (A-IBE), in which a judge can differentiate the PKG from the user as the source of a decryption software. Via this "tracing" mechanism, A-IBE deters the PKG from leaking the user's secret key and hence offers a defense mechanism for IBE users against a malicious PKG. All previous works on A-IBE focused on specialized constructions trying to achieve different properties and efficiency enhancements. In this paper for the first time we show how to add accountability to any IBE scheme using oblivious transfer (OT), with almost the same cipher text efficiency as the underlying IBE. Furthermore, we extend our generic construction to support identity reuse without losing efficiency. This property is desirable in practice as users may accidentally lose their secret keys and they -naturally- prefer not to abandon their identities. How to achieve this property was open until our work. Along the way, we first modify the generic construction and develop a new technique to provide public traceability generically.

3. Short Accountable Ring Signatures Based on DDH

Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, Jens Groth and Christophe Petit (University College London, UK)

Abstract: Ring signatures and group signatures are prominent cryptographic primitives offering a combination of privacy and authentication. They enable individual users to anonymously sign messages on behalf of a group of users. In ring signatures, the group, i.e. the ring, is chosen in an ad hoc manner by the signer. In group signatures, group membership is controlled by a group manager. Group signatures additionally enforce accountability by providing the group manager with a secret tracing key that can be used to identify the otherwise anonymous signer when needed. Accountable ring signatures, introduced by Xu and Yung (CARDIS 2004), bridge the gap between the two notions. They provide maximal flexibility in choosing the ring, and at the same time maintain accountability by supporting a designated opener that can identify signers when needed. We revisit accountable ring signatures and offer a formal security model for the primitive. Our model offers strong security definitions incorporating protection against maliciously chosen keys and at the same time flexibility both in the choice of the ring and the opener. We give a generic construction using standard tools. We give a highly efficient instantiation of our generic construction in the random oracle model by meticulously combining Camenisch's group signature scheme (CRYPTO 1997) with a generalization of the one-out-of-many proofs of knowledge by Groth and Kohlweiss (EUROCRYPT 2015). Our instantiation yields signatures of logarithmic size (in the size of the ring) while relying solely on the well-studied decisional Diffie-Hellman assumption. In the process, we offer a number of optimizations for the recent Groth and Kohlweiss one-out-of-many proofs, which may be useful for other applications. Accountable ring signatures imply traditional ring and group signatures. We therefore also obtain highly efficient instantiations of those primitives with signatures shorter than all existing ring signatures as well as existing group signatures relying on standard assumptions.

18.00-22.00 Mayor´s Reception

Meeting point: 18:00 in front of the Conference Venue (after the last session)

A vintage tram will take us to the Mayor's Reception, which will take place at the Heurigenrestaurant „10er Marie". The „10er-Marie"is the oldest wine tavern of Vienna (1740).

10er Marie
Ottakringer Straße 222-224
1160 Vienna
(Metro stop U3 „Ottakring"– directions will be provided, no organized transport for returning)

Thursday, 24th September 2015

09.00-10.00 Keynote Session

Session Chair: Günther Pernul (Universität Regensburg, Germany)

Lecture Hall A

Adversarial and Uncertain Reasoning for Adaptive Cyber Defense: Building the Scientific Foundation

Sushil Jajodia (George Mason University Fairfax, USA)

Abstract: Today's cyber defenses are largely static. They are governed by slow deliberative processes involving testing, security patch deployment, and human-in-the-loop monitoring. As a result, adversaries can systematically probe target networks, pre-plan their attacks, and ultimately persist for long times inside compromised networks and hosts. A new class of technologies, called Adaptive Cyber Defense (ACD), is being developed that presents adversaries with optimally changing attack surfaces and system configurations, forcing adversaries to continually re-assess and re-plan their cyber operations. Although these approaches (e.g., moving target defense, dynamic diversity, and bio-inspired defense) are promising, they assume stationary and stochastic, but non-adversarial, environments. To realize the full potential, we need to build the scientific foundations so that system resiliency and robustness in adversarial settings can be rigorously defined, quantified, measured, and extrapolated in a rigorous and reliable manner.

10.00-10.30 Coffee Break

10.30-12.00 Session 4A: Privacy I

Session Chair: Florian Kerschbaum (SAP SE, Germany)

Lecture Hall C

1. FP-Block: usable web privacy by controlling browser fingerprinting

Christof Torres (University of Luxembourg, Luxembourg), Hugo Jonker (Open University of the Netherlands, Netherlands) and Sjouke Mauw (University of Luxembourg, Luxembourg)

Abstract: Online tracking of users is used for benign goals, such as detecting fraudulent logins, but also to invade user privacy. We posit that for non-oppressed users, tracking within one website does not have a substantial negative impact on privacy, while it enables legitimate benefits. In contrast, cross-domain tracking negatively impacts user privacy, while being of little benefit to the user. Existing methods to counter fingerprint-based tracking treat cross domain tracking and regular tracking the same. This often results in hampering or disabling desired functionality, such as embedded videos. By distinguishing between regular and cross-domain tracking, more desired functionality can be preserved. We have developed a prototype tool, FPBlock, that counters cross-domain fingerprint-based tracking while still allowing regular tracking. FP-Block ensures that any embedded party will see a different, unrelatable fingerprint for each site on which it is embedded. Thus, the user's fingerprint can no longer be tracked across the web, while desired functionality is better preserved compared to existing methods.

2. Mind-Reading: Privacy Attacks Exploiting Cross-App KeyEvent Injections

Wenrui Diao, Xiangyu Liu, Zhe Zhou, Kehuan Zhang (The Chinese University of Hong Kong, China) and Zhou Li (IEEE Member, USA)

Abstract: Input Method Editor (IME) has been widely installed on mobile devices to help user type non-Latin characters and reduce the number of key presses. To improve the user experience, popular IMEs integrate personalized features like reordering suggestion list of words based on user's input history, which inevitably turn them into the vaults of user's secret. In this paper, we make the first attempt to evaluate the security implications of IME personalization and the back-end infrastructure on Android devices. In the end, we identify a critical vulnerability lying under the Android KeyEvent processing framework, which can be exploited to launch cross-app KeyEvent injection (CAKI) attack and bypass the app-isolation mechanism. By abusing such design flaw, an adversary is able to harvest entries from the personalized user dictionary of IME through an ostensibly innocuous app only asking for common permissions. Our evaluation over a broad spectrum of Android OSes, devices, and IMEs suggests such issue should be fixed immediately. All Android versions and most IME apps are vulnerable and private information, like contact names, location, etc., can be easily exfiltrated. Up to hundreds of millions of mobile users are under this threat. To mitigate this security issue, we propose a practical defense mechanism which augments the existing KeyEvent processing framework without forcing any change to IME apps.

3. Enabling Privacy-assured Similarity Retrieval over Millions of Encrypted Records

Xingliang Yuan, Helei Cui, Xinyu Wang and Cong Wang (City University of Hong Kong, China)

Abstract: Searchable symmetric encryption (SSE) has been studied extensively for its full potential in enabling exact-match queries on encrypted records. Yet, situations for similarity queries remain to be fully explored. In this paper, we design privacy-assured similarity search schemes over millions of encrypted high-dimensional records. Our design employs locality-sensitive hashing (LSH) and SSE, where the LSH hash values of records are treated as keywords fed into the framework of SSE. As direct combination of the two does not facilitate a scalable solution for large datasets, we then leverage a set of advanced hash-based algorithms including multiple-choice hashing, open addressing, and cuckoo hashing, and craft a high performance encrypted index from the ground up. It is not only space efficient, but supports secure and sufficiently accurate similarity search with constant time. Our designs are proved to be secure against adaptive adversaries. The experiment on 10 million encrypted records demonstrates that our designs function in a practical manner.

10:30-12:00 Session 4B: Signatures

Session Chair: Kostas Markantonakis (Royal Holloway University, UK)

Lecture Hall D

1. Verifiably Encrypted Signatures: Security Revisited and a New Construction

Christian Hanser (Graz University of Technology, Austria), Max Rabkin and Dominique Schröder (Saarland University, Germany)

Abstract: In structure-preserving signatures on equivalence classes (SPS-EQ-R), introduced at Asiacrypt 2014, each message M in (G ∗)l is associated to its projective equivalence class, and a signature commits to the equivalence class: anybody can transfer the signature to a new, scaled, representative. In this work, we give the first black-box construction of a public-key encryption scheme from any SPS-EQ-R satisfying a simple new property which we call perfect composition. The construction does not involve any non-black-box technique and the implication is that such SPS-EQ-R cannot be constructed from one-way functions in a black-box way. The main idea of our scheme is to build a verifiable encrypted signature (VES) first and then apply the general transformation suggested by Calderon et al. (CT-RSA 2014). The original definition of VES requires that the underlying signature scheme be correct and secure in addition to other security properties. The latter have been extended in subsequent literature, but the former requirements have sometimes been neglected, leaving a hole in the security notion. We show that Calderon et al.'s notion of resolution independence fills this gap.

2. Updatable Hash Proof System and Its Applications

Rupeng Yang, Qiuliang Xu (Shandong University, China), Yongbin Zhou, Rui Zhang (Chinese Academy of Sciences (CAS), China), Chengyu Hu and Zuoxia Yu(Shandong University, China)

Abstract: To tackle with physical attacks to real world cryptosystems, leakage resilient cryptography was developed. In this setting, the adversary is allowed to have access to the internal state of a cryptographic system, thus violates the black-box reduction used in cryptography. Especially when considering continual memory leakage (CML), i.e., there is no predetermined bound on the leakage of the internal information, the task is extremely tough. In this paper, we solve this problem by introducing a new primitive called updatable hash proof system (UHPS). A UHPS can be viewed as a special Hash proof system (HPS), which served as a fundamental tool in constructing public key encryption (PKE) schemes in both leakage-free and leaky settings. A remarkable property of UHPS is that by simply substituting the HPS component with a UHPS component in a PKE scheme, one obtains a new PKE scheme secure in the CML setting. Moreover, the resulting PKE scheme enjoys the same advantage of the original HPS-based PKE, for instance, still "compatible" with known transforms [8,20,24,32]. We then give instantiations of UHPS from widely-accepted assumptions, including the symmetric external Diffie-Hellman assumption and the d-linear assumption. Interestingly, we notice that when instantiated with concrete assumptions, the resulting chosen-cipher text secure PKE scheme is by far the most efficient.

3. Server-Aided Revocable Identity-Based Encryption

Baodong Qin, Robert Deng, Yingjiu Li (Singapore Management University, Singapore) and Shengli Liu (Shanghai Jiao Tong University, China)

Abstract: Efficient user revocation in Identity-Based Encryption (IBE) has been a challenging problem and has been the subject of several research efforts in the literature. Among them, the tree-based revocation approach, due to Boldyreva, Goyal and Kumar, is probably the most efficient one. In this approach, a trusted Key Generation Center (KGC) periodically broadcasts a set of key updates to all (non-revoked) users through public channels, where the size of key updates is only O(r log N r), with N being the number of users and r the number of revoked users, respectively; however, every user needs to keep at least O(logN) longterm secret keys and all non-revoked users are required to communicate with the KGC regularly. These two drawbacks pose challenges to users who have limited resources to store their secret keys or cannot receive key updates in real-time. To alleviate the above problems, we propose a novel system model called server-aided revocable IBE. In our model, almost all of the workloads on users are delegated to an untrusted server which manages users' public keys and key updates

sent by a KGC periodically. The server is untrusted in the sense that it does not possess any secret information. Our system model requires each user to keep just one short secret key and does not require users to communicate with either the KGC or the server during key updating. In addition, the system supports delegation of users' decryption keys, namely it is secure against decryption key exposure attacks. We present a concrete construction of the system that is provably secure against adaptive-ID chosen plaintext attacks under the DBDH assumption in the standard model. One application of our server-aided revocable IBE is encrypted email supporting lightweight devices (e.g., mobile phones) in which an email server plays the role of the untrusted server so that only non-revoked users can read their email messages.

12.00-13.30 Lunch Break

13.30-15.00 Session 5A: Privacy II

Session Chair: Cong Wang (City University of Hong Kong, China)

Lecture Hall C

1. Privacy-Preserving Link Prediction in Decentralized Online Social Networks

Yao Zheng, Bing Wang, Wenjing Lou and Y. Thomas Hou (Virginia Polytechnic Institute and State University, USA)

Abstract: We consider the privacy-preserving link prediction problem in decentralized online social network (OSNs).We formulate the problem as a sparse logistic regression problem and solve it with a novel decentralized two-tier method using alternating direction method of multipliers (ADMM). This method enables end users to collaborate with their online service providers without jeopardizing their data privacy. The method also grants end users fine-grained privacy control to their personal data by supporting arbitrary public/private data split. Using real-world data, we show that our method enjoys various advantages including high prediction accuracy, balanced workload, and limited communication overhead. Additionally, we demonstrate that our method copes well with link reconstruction attack.

2. Privacy-Preserving Observation in Public Spaces

Florian Kerschbaum (SAP, Germany) and Hoon Wei Lim (Singtel R&D Laboratory, Singapore)

Abstract: One method of privacy-preserving accounting or billing in cyber-physical systems, such as electronic toll collection or public transportation ticketing, is to have the user present an encrypted record of transactions and perform the accounting or billing computation securely on them. Honesty of the user is ensured by spot checking the record for some selected surveyed transactions. But how much privacy does that give the user, i.e. how many transactions need to be surveyed? It turns out that due to collusion in mass surveillance all transactions need to be observed, i.e. this method of spot checking provides no privacy at all. In this paper we present a cryptographic solution to the spot checking problem in cyber-physical systems. Users carry an authentication device that authenticates only based on fair random coins. The probability can be set high enough to allow for spot checking, but in all other cases privacy is perfectly preserved. We analyze our protocol for computational efficiency and show that it can be efficiently implemented even on platforms with limited computing resources, such as smart cards and smart phones.

3. Privacy-preserving Context-aware Recommender Systems: Analysis and New Solutions

Qiang Tang and Jun Wang (University of Luxembourg, Luxembourg)

Abstract: Nowadays, recommender systems have become an indispensable part of our daily life and provide personalized services for almost everything. However, nothing is for free – such systems have also upset the society with severe privacy concerns because they accumulate a lot of personal information in order to provide recommendations. In this work, we construct privacy-preserving recommendation protocols by incorporating cryptographic techniques and the inherent data characteristics in recommender systems. We first revisit the protocols by Jeckmans et al. and show a number of security issues. Then, we propose two privacy preserving protocols, which compute predicted ratings for a user based on inputs from both the user's friends and a set of randomly chosen strangers. A user has the flexibility to retrieve either a predicted rating for an unrated item or the Top-N unrated items. The proposed protocols prevent information leakage from both protocol executions and the protocol outputs. Finally, we use the well-known MovieLens 100k dataset to evaluate the performances for different parameter sizes.

13.30-15.00 Session 5B: Applied Security I

Session Chair: Feng Hao (Newcastle University, UK)

Lecture Hall D

1. Web-to-Application Injection Attacks on Android: Characterization and Detection

Behnaz Hassanshahi, Yaoqi Jia, Roland Yap, Prateek Saxena and Zhenkai Liang (National University of Singapore, Singapore)

Abstract: Vulnerable Android applications (or apps) are traditionally exploited via malicious apps. In this paper, we study an underexplored class of Android attacks which do not require the user to install malicious apps, but merely to visit a malicious website in an Android browser. We call them web-to-app injection (or W2AI) attacks, and distinguish between different categories of W2AI side-effects. To estimate their prevalence, we present an automated W2AIScanner to find and confirm W2AI vulnerabilities. We analyze real apps from the official Google Play store and found 286 confirmed vulnerabilities in 134 distinct applications. This findings suggest that these attacks are pervasive and developers do not adequately protect apps against them. Our tool employs a novel combination of static analysis, symbolic execution and dynamic testing. We show experimentally that this design significantly enhances the detection accuracy compared with an existing state-of-the-art analysis.

2. Enhancing Java Runtime Environment for Smart Cards Against Runtime Attacks

Raja Naeem Akram, Konstantinos Markantonakis and Keith Mayes (Royal Holloway, University of London, UK)

Abstract: Smart cards are mostly deployed in security-critical environments in order to provide a secure and trusted access to the provisioned services. These services are delivered to a cardholder using the Service Provider's (SPs) applications on his or her smart card(s). These applications are at their most vulnerable state when they are executing. There exist a variety of runtime attacks that can circumvent the security checks implemented either by the respective application or the runtime environment to protect the smart card platform, user and/or application. In this paper, we discuss the Java Runtime Environment and a potential threat model based on runtime attacks. Subsequently, we discussed the counter-measures that can be deployed to provide a secure and reliable execution platform, along with an evaluation of their effectiveness, incurred performance-penalty and latency.

3. Making Bitcoin Exchanges Transparent

Christian Decker, James Guthrie, Jochen Seidel and Roger Wattenhofer (ETH Zurich, Switzerland)

Abstract: Bitcoin exchanges are a vital component of the Bitcoin ecosystem. They are a gateway from the classical economy to the cryptocurrency economy, facilitating the exchange between fiat currency and bitcoins. However, exchanges are also single points of failure, operating outside the Bitcoin block chain, requiring users to entrust them with their funds in order to operate. In this work we present a solution, and a proof-of-concept implementation, that allows exchanges to prove their solvency, without publishing any information of strategic importance.

15.00-15.30 Coffee Break

15.30-17.00 Session 6A: Cloud Security

Session Chair: Cong Wang (City University of Hong Kong, China)

Lecture Hall C

1. Rich Queries on Encrypted Data: Beyond Exact Matches

Sky Faber, Stanislaw Jarecki, Hugo Krawczyk, Quan Nguyen, Marcel C. Rosu and Michael Steiner (Yorktown, USA)

Abstract: We extend the searchable symmetric encryption (SSE) protocol of [Cash et al., Crypto'13] adding support for range, substring, wildcard, and phrase queries, in addition to the Boolean queries supported in the original protocol. Our techniques apply to the basic single client scenario underlying the common SSE setting as well as to the more complex Multi-Client and Outsourced Symmetric PIR extensions of [Jarecki et al., CCS'13]. We provide performance information based on our prototype implementation, showing the practicality and scalability of our techniques to very large databases, thus extending the performance results of [Cash et al., NDSS'14] to these rich and comprehensive query types.

2. Extended Proxy-Assisted Approach: Achieving Revocable Fine-Grained Cloud Data Encryption

Yanjiang Yang (Institute for Infocomm Research, Singapore), Joseph Liu (Monash University, Australia), Kaitai Liang (Aalto University, Finland), Raymond Choo (University of South Australia, Australia) and Jianying Zhou (Institute for Infocomm Research, Singapore)

Abstract: Attribute-based encryption has the potential to be deployed in a cloud computing environment to provide scalable and fine-grained data sharing. However, user revocation within ABE deployment remains a challenging issue to overcome,

particularly when there is a large number of users. In this work, we introduce an extended proxy-assisted approach, which weakens the trust required of the cloud server. Based on an all-or-nothing principle, our approach is designed to discourage a cloud server from colluding with a third party to hinder the user revocation functionality. We demonstrate the utility of our approach by presenting a construction of the proposed approach, designed to provide efficient cloud data sharing and user revocation. A prototype was then implemented to demonstrate the practicality of our proposed construction.

3. Batch Verifiable Computation of Polynomials on Outsourced Data

Liang Feng Zhang (ShanghaiTech University, China) and Reihaneh Safavi-Naini (University of Calgary, Canada)

Abstract: Secure outsourcing of computation to cloud servers has attracted much attention in recent years. In a typical outsourcing scenario, the client stores its data on a cloud server and later asks the server to perform computations on the stored data. The verifiable computation (VC) of Gennaro, Gentry, Parno (Crypto 2010) and the homomorphic MAC (HomMAC) of Backes, Fiore, Reischuk (CCS 2013) allow the client to verify the server's computation with substantially less computational cost than performing the outsourced computation. The existing VC and HomMAC schemes that can be considered practical (do not required heavy computations such as computing fully homomorphic encryptions), are limited to compute linear and quadratic polynomials on the outsourced data. In this paper, we introduce a batch verifiable computation (BVC) model that can be used when the computation of the same function on multiple datasets is required, and construct two schemes for computing polynomials of high degree on the outsourced data. Our schemes allow efficient client verification, efficient server computation, and composition of computation results. Both schemes allow new elements to be added to each outsourced dataset. The second scheme also allows new datasets to be added. A unique feature of our schemes is that the storage required at the server for storing the authentication information, stays the same as the number of outsourced datasets is increased, and so the server storage overhead (the ratio of the server storage to the total size of the datasets) approaches 1. In all existing schemes this ratio is ≥ 2. Hence, our BVC can effectively halve the required server storage.

4. CloudBI: Practical Privacy-Preserving Outsourcing of Biometric Identification in the Cloud

Qian Wang, Shengshan Hu (Wuhan University, China), Kui Ren (University at Buffalo, USA), Meiqi He, Minxin Du and Zhibo Wang (Wuhan University, China)

Abstract: Biometric identification has been incredibly useful in the law enforcement to authenticate an individual's identity and/or to figure out who someone is, typically by scanning a database of records for a close enough match. In this work, we investigate the privacy-preserving biometric identification outsourcing problem, where the database owner outsources both the large-scale encrypted database and the computationally intensive identification job to the semi-honest cloud, relieving itself from data storage and computation burden. We present new privacy preserving biometric identification protocols, which substantially reduce the computation burden on the database owner. Our protocols build on new biometric data encryption, distance-computation and matching algorithms that novelly exploit inherent structures of biometric data and properties of identification operations. A thorough security analysis shows that our solutions are practically-secure, and the ultimate solution offers a higher level of privacy protection than the-state-of-the-art on biometric identification outsourcing. We evaluate our protocols by implementing an efficient privacy-preserving fingerprint-identification system, showing that our protocols meet both the security and efficiency needs well, and they are appropriate for use in various privacy-preserving biometric identification applications.

15.30-17.00 Session 6B: Protocols & Attribute-based encryption

Session Chair: Peter Y A Ryan (University of Luxembourg, Luxembourg)

Lecture Hall D

1. Typing and Compositionality for Security Protocols: A Generalization to the Geometric Fragment

Omar Almousa, Sebastian A. Mödersheim (DTU Compute, Denmark), Paolo Modesti (Newcastle University, UK) and Luca Viganò (King's College London, UK)

Abstract: We integrate, and improve upon, prior relative soundness results of two kinds. The first kind are typing results showing that any security protocol that fulfils a number of sufficient conditions has an attack if it has a well-typed attack. The second kind considers the parallel composition of protocols, showing that when running two protocols in parallel allows for an attack, then at least one of the protocols has an attack in isolation. The most important generalization over previous work is the support for all security properties of the geometric fragment.

2. Checking trace equivalence: How to get rid of nonces?

Rémy Chrétien, Veronique Cortier (LORIA, INRIA Nancy - Grand-Est, France) and Stephanie Delaune (LSV, ENS Cachan & CNRS, France)

Abstract: Security protocols can be successfully analyzed using formal methods. When proving security in symbolic settings for an unbounded number of sessions, a typical technique consists in abstracting away fresh nonces and keys by a bounded set of

constants. While this abstraction is clearly sound in the context of secrecy properties (for protocols without else branches), this is no longer the case for equivalence properties. In this paper, we study how to soundly get rid of nonces in the context of equivalence properties. We show that nonces can be replaced by constants provided that each nonce is associated to two constants (instead of typically one constant for secrecy properties). Our result holds for deterministic (simple) protocols and a large class of primitives that includes e.g. standard primitives, blind signatures, and zero-knowledge proofs.

3. Attribute Based Broadcast Encryption with Short Ciphertext and Decryption Key

Tran Viet Xuan Phuong, Guomin Yang (University of Wollongong, Australia) and Willy Susilo (Xidian University, China)

Abstract: Attribute Based Broadcast Encryption (ABBE) is a combination of Attribute Based Encryption (ABE) and Broadcast Encryption (BE). It allows a broadcaster (or encrypter) to broadcast an encrypted message that can only be decrypted by the receivers who are within a predefined user set and satisfy the access policy specified by the broadcaster. Compared with normal ABE, ABBE allows direct revocation, which is important in many real-time broadcasting applications such as Pay TV. In this paper, we propose two novel ABBE schemes that have distinguishing features: the first scheme is key-policy based and has short ciphertext and constant size decryption key; and the second one is ciphertext-policy based and has constant size ciphertext and short decryption key. Both of our schemes allow access policies to be expressed using AND-gate with positive, negative, and wildcard symbols, and are proven secure under the Decision n-BDHE assumption without random oracles.

4. Accountable Authority Ciphertext-Policy Attribute-Based Encryption with White-Box Traceability and Public Auditing in the Cloud

Jianting Ning (Shanghai Jiao Tong University, China), Xiaolei Dong, Zhenfu Cao (East China Normal University, China) and Lifei Wei (Shanghai Ocean University, China)

Abstract: As a sophisticated mechanism for secure fine-grained access control, ciphertext-policy attribute-based encryption (CP-ABE) is a highly promising solution for commercial applications such as cloud computing. However, there still exists one major issue awaiting to be solved, that is, the prevention of key abuse. Most of the existing CP-ABE systems missed this critical functionality, hindering the wide utilization and commercial application of CP-ABE systems to date. In this paper, we address two practical problems about the key abuse of CP-ABE: (1) The key escrow problem of the semi-trusted authority; and, (2) The malicious key delegation problem of the users. For the semi-trusted authority, its misbehavior (i.e., illegal key (re-)distribution) should be caught and prosecuted. And for a user, his/her malicious behavior (i.e., illegal key sharing) need be traced. We affirmatively solve these two key abuse problems by proposing the first accountable authority CP-ABE with whitebox traceability that supports policies expressed in any monotone access structures. Moreover, we provide an auditor to judge publicly whether a suspected user is guilty or is framed by the authority.

17.00-23.00 Conference Dinner

Meeting point: 17:00 in front of the Conference Venue (after the last session)

A bus will take us to **Schönbrunn Palace**, Empress Sisi's former summer residence. The palace is part of UNESCO's cultural heritage due to its historic importance, its unique grounds and its splendid furnishings. At Schönbrunn Palace we have organized a Grand Tour, which will give you a picture of the different stylistic eras of the imperial monarchy and the life's of the palace´s inhabitants.

After the tour little trains will take us to the Conference Dinner location, the **Orang.erie**, which is located in the „Vienna Zoo". Founded as an imperial menagerie in 1752, it is the oldest zoo in the world. The Vienna Zoo is located on the grounds of the Schönbrunn Palace, on our way from the Palace to the Dinner location you will see parts of it.

Address:
Orang.erie
Maxerstraße 13
1130 Vienna
(Metro stop U4 „Hietzing" – directions will be provided, no organized transport for returning)

Friday, 25th September 2015

08.00-17.00 Registration

09.00-10.30 Session 7A: Code Analysis & Side-Channels

Session Chair: Günther Pernul (Universität Regensburg, Germany)

Lecture Hall C

1. DexHunter: Toward Extracting Hidden Code from Packed Android Applications

Yueqian Zhang, Xiapu Luo and Haoyang Yin (The Hong Kong Polytechnic University, China)

Abstract: The rapid growth of mobile application (or simply app) economy provides lucrative and profitable targets for hackers. Among OWASP's top ten mobile risks for 2014, the lack of binary protections makes it easy to reverse, modify, and repackage Android apps. Recently, a number of packing services have been proposed to protect Android apps by hiding the original executable file (i.e., dex file). However, little is known about their effectiveness and efficiency. In this paper, we perform the first systematic investigation on such services by answering two questions: (1) what are the major techniques used by these services and their effects on apps? (2) can the original dex file in a packed app be recovered? If yes, how? We not only reveal their techniques and evaluate their effects, but also propose and develop a novel system, named Dex- Hunter, to extract dex files protected by these services. It is worth noting that DexHunter supports both the Dalvik virtual machine (DVM) and the new Android Runtime (ART). The experimental results show that DexHunter can extract dex files from packed apps effectively and efficiently.

2. Identifying Arbitrary Memory Access Vulnerabilities in Privilege-Separated Software

Hong Hu, Zheng Leong Chua, Zhenkai Liang and Prateek Saxena (National University of Singapore, Singapore)

Abstract: Privilege separation is a widely used technique to secure complex software systems. With privilege separation, software components are divided into several partitions and these partitions can only communicate through limited interfaces. However, the interfaces still provide a channel for one partition to influence code in other partitions. As a result, certain memory access patterns can be leveraged by attackers to perform arbitrary memory access. We refer to this type of memory access errors by the acronym DUI (Dereference Under the Influence). In this paper, we present a systematic method to detect vulnerabilities leading to DUI through binary analysis, and to estimate the capability attackers can obtain through DUI exploits. The evaluation shows that our approach can accurately identify vulnerable code that leads to arbitrary memory access in real-world software components and programs, when they are transformed to privilege-separated designs.

3. vBox: Proactively Establishing Secure Channels between Wireless Devices without Prior Knowledge

Wei Wang, Jingqiang Lin, Zhan Wang, Ze Wang and Luning Xia (Chinese Academy of Sciences, China)

Abstract: Establishing secure channels between two wireless devices without any prior knowledge is challenging, especially when such devices only have very simple user interface. Most existing authentication and key negotiation solutions leverage the received signal strength (RSS) of wireless signals, and the security guarantees depend on the environments too much; in a static environment of less motion, the adversaries could control or predict the RSS of legitimate devices. We propose vBox in this paper, a proactive method to establish secure channels between wireless devices, without the assumption on environments. By holding and waving two devices to communicate, the owner creates a virtual "shield box". The adversaries outside the box cannot send signals with stable RSS into the box, so the legitimate devices can easily be authenticated based on the variation of RSS. At the same time, the adversaries cannot correctly measure or detect the RSS of wireless signals transmitted between the in-box devices, and then they can directly transmit secret keys in plaintext. Then, after the simple operation by the owner for a few seconds, the authenticated nodes will securely communicate using the shared secret key. We implement the vBox prototype on commercial off- the-shelf ZigBee devices, and evaluate it with extensive experiments under the normal case and several attack scenarios. The experiment results and security analysis show that, vBox establishes secure channels handily against various attacks and is suitable for different environments.

09.00-10.30 Session 7B: Crypto Applications & Attacks

Session Chair: Haya Shulman (Fraunhofer SIT, Germany)

Lecture Hall D

1. Challenging the Trustworthyness of PGP: Is the Web-of-Trust Tear-proof?

Alessandro Barenghi, Alessandro Di Federico, Gerardo Pelosi and Stefano Sanfilippo (Politecnico di Milano, Italy)

Abstract: The OpenPGP protocol provides a long time adopted and widespread tool for secure and authenticated asynchronous communications, as well as supplies data integrity and authenticity validation for software distribution. In this work, we analyze

the Web-of-Trust on which the OpenPGP public key authentication mechanism is based, and evaluate a threat model where its functionality can be jeopardized. Since the threat model is based on the viability of compromising an OpenPGP keypair, we performed an analysis of the state of health of the global OpenPGP key repository. Despite the detected amount of weak keypairs is rather low, our results show how, under reasonable assumptions, approximately 70% of the Web-of-Trust strong set is potentially affected by the described threat. Finally, we propose viable mitigation strategies to cope with the highlighted threat.

2. Transforming Out Timing Leaks, More or Less

Heiko Mantel and Artem Starostin (TU Darmstadt, Germany)

Abstract: We experimentally evaluate program transformations for removing timing side-channel vulnerabilities wrt. security and overhead. Our study of four well-known transformations confirms that their performance overhead differs substantially. A novelty of our work is the empirical investigation of channel bandwidths, which clarifies that the transformations also differ wrt. how much security they add to a program. Interestingly, we observe such differences even between transformations that have been proven to establish timing-sensitive noninterference. Beyond clarification, our findings provide guidance for choosing a suitable transformation for removing timing side-channel vulnerabilities. Such guidance is needed because there is a trade-off between security and overhead, which makes choosing a suitable transformation non-trivial.

3. Small Tweaks do Not Help: Differential Power Analysis of MILENAGE Implementations in 3G/4G USIM Cards

Junrong Liu, Yu (Shanghai Jiao Tong University, China), Francois-Xavier Standaert (Universit´e catholique de Louvain, Belgium), Zheng Guo, Dawu Gu, Wei Sun, Yijie Ge, Rong Fu (Shanghai Jiao Tong University, China), and Xinjun Xie (Shanghai Modern General Recognition Technology Corporation, China)

Abstract: Side-channel attacks are an increasingly important concern for the security of cryptographic embedded devices, such as the SIM cards used in mobile phones. Previous works have exhibited such attacks against implementations of the 2G GSM algorithms (COMP-128, A5). In this paper, we show that they remain an important issue for USIM cards implementing the AES-based MILENAGE algorithm used in 3G/4G communications. In particular, we analyze instances of cards from a variety of operators and manufacturers, and describe successful Differential Power Analysis attacks that recover encryption keys and other secrets (needed to clone the USIM cards) within a few minutes. Further, we discuss the impact of the operator-defined secret parameters in MILENAGE on the difficulty to perform Differential Power Analysis, and show that they do not improve implementation security. Our results back up the observation that physical security issues raise long-term challenges that should be solved early in the development of cryptographic implementations, with adequate countermeasures.

09:00-10:30 PhD Symposium – Session 1

Session Chair: Rolf Schillinger (Universität Regensburg, Germany)

Lecture Hall E

1. Improvement of Network Intrusion Detection Using Various Obfuscation Techniques

Ivan Homoliak (Brno University of Technology, Czech Republic)

Abstract: The main goal of my PhD research is to improve detection capabilities of academical NIDS called Automated Intrusion Prevention System (AIPS) whose detection engine was substantially designed in my master's thesis as part of related project. The AIPS system was designed to perform statistical and behavioral analysis of connection-oriented network traffic ows in order to detect zero-day attacks and divergent types of network attacks. The principal technique which is being used to improve performance of AIPS takes into account the idea of bypassing detection capability of the system and consequently provides better expert knowledge containing obfuscated communications, especially malicious. Because of AIPS is based upon behavioral and statistical analysis, which often use time and index slope of connections or analysis of payload distribution, there can arise a question of breaching detection of AIPS. The most of AIPS detection features called Advanced Security Network Metrics (ASNM) use information gathered from L3 and L4 packets headers. There are suggested to use various non-payload based obfuscation techniques to examine detection properties of ASNM features. Examples of the obfuscations include: tunneling in other application layer protocol; spreading out packets in time; segmentation & fragmentation; changing of packets` order; simulation of unreliable network channel; packets' loss; packets` duplication etc. Combinations of these techniques are suggested to use as well.

2. Semantic technologies applied to digital forensics analysis and evidence modelling

Rodrigo Carvalho (Brazilian Federal Police, Brazil)

Abstract: Cybercrime tackling is a major challenge for Law Enforcement Agencies (LEAs). Traditional digital forensics and investigation procedures are not coping with the sheer amount of data to analyze, which is stored in multiple devices seized from distinct, possibly-related cases. Moreover, inefficient information representation and exchange hampers evidence recovery and relationship discovery. Aiming at a better balance between human reasoning skills and computer processing

capabilities, our project will research about how semantic technologies could make digital forensics more efficient. It will take the example of online banking fraud to propose an ontology aimed at mapping criminal organizations and identifying malware developers. Although still in early stage of development, it reviews concepts to extend from well-established ontologies and proposes novel abstractions that could enhance relationship discovery. Finally, it suggests inference rules based on empirical knowledge which could better address the needs of the human analyst.

3. Technology Analysis of IDS and NBA systems from the view of detection effectivity

Dominik Breitenbacher (BUT, Czech Republic)

Abstract: My research will be focused on the network security, closely on the IDS (intrusion detection system) and NBA (network behavior analysis) systems effectiveness and ability to react on various kinds of attacks. At the beginning of my work I would like to make a dataset of known vulnerable applications with their exploits and references to vulnerabilities. The motivation of this step is the fact, that in common it is very difficult to obtain vulnerable applications which could be used for exploitation analysis. The reason why almost all vendors do not keep vulnerable SW available is straightforward. The dataset will be large and representative enough to provide reliable results when used in research. Then, the testing framework will be proposed which will serve for building of VMs with prepared OS and feasible conditions for attacks execution. Using the testing framework I would like to analyze various NIDS (network intrusion detection system), HIDS (host intrusion detection system), NBA, anti-virus systems, report evaluated results and propose how to solve issues that were found. Collected features of various intrusion detection systems will be collected as well and if they will be available. Testing framework with gathered dataset will be available for interested academic or non-academic communities and it would be used in penetration testing, vulnerability analysis and data mining.

10.30-11.00 Coffee Break

11.00-12.30 Session 8A: Authentication I

Session Chair: Kui Ren (SUNY Buffalo, USA)

Lecture Hall C

1. On Security of Content-based Video Stream Authentication

Swee-Won Lo, Zhuo Wei, Robert Deng and Xuhua Ding (Singapore Management University, Singapore)

Abstract: Content-based authentication (CBA) schemes are used to authenticate multimedia streams while allowing content-preserving manipulations such as bit-rate transcoding. In this paper, we survey and classify existing transform-domain CBA schemes for videos into two categories, and point out that in contrary to CBA for images, there exists a common design flaw in these schemes. We present the principles (based on video coding concept) on how the flaw can be exploited to mount semantic-changing attacks in the transform domain that cannot be detected by existing CBA schemes. We show attack examples including content removal, modification and insertion attacks. Noting that these CBA schemes are designed at the macroblock level, we discuss, from the attacker's point of view, the conditions in attacking content based authenticated macroblocks.

2. Oblivious Maximum Bipartite Matching Size Algorithm with Applications to Secure Fingerprint Identification

Marina Blanton and Siddharth Saraph (University of Notre Dame, USA)

Abstract: The increasing availability and use of biometric data leads to situations when sensitive biometric data is to be handled by entities who may not be fully trusted or otherwise are not authorized to have full access to such data. This calls for mechanisms of provably protecting biometric data while still allowing the computation to take place. Our focus is on privacy-preserving matching of two fingerprints (authentication or identification purposes) using traditional minutia-based representation of fingerprints that leads to the most discriminative fingerprint comparisons. Unlike previous work in the security literature, we would like to focus on algorithms that are guaranteed to find the maximum number of minutiae that can be paired together between two fingerprints leading to more accurate comparisons. To address this problem, we formulate it as a flow network problem and reduce it to finding maximum matching size in bipartite graphs. The resulting problem is in turn reduced to computing the rank of a (non-invertible) matrix, formed as a randomized adjacency matrix of the bipartite graph. We then provide data-oblivious algorithms for matrix rank computation and consecutively finding maximum matching size in a bipartite graph and also extend the algorithms to solve the problem of accurate fingerprint matching. These algorithms lead to their secure counterparts using standard secure two-party or multi-party techniques. Lastly, we implement secure fingerprint matching in the secure two-party computation setting using garbled circuit evaluation. Our experimental results demonstrate that the techniques are efficient, leading to performance similar to that of other fastest secure fingerprint matching techniques, despite higher complexity of our solution that higher accuracy demands.

3. Practical Threshold Password-Authenticated Secret Sharing Protocol

Xun Yi (RMIT University, Australia), Feng Hao (Newcastle University, UK), Liqun Chen (Hewlett-Packard Laboratories, UK)and Joseph Liu (Monash University, Australia)

Abstract: Threshold password-authenticated secret sharing (TPASS) protocols allow a client to secret-share a secret s among n servers and protect it with a password pw, so that the client can later recover s from any subset of t of the servers using the password pw, but so that no coalition smaller than t learns anything about s or can mount an offline dictionary attack on the password pw. Some TPASS protocols have appeared in the literature recently. The protocol by Bagherzandi et al. (CCS 2011) leaks the password if a client mistakenly executes the protocol with malicious servers. The first t-out-of-n TPASS protocol for any n > t that does not suffer from this shortcoming was given by Camenisch et al. (CRYPTO 2014). This protocol, proved to be secure in the UC framework, requires the client to involve in many communication rounds so that it becomes impractical for the client. In this paper, we present a practical TPASS protocol which is in particular efficient for the client, who only needs to send a request and receive a response. In addition, we have provided a rigorous proof of security for our protocol in the standard model.

11.00-12.30 Session 8B: Policies

Session Chair: Frederic Cuppens (Telecom Bretagne, France)

Lecture Hall D

1. A Theory of Gray Security Policies

Donald Ray and Jay Ligatti (University of South Florida, Tampa, USA)

Abstract: This paper generalizes traditional models of security policies, from specifications of whether programs are secure, to specifications of how secure programs are. This is a generalization from qualitative, black-and-white policies to quantitative, gray policies. Included are generalizations from traditional definitions of safety and liveness policies to definitions of gray-safety and gray-liveness policies. These generalizations preserve key properties of safety and liveness, including that the intersection of safety and liveness is a unique allow-all policy and that every policy can be written as the conjunction of a single safety and a single liveness policy. It is argued that the generalization provides several benefits, including that it serves as a unifying framework for disparate approaches to security metrics, and that it separates—in a practically useful way—specifications of how secure systems are from specifications of how secure users require their systems to be.

2. Factorization of Behavioral Integrity

Ximeng Li, Flemming Nielson and Hanne Riis Nielson (Technical University of Denmark, Denmark)

Abstract: We develop a bisimulation-based noninterference property that describes the allowed dependencies between communication behaviors of different integrity levels. The property is able to capture all possible combinations of integrity levels for the “presence” and “content” of actual communications. Channels of low presence integrity and high content integrity can be used to model the effect of Message Authentication Codes or the consequence of Denial of Service Attacks. In case the distinction between “presence” and “content” is deliberately blurred, the noninterference property specializes to a classical process-algebraic property (called SBNDC). A compositionality result is given to facilitate a structural approach to the analysis of concurrent systems.

3. Checking Interaction-Based Declassification Policies for Android Using Symbolic Execution

Kristopher Micinski, Jonathan Fetter-Degges, Jinseong Jeon, Jeffrey Foster (University of Maryland, USA) and Michael Clarkson (Cornell University, USA)

Abstract: Mobile apps can access a wide variety of secure information, such as contacts and location. However, current mobile platforms include only coarse access control mechanisms to protect such data. In this paper, we introduce interaction-based declassification policies, in which the user’s interactions with the app constrain the release of sensitive information. Our policies are defined extensionally, so as to be independent of the app’s implementation, based on sequences of security-relevant events that occur in app runs. Policies use LTL formulae to precisely specify which secret inputs, read at which times, may be released. We formalize a semantic security condition, interaction-based noninterference, to define our policies precisely. Finally, we describe a prototype tool that uses symbolic execution of Dalvik bytecode to check interaction-based declassification policies for Android, and we show that it enforces policies correctly on a set of apps.

11.00-12.30 PhD Symposium – Session 2

Session Chair: Edgar Weippl (SBA Research, Austria)

Lecture Hall E

1. Cryptogenography

Sune K. Jakobsen (Queen Mary, University of London, UK)

Abstract: It is possible to reveal information anonymously if no one will actively help you to do so? In a world where politicians are considering banning back-door-free encryption, this is becoming an important question. I have shown that it is impossible in some standard interpretations of the question, but if we weaken some assumptions is becomes possible. For example, if the sender has access to a small anonymous channel, we have shown that this can be used to bootstrap a large anonymous channel. In another result I have shown that many people can collaborate to send a small amount of information in such a way that even an adversary with unbounded computational power will always have reasonable doubt about whether any particular person was sending information.

2. Detecting and Preventing Abuse of Resources in IaaS Cloud Computing

Jens Lindemann (University of Hamburg, Germany)

Abstract: Cloud computing is being used by more and more organizations. However, cloud services can also be abused either by malicious users or hackers. If abuse of cloud services affects third parties, bad publicity or even legal problems may ensue for a cloud service provider. Abuse of cloud services is considered to be one of the nine top threats to cloud computing by the Cloud Security Alliance. While there has been research on detecting and preventing attacks on cloud resources, detecting abuse of cloud resources for malicious activities has seen only limited research and even commercial cloud offerings currently lack sufficient abuse protection. The research will assess what security measures currently exist against abuse of cloud computing resources. It will further conceive concepts for abuse detection and prevention, which will be implemented and evaluated. The results will not only be useful to better quantify the risk stemming from the abuse of cloud services, but they will also provide insights regarding the potential and the limitations of cloud abuse detection and prevention techniques in practice.

3. Why the Bitcoin Community needs to pursue Bitcoin-based Authentication

Patrick McCorry (Newcastle University, UK)

Abstract: This presentation focuses on two pieces of research; 1) we initiate the first study on the post-payment scenario for Bitcoin payments and propose two concentrate post-payment protocols that allows a merchant to re-authenticate a previous pseudonymous customer and establish a secure end-to-end communication channel using their shared transaction history stored on Bitcoin's Blockchain and 2) we highlight new attacks on the community accepted BIP70: Payment Protocol standard that governs how a merchant and customer perform payments in Bitcoin. This protocol is supported by most major wallets and the two dominant Payment Processors Coinbase and BitPay who provide the infrastructure for accepting Bitcoin as a form of payment to 88,000+ merchants.

12.30-14.00 Lunch

14.00-15.30 Session 9A: Authentication II

Session Chair: Artemios Voyiatzis (SBA Research, Austria)

Lecture Hall D

1. Towards Attack-Resistant Peer-Assisted Indoor Localization

Jingyu Hua, Shaoyong Du and Sheng Zhong (Nanjing University, China)

Abstract: Peer-assisted smartphone localization, which leverages pairwise acoustic ranging among nearby peer phones to refine location estimation, significantly pushes the accuracy limit of WiFi-based indoor localization. Unfortunately, this technique is designed for non-adversarial settings. Dishonest peers may cheat in their distance measurements. Outside attackers may interfere with the acoustic ranging by continually broadcasting interference signals. In this paper, we propose countermeasures against each of these attacks. We first present an algorithm that can identify peers that are not cheating in the current localization, by searching for devices that can be embedded into the same plane according to their pairwise distances. We also design a robust acoustic ranging method exploiting signal modulation, which can defend effectively against intentional interference of outside attackers. Experimental results demonstrate that our countermeasures can greatly improve the obustness of peer-assisted localization.

2. Leveraging Real-Life Facts to Make Random Passwords More Memorable

Mahdi Nasrullah Al-Ameen, Kanis Fatema, Matthew Wright and Shannon Scielzo (The University of Texas at Arlington, USA)

Abstract: User-chosen passwords fail to provide adequate security. System-assigned random passwords are more secure but suffer from memorability problems. We argue that the system should remove this burden from users by assisting with the memorization of randomly assigned passwords. To meet this need, we aim to apply the scientific understanding of long-term memory. In particular, we examine the efficacy of augmenting a system-assigned password scheme based on textual recognition by providing users with verbal cues—real-life facts corresponding to the assigned keywords. In addition, we explore

the usability gain of including images related to the keywords along with the verbal cues. We conducted a multi-session in-lab user study with 52 participants, where each participant was assigned three different passwords, each representing one study condition. Our results show that the textual recognition-based scheme offering verbal cues had a significantly higher login success rate (94%) as compared to the control condition, i.e., textual recognition without verbal cues (61%). The comparison between textual and graphical recognition reveals that when users were provided with verbal cues, adding images did not significantly improve the login success rate, but it did lead to faster recognition of the assigned keywords. We believe that our findings make an important contribution to understanding the extent to which different types of cues impact the usability of system-assigned passwords.

3. The Emperor's New Password Creation Policies

Ding Wang and Ping Wang (National Engineering Research Center for Software Engineering, China)

Abstract: While much has changed in Internet security over the past decades, textual passwords remain as the dominant method to secure user web accounts and they are proliferating in nearly every new web services. Nearly every web services, no matter new or aged, now enforce some form of password creation policy. In this work, we conduct an extensive empirical study of 50 password creation policies that are currently imposed on high-profile web services, including 20 policies mainly from US and 30 ones from mainland China. We observe that no two sites enforce the same password creation policy, there is little rationale under their choices of policies when changing policies, and Chinese sites generally enforce more lenient policies than their English counterparts. We proceed to investigate the effectiveness of these 50 policies in resisting against the primary threat to password accounts (i.e. online guessing) by testing each policy against two types of weak passwords which represent two types of online guessing. Our results show that among the total 800 test instances, 541 ones are accepted: 218 ones come from trawling online guessing attempts and 323 ones come from targeted online guessing attempts. This implies that, currently, the policies enforced in leading sites largely fail to serve their purposes, especially vulnerable to targeted online guessing attacks.

14.00-15.30 Session 9B: Detection & Monitoring

Session Chair: Stefan Brunthaler (SBA Research, Austria)

Lecture Hall C

1. Thing. Accurate Specification for Robust Detection of Malicious Behavior in Mobile Environments

Sufatrio, Tong-Wei Chua, Darell J. J. Tan and Vrizlynn L. L. (Institute for Infocomm Research, Singapore)

Abstract: The need to accurately specify and detect malicious behavior is widely known. This paper presents a novel and convenient way of accurately specifying malicious behavior in mobile environments by taking Android as a representative platform of analysis and implementation. Our specification takes a sequence-based approach in declaratively formulating a malicious action, whereby any two consecutive security sensitive operations are connected by either a control or taint flow. It also captures the invocation context of an operation within an app's component type and lifecycle/callback method. Additionally, exclusion of operations that are invoked from UI-related callback methods can be specified to indicate an action's stealthy execution portions. We show how the specification is sufficiently expressive to describe malicious patterns that are commonly exhibited by mobile malware. To show the usefulness of the specification, and to demonstrate that it can derive stable and distinctive patterns of existing Android malware, we develop a static analyzer that can automatically check an app for numerous security sensitive actions written using the specification. Given a target app's uncovered behavior, the analyzer associates it with a collection of known malware families. Experiments show that our obfuscation-resistant analyzer can associate malware samples with their correct family with an accuracy of 97.2%, while retaining the ability to differentiate benign apps from the profiled malware families with an accuracy of 97.6%. These results positively show how the specification can lend to robust mobile malware detection.

2. A Bytecode Interpreter for Secure Program Execution in Untrusted Main Memory

Maximilian Seitzer, Michael Gruhn and Tilo Müller (Friedrich-Alexander University Erlangen-N¨urnberg, Germany)

Abstract: Physical access to a system allows attackers to read out RAM through cold boot and DMA attacks. Thus far, counter measures protect only against attacks targeting disk encryption keys, while the remaining memory content is left vulnerable. We present a bytecode interpreter that protects code and data of programs against memory attacks by executing them without using RAM for sensitive content. Any program content within memory is encrypted, for which the interpreter utilizes TRESOR [1], a cold boot resistant implementation of the AES cipher. The interpreter was developed as a Linux kernel module, taking advantage of the CPU instruction sets AVX for additional registers, and AESNI for fast encryption. We show that the interpreter is secure against memory attacks, and that the overall performance is only a factor of 4 times slower than the performance of Python. Moreover, the performance penalty is mostly induced by the encryption.

3. Learning from Others: User Anomaly Detection Using Anomalous Samples from Other Users

Youngja Park, Ian Molloy, Suresh Chari (IBM T.J. Watson Research Center, USA), Zenglin Xu, Chris Gates and Ninghui Li (Purdue University, USA)

Abstract: Machine learning is increasingly used as a key technique in solving many security problems such as botnet detection, transactional fraud, insider threat, etc. One of the key challenges to the widespread application of ML in security is the lack of labeled samples from real applications. For known or common attacks, labeled samples are available, and, therefore, supervised techniques such as multi-class classification can be used. However, in many security applications, it is difficult to obtain labeled samples as each attack can be unique. In order to detect novel, unseen attacks, researchers used unsupervised outlier detection or one-class classification approaches, where they treat existing samples as benign samples. These methods, however, yield high false positive rates, preventing their adoption in real applications. This paper presents a local outlier factor (LOF)-based method to automatically generate both benign and malicious training samples from unlabeled data. Our method is designed for applications with multiple users such as insider threat, fraud detection, and social network analysis. For each target user, we compute LOF scores of all samples with respect to the target user's samples. This allows us to identify (1) other users' samples that lie in the boundary regions and (2) outliers from the target user's samples that can distort the decision boundary. We use the samples from other users as malicious samples, and use the target user's samples as benign samples after removing the outliers. We validate the effectiveness of our method using several datasets including access logs for valuable corporate resources, DBLP paper titles, and behavioral biometrics of user typing behavior. The evaluation of our method on these datasets confirms that, in almost all cases, our technique performs significantly better than both one-class classification methods and prior two-class classification methods. Further, our method is a general technique that can be used for many security applications.

14.00-15.30 PhD Symposium – Session 3

Session Chair: Edgar Weippl (SBA Research, Austria)

Lecture Hall E

1. A Coinductive System Calculus for Security Properties

Eric Rothstein Morris (University of Passau, Germany)

Abstract: We tackle the security property satisfaction problem by studying security properties defined as behavioral differential equations (BDEs) in a coinductive calculus of systems. This approach addresses a variety of systems (including non-deterministic, probabilistic and non-terminating systems) in one unified framework. If a security property is defined as a BDE and such BDE is solvable, we can soundly and transparently transform a system into its secure version; effectively satisfying the security property. Security properties belong to three different abstraction layers: state, execution and system. System properties imply execution properties, which in turn imply state properties. We are interested in classifying system properties according to their BDE format and abstraction layer, but our main interest is to find BDEs that define and combine security properties. We want to provide tool support in the form of a Haskell-based unified framework where systems and security properties can be naturally expressed and reasoned about.

2. Data Quality Management in Information Systems Security Documentation

Christian Sillaber (University of Innsbruck, Austria)

Abstract: Businesses are increasingly required to document, implement, improve and monitor IS security requirements derived from different sources to ensure proper implementation of controls, overall compliance and to support managerial decision making. However, the documentation of IS security is fraught with a variety of challenges, including missing tool support, low stakeholder awareness, different levels of formalization that lead to hardly maintainable documentation entities stored in different ISMS and GRC tools and productivity platforms. The goal of this PhD thesis is to create a data quality model and associated processes to help organizations overcome these challenges and to provide them with tool support that ensures a high level of data quality in the documentation of IS security at various organizational levels. We are the first to address these quality issues in a systematic way and to build a data quality model and tool support in empirically grounded research. First research results were already transferred to industry and empirically validated.

3. Formal specifica6on and verificaton of Security guidelines, Derivation of Security properes using static code analysis.

Zhioua Zeineb (SAP Labs France, EURECOM, Telecom ParisTech, France)

Abstract: The development and delivery of secure software is a challenging task that gets even harder when the developer tries to adhere to both application and organization--specific security requirements translated into security guidelines. These guidelines serve as best practices or recommendations that help reduce application exposure to vulnerabilities, and have concrete guarantees about the application adherence to high level and abstract security requirements. Our approach aims at integrating the formal specification and verification of security guidelines not only in early stages of the development phase but throughout the software lifecycle. This would help the developer to ensure the compliance with security specifications

throughout the software development lifecycle. This same approach would also help the Marketplace operator in verifying the compliance of third--party applications with its security requirements and making decisions regarding the approval or the rejection of the submitted applications before they find their way to the end--users devices.

15:30-15:45 Coffee Break

15.45-17.15 Session 10: Applied Security II

Session Chair: Edgar Weippl (SBA Research, Austria)

Lecture Hall C

1. All Your Voices Are Belong to Us: Stealing Voices to Fool Humans and Machines

Dibya Mukhopadhyay, Maliheh Shirvanian and Nitesh Saxena (University of Alabama at Birmingham, USA)

Abstract: In this paper, we study voice impersonation attacks to defeat humans and machines. Equipped with the current advancement in automated speech synthesis, our attacker can build a very close model of a victim's voice after learning only a very limited number of samples in the victim's voice (e.g., mined through the Internet, or recorded via physical proximity). Specifically, the attacker uses voice morphing techniques to transform its voice – speaking any arbitrary message – into the victim's voice. We examine the aftermaths of such a voice impersonation capability against two important applications and contexts: (1) impersonating the victim in a voice-based user authentication system, and (2) mimicking the victim in arbitrary speech contexts (e.g., posting fake samples on the Internet or leaving fake voice messages). We develop our voice impersonation attacks using an off-the-shelf voice morphing tool, and evaluate their feasibility against state-of-the-art automated speaker verification algorithms (application 1) as well as human verification (application 2). Our results show that the automated systems are largely ineffective to our attacks. The average rates for rejecting ake voices were under 10–20% for most victims. Even human verification is vulnerable to our attacks. Based on two online studies with about 100 users, we found that only about an average 50% of the times people rejected the morphed voice samples of two celebrities as well as briefly familiar users.

2. Balloon: A Forward-Secure Append-Only Persistent Authenticated Data Structure

Tobias Pulls (Karlstad University, Sweden) and Roel Peeters (KU Leuven, Belgium)

Abstract: We present Balloon, a forward-secure append-only persistent authenticated data structure. Balloon is designed for an initially trusted author that generates events to be stored in a data structure (the Balloon) kept by an untrusted server, and clients that query this server for events intended for them based on keys and snapshots. The data structure is persistent such that clients can query keys for the current or past versions of the data structure based upon snapshots, which are generated by the author as new events are inserted. The data structure is authenticated in the sense that the server can verifiably prove all operations with respect to snapshots created by the author. No event inserted into the data structure prior to the compromise of the author can be modified or deleted without detection due to Balloon being publicly verifiable. Balloon supports efficient (non-)membership proofs and verifiable inserts by the author, enabling the author to verify the correctness of inserts without having to store a copy of the Balloon. We formally define and prove that Balloon is a secure authenticated data structure.

3. On the Fly Design and Co-simulation of Responses against Simultaneous Attacks

Léa Samarji, Nora Cuppens-Boulahia, Frédéric Cuppens (Telecom Bretagne, France), Serge Papillon, Waël Kanoun and Samuel Dubus (Alcatel-Lucent Bell Labs, France)

Abstract: The growth of critical information systems in size and complexity has driven the research community to propose automated response systems. These systems must cope with the steady progress of the attacks' sophistication, coordination and effectiveness. Unfortunately, existing response systems still handle attacks independently, suffering thereby from (i) efficiency issues against coordinated attacks (e.g. DDoS), (ii) conflicts between parallel responses, and (iii) unexpected side effects of responses on the system. We, thus, propose in this paper a new response model against simultaneous threats. Our response is dynamically designed based on a new definition of capability-aware logic anticorrelation, and modeled using the Situation Calculus (SC) language. Even though a response can prevent or reduce an attack scenario, it may also have side effects on the system and unintentionally ease one of the attackers to progress on its scenario. We address this issue by proposing a response co-simulator based on SC planning capabilities. This co-simulator considers each response candidate apart and reasons, from the current system's and attackers' state, to assess the achieved risk mitigation on the protected system. Experimentations were led to highlight the benefits of our solution.

Keynote Speakers

Sushil Jajodia

George Mason University Fairfax, USA

Keynote: Adversarial and Uncertain Reasoning for Adaptive Cyber Defense: Building the Scientific Foundation

Thursday, September 24th, 09.00 – 10 00, Lecture Hall A

Abstract: *Today's cyber defenses are largely static. They are governed by slow deliberative processes involving testing, security patch deployment, and human-in-the-loop monitoring. As a result, adversaries can systematically probe target networks, pre-plan their attacks, and ultimately persist for long times inside compromised networks and hosts. A new class of technologies, called Adaptive Cyber Defense (ACD), is being developed that presents adversaries with optimally changing attack surfaces and system configurations, forcing adversaries to continually re-assess and re-plan their cyber operations. Although these approaches (e.g., moving target defense, dynamic diversity, and bio-inspired defense) are promising, they assume stationary and stochastic, but non-adversarial, environments. To realize the full potential, we need to build the scientific foundations so that system resiliency and robustness in adversarial settings can be rigorously defined, quantified, measured, and extrapolated in a rigorous and reliable manner.*

Sushil Jajodia is University Professor, BDM International Professor, and the founding director of Center for Secure Information Systems in the Volgenau School of Engineering at the George Mason University, Fairfax, Virginia. He is also the founding site director of the recently approved NSF I/UCRC Center for Configuration Analytics and Automation at Mason. He served as the chair of the Department of Information and Software Engineering during 1998-2002. He joined Mason after serving as the director of the Database and Expert Systems Program within the Division of Information, Robotics, and Intelligent Systems at the National Science Foundation. Before that he was the head of the Database and Distributed Systems Section in the Computer Science and Systems Branch at the Naval Research Laboratory, Washington and Associate Professor of Computer Science and Director of Graduate Studies at the University of Missouri, Columbia. He has also been a visiting professor at the University of Milan, Italy; Sapienza University of Rome, Italy; Isaac Newton Institute for Mathematical Sciences, Cambridge University, England; King's College, London, England; and Paris Dauphine University, France.

Richard Clayton

University of Cambridge, UK

Keynote: Cybercrime data: Big, Biased and Beyond Review?

Wednesday, September 23rd, 09.15 – 10.15, Lecture Hall A

Abstract: *I spend my academic life generating and processing data about cybercrime. These datasets are big and getting bigger. Some people say that's true of cybercrime as well, but I don't entirely agree! My datasets are also significantly biased, but once you accept that the bias is there it can lead one to find some really useful results. But perhaps the greatest problem that we all have with cybercrime data is an inability to reproduce each other's work — an essential technique for detecting inadvertent errors and improving analysis techniques. At Cambridge we have a new approach to cybercrime data sharing; and I'll be explaining how it is possible to get involved.*

Richard Clayton is a software developer by trade. In the 1980s he co- founded a software house that created the system software for Amstrad CPC and PCW machines — which sold in the millions. In the first half of the 1990s the company produced one of the first Internet access and Internet email systems for Windows. The company was sold to the UK's largest ISP and he worked there until in 2000 he returned to Cambridge to study for a PhD.

He has remained an academic („because it's more fun than working") in the field of 'security economics'. In particular he has been studying wickedness on the Internet for years; be it spam, DDoS attacks (intentional and unintentional), or crimes such as phishing. His approach generally involves identifying datasets of cybercrime activity, often of substantial size, and then attempting to turn raw data into illuminating Information

As of October 2015 he will become Director of the Cambridge Cloud Cybercrime Centre. The Centre intends to build one of the largest and most diverse data sets about cybercrime that any organisation holds and more importantly aims to make this data

available to other academics for them to apply their own skills to address cybercrime issues. Academics currently face considerable difficulties in researching cybercrime and the centre intends to drive a step change in the amount of cybercrime research by making datasets available, not just of URLs but content as well, so that other academics can concentrate on their particular areas of expertise and start being productive immediately.

Afonso Ferreira

Trust & Security Unit, European Commission, Belgium

Invited Talk: The European Strategic Agenda for Research and Innovation in Cybersecurity

Wednesday, September 23rd, 12.15 – 13.00, Lecture Hall A

Abstract: *This talk will present the European Strategic Research and Innovation Agenda (SRA) for cybersecurity as it is being released by the Working Group on Secure ICT Research and Innovation (aka WG3) of the Network and Information Security Platform, which is a public-private partnership put in place by the European Commission in 2013. Members of WG3 are close to two hundred. They address issues related to cybersecurity research and innovation in the context of the EU Strategy for Cyber Security and of the Network and Information Security Platform. WG3 identified the key challenges and corresponding desired outcomes in terms of innovation-focused, applied but also basic research in cybersecurity, privacy, and trust. The European SRA for cybersecurity designed by WG3 serves as main input for the drafting of Horizon 2020 Work Programs by the European Commission and is source of inspiration for the coordination of, and collaboration between, research agendas across Europe, including industry research roadmaps and national research and innovation programs of the Member States.*

Afonso Ferreira is currently in charge, amongst others, of the general secretariat of the Working Group on “Secure ICT Research and Innovation” of the European Network and Information Security Platform, which provides the input for Horizon 2020 Work-Programmes in Digital Security, and is leading the planning and financing of cybersecurity activities through the Connecting Europe Facility programme. He has been seconded as a French expert to the European Commission since 2011, working now as policy officer at the Trust and Security unit of the DG CONNECT. Other assignments included the Future and Emerging Technologies unit and the Digital Futures task force.

Social Events

Wednesday, 23rd September 2015 – Mayor's Reception

A vintage tram will take us to the Heurigenrestaurant "10er Marie", the oldest wine tavern of Vienna (1740) and the location of the Mayor's Reception. During the ride you will be able to see several main attractions such as the Vienna State Opera, the Museum of Fine Arts, the Museum of Natural History, the Heldenplatz and the Austrian Parliament.

Meeting point: 18:00 in front of the Conference Venue (after the last session)

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

Address:
10er Marie
Ottakringer Straße 222-224
1160 Vienna
(Metro stop U3 „Ottakring"– directions will be provided, no organized transport for returning)

Thursday, 24th September 2015 – Conference Dinner

A bus will take us to **Schönbrunn Palace**, Empress Sisi's former summer residence. The palace is part of UNESCO's cultural heritage due to its historic importance, its unique grounds and its splendid furnishings. At Schönbrunn Palace we have organized a Grand Tour, which will give you a picture of the different stylistic eras of the imperial monarchy and the life's of the palace´s inhabitants.

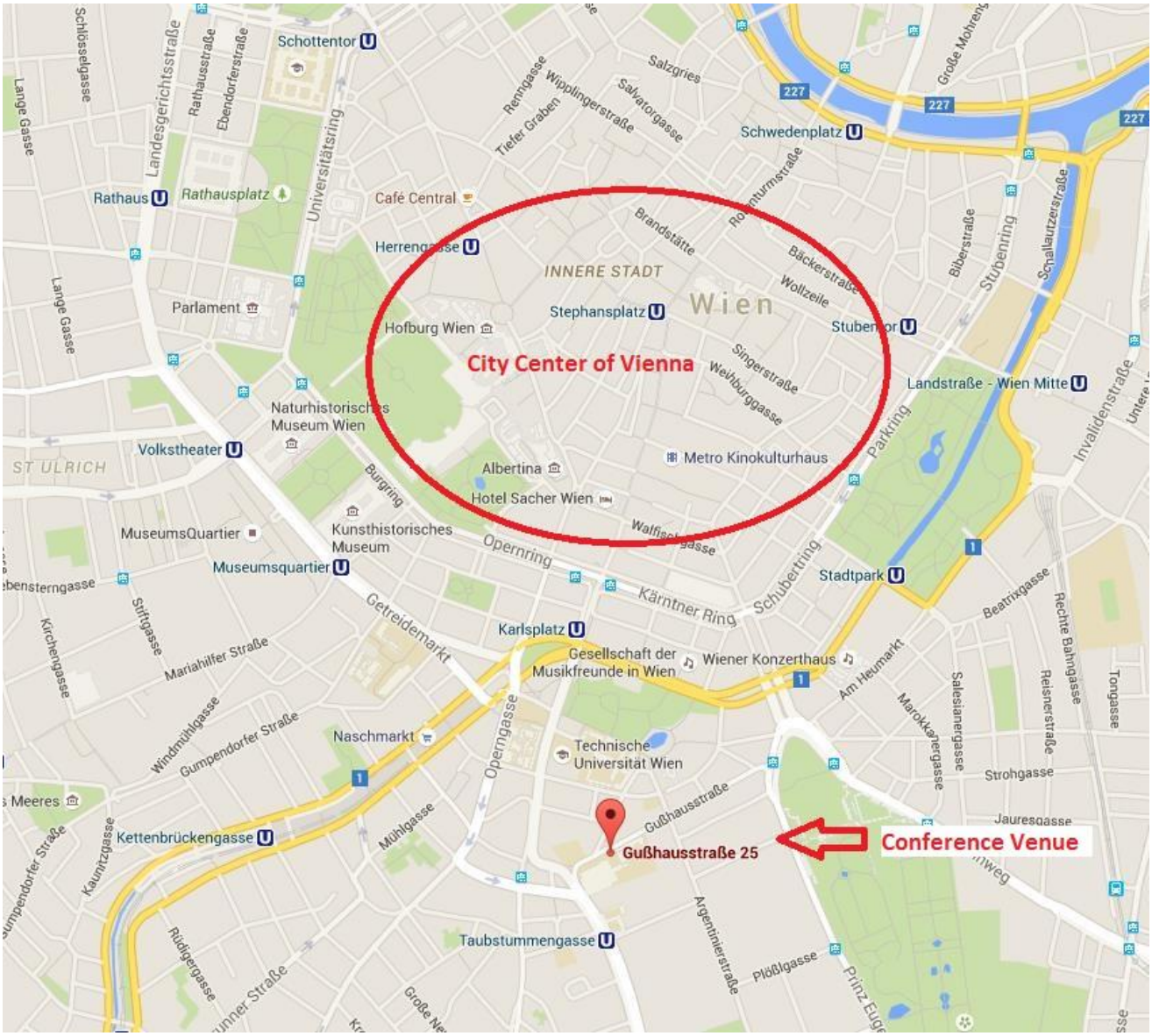
After the tour little trains will take us to the Conference Dinner location, the **Orang.erie**, which is located in the „Vienna Zoo". Founded as an imperial menagerie in 1752, it is the oldest zoo in the world. The Vienna Zoo is located on the grounds of the Schönbrunn Palace, on our way from the Palace to the Dinner location you will see parts of it.

Meeting point: 17:00 in front of the Conference Venue (after the last session)

Address:
Orang.erie
Maxerstraße 13
1130 Vienna
(Metro stop U4 „Hietzing"– directions will be provided, no organized transport for returning)

Schönbrunn Palace

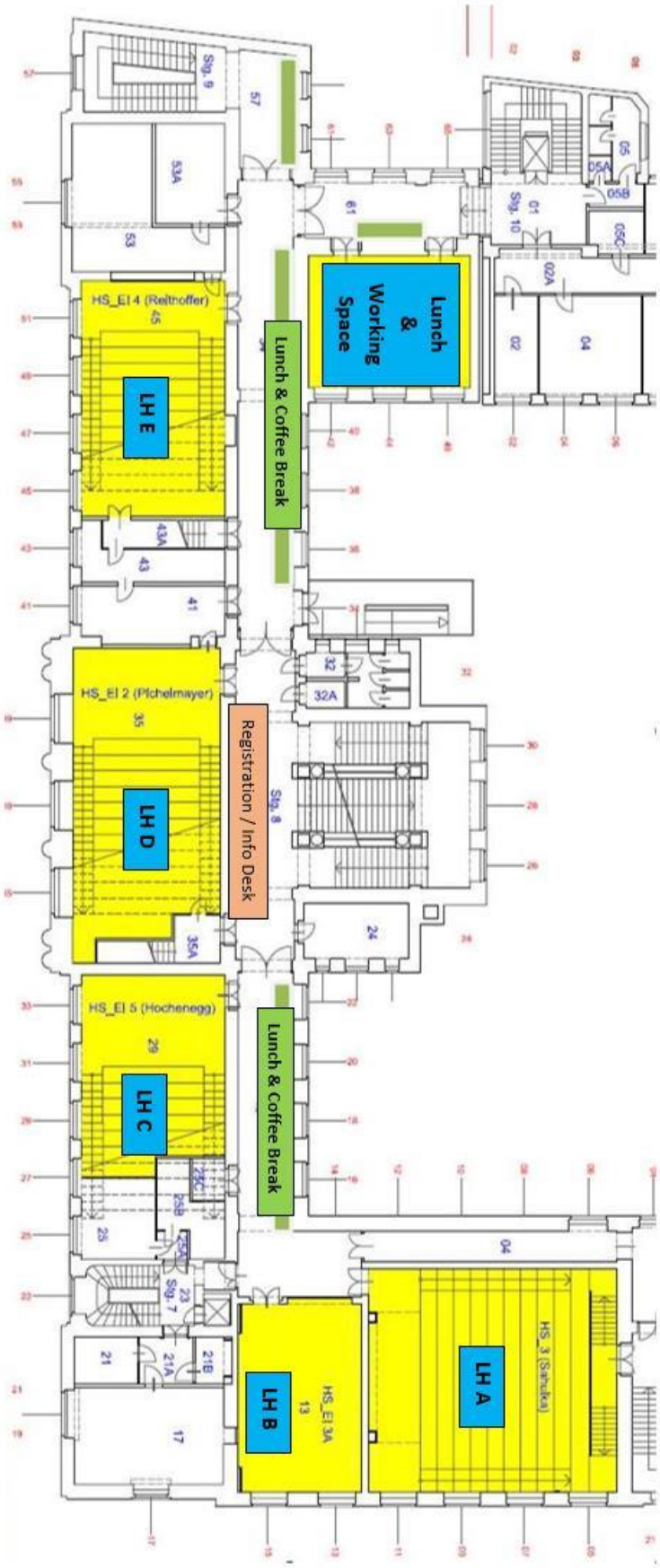
Venue Overview



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:

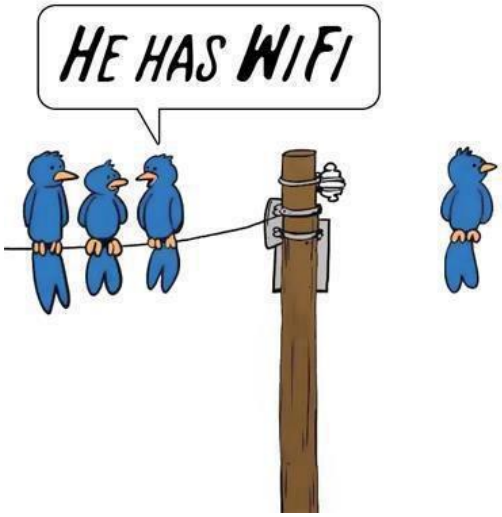
Wednesday, September 23rd 2015
French onion soup
Meat (pork) cut into strips Zurich style with spiral noodles **or** cauliflower cheese burger with ratatouille

Thursday, September 24th 2015
Peas cream soup
Roast beef in pepper cream soup with bread dumplings **or** Potato goulash

Friday, September 25th 2015
Clear vegetable soup with small egg dumplings
Roast chicken breast on vegetables with almond rice **or** Penne with tomatoes basil sauce and 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.

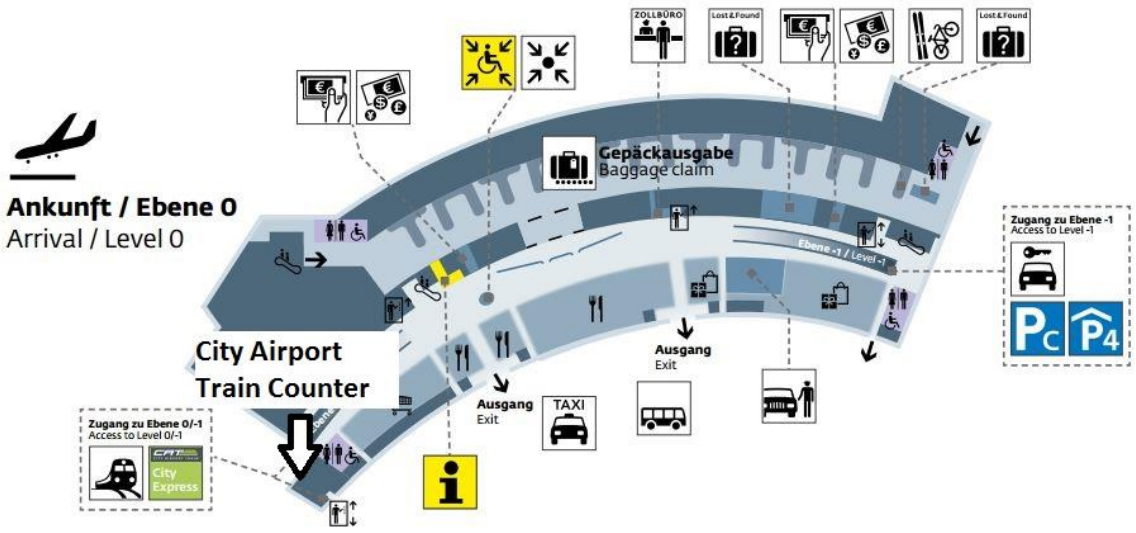
1. City Airport Train / CAT

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.

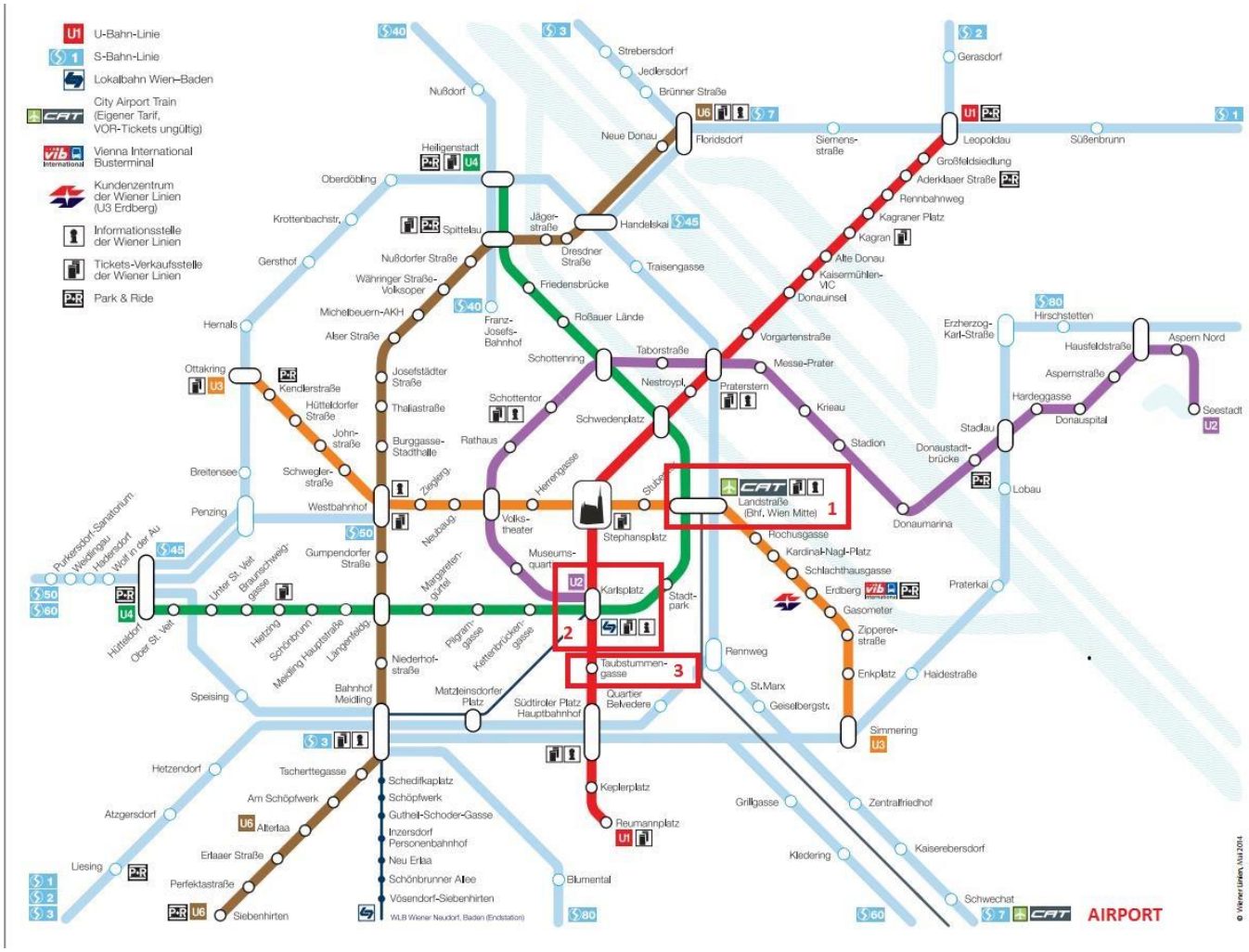
If you decide to take the S-Bahn to get to the Conference Venue:

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

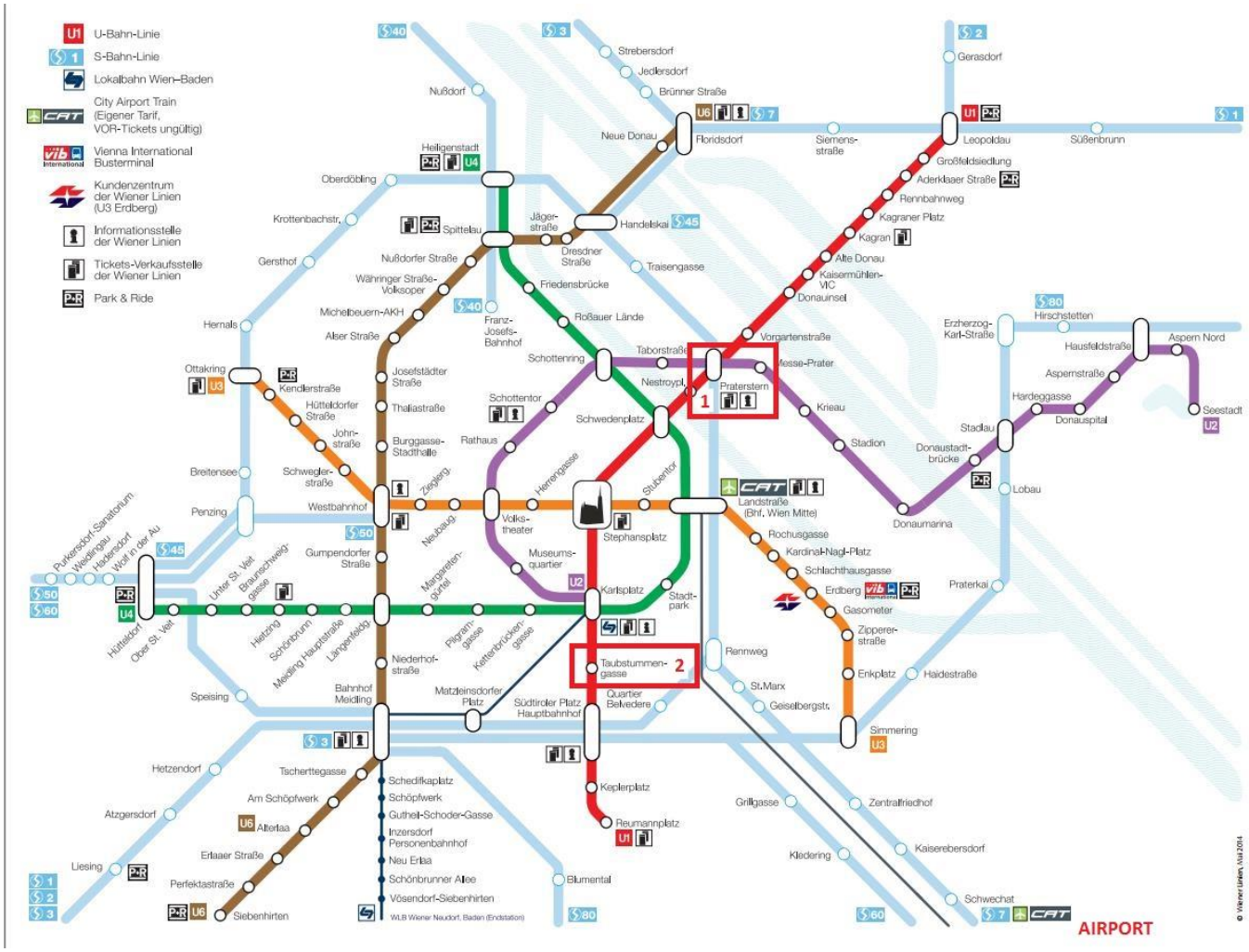
Stop „Taubstummengasse“ to the conference venue:

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

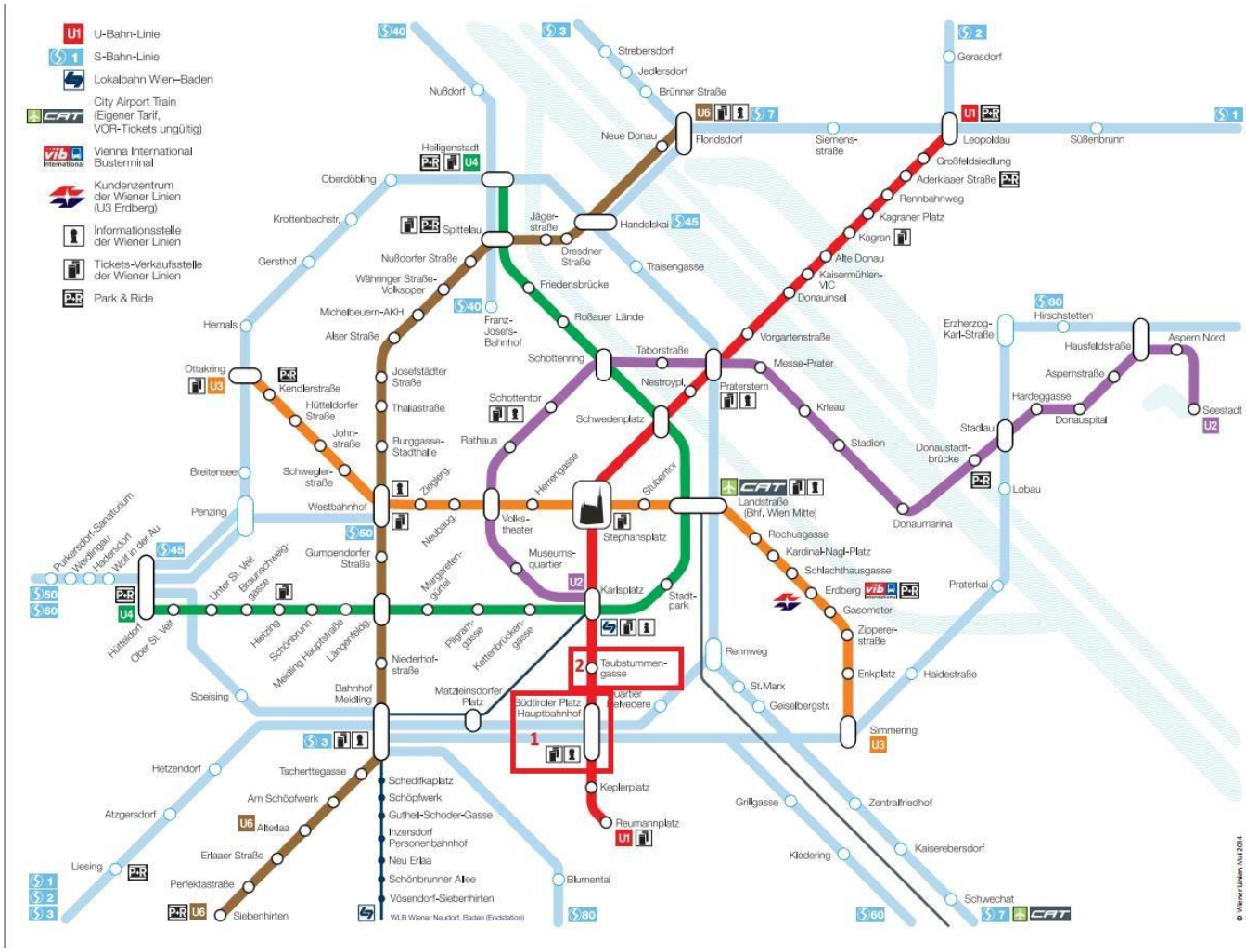


Map 6: S-Bahn: Airport -> Conference Venue

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

2 Get out at “Taubstummengasse”

Underground MAP ICE

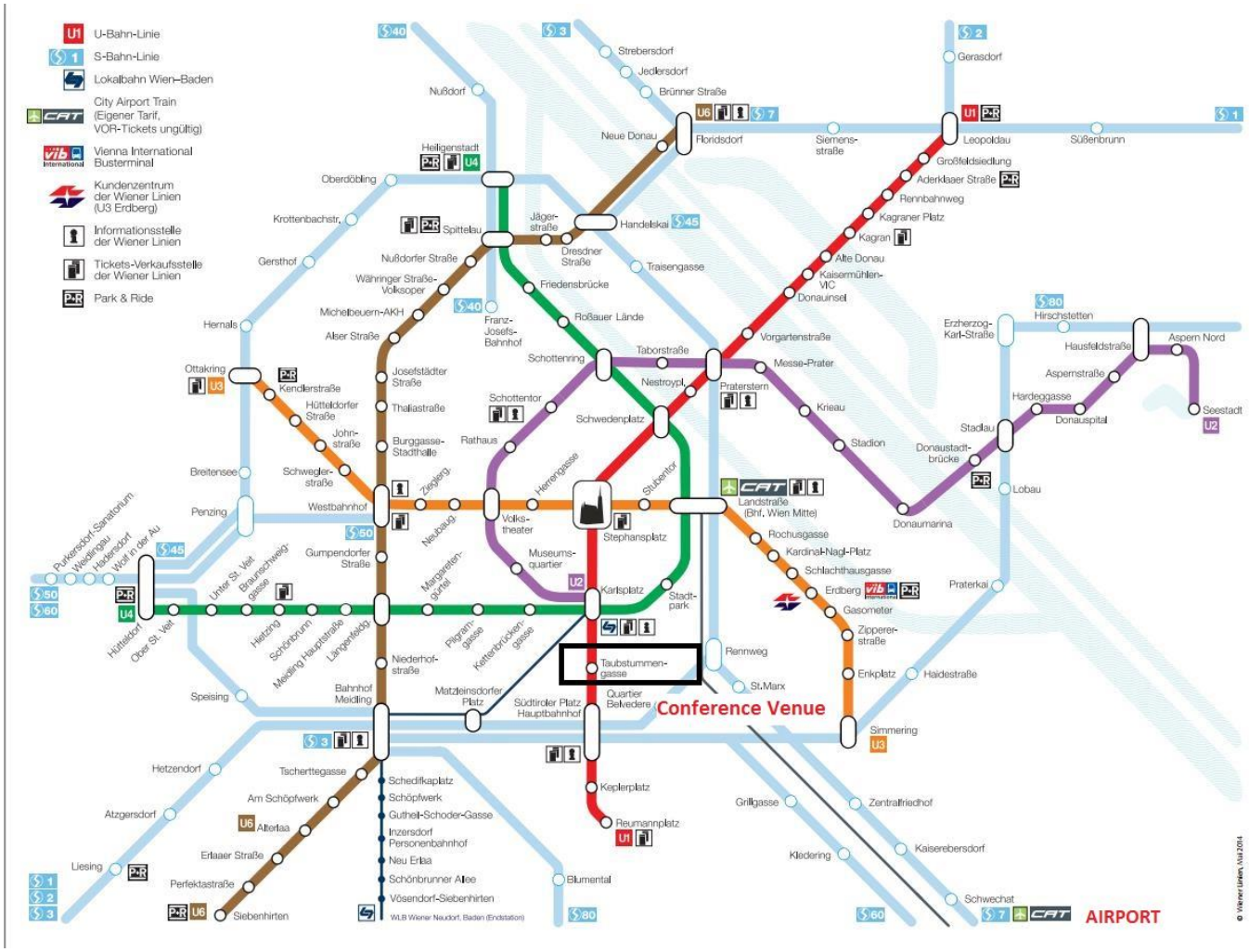


Map 7: ICE Airport -> Conference Venue

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.

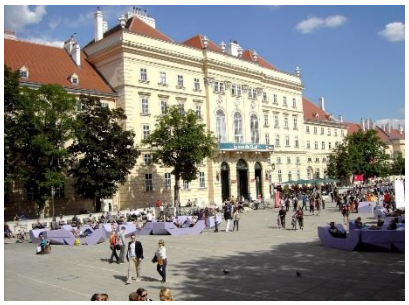

Volksgarten

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€

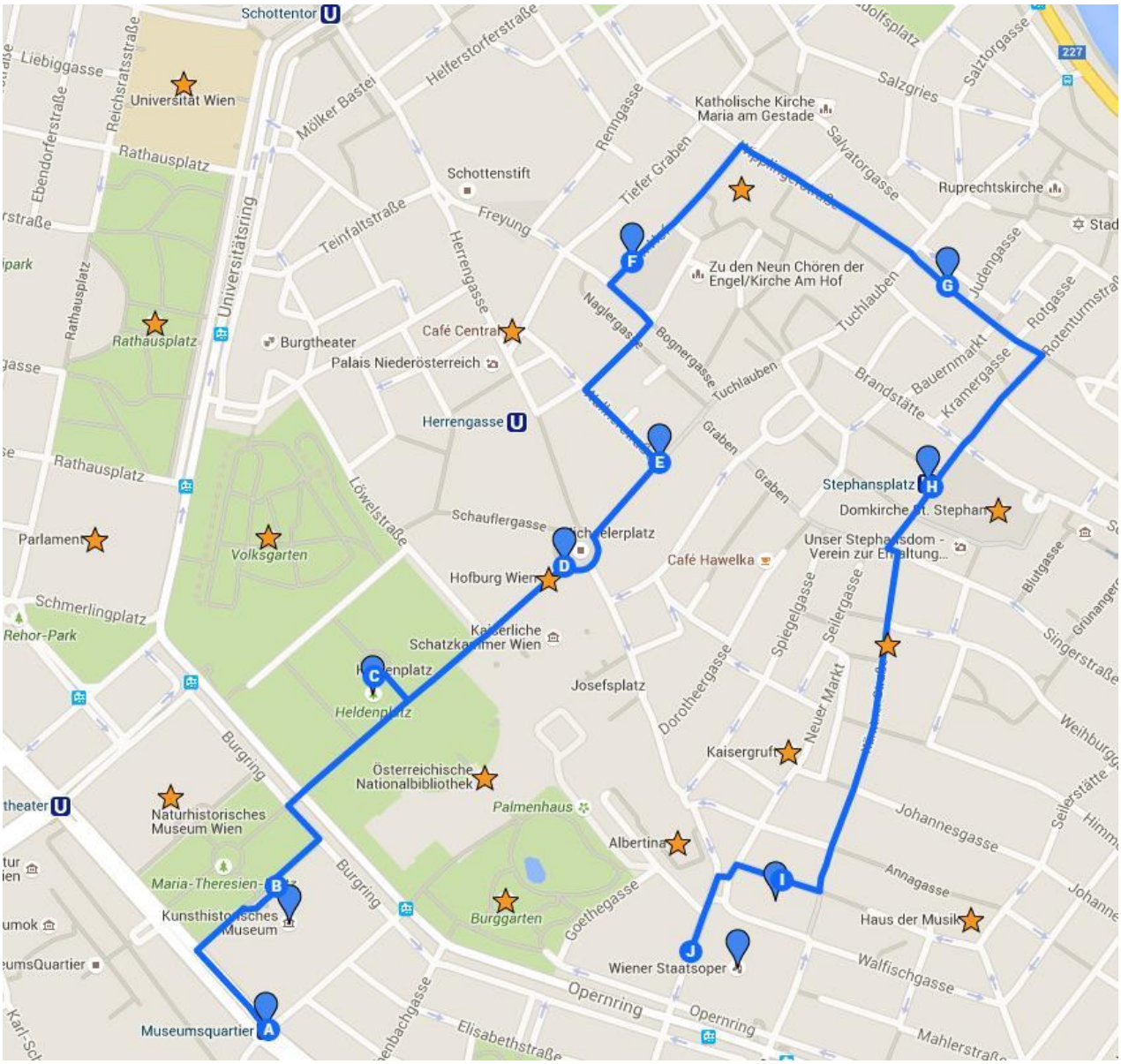
Guided Tours Spanish Horse Riding School

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

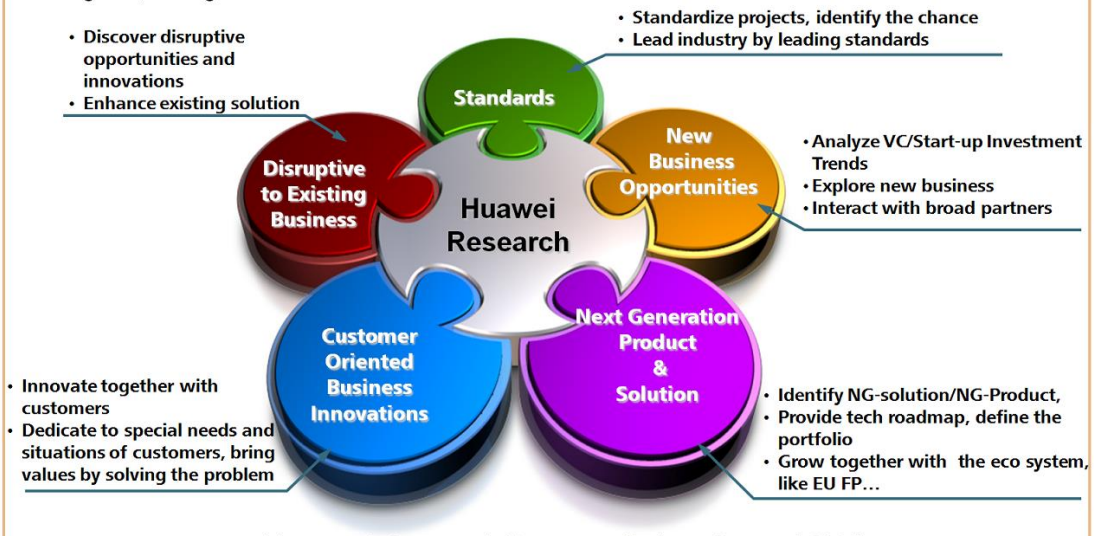
Bettina Bauer
bbauer@sba-research.org
Tel: +43 664 254 03 14

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

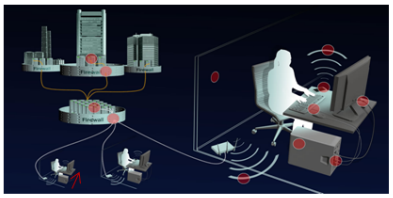
Shield Lab has four branches distributed in Singapore, Beijing, Shenzhen and Paris, and is focusing on the security technologies for the forthcoming ICT, including but not limited to:

- 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

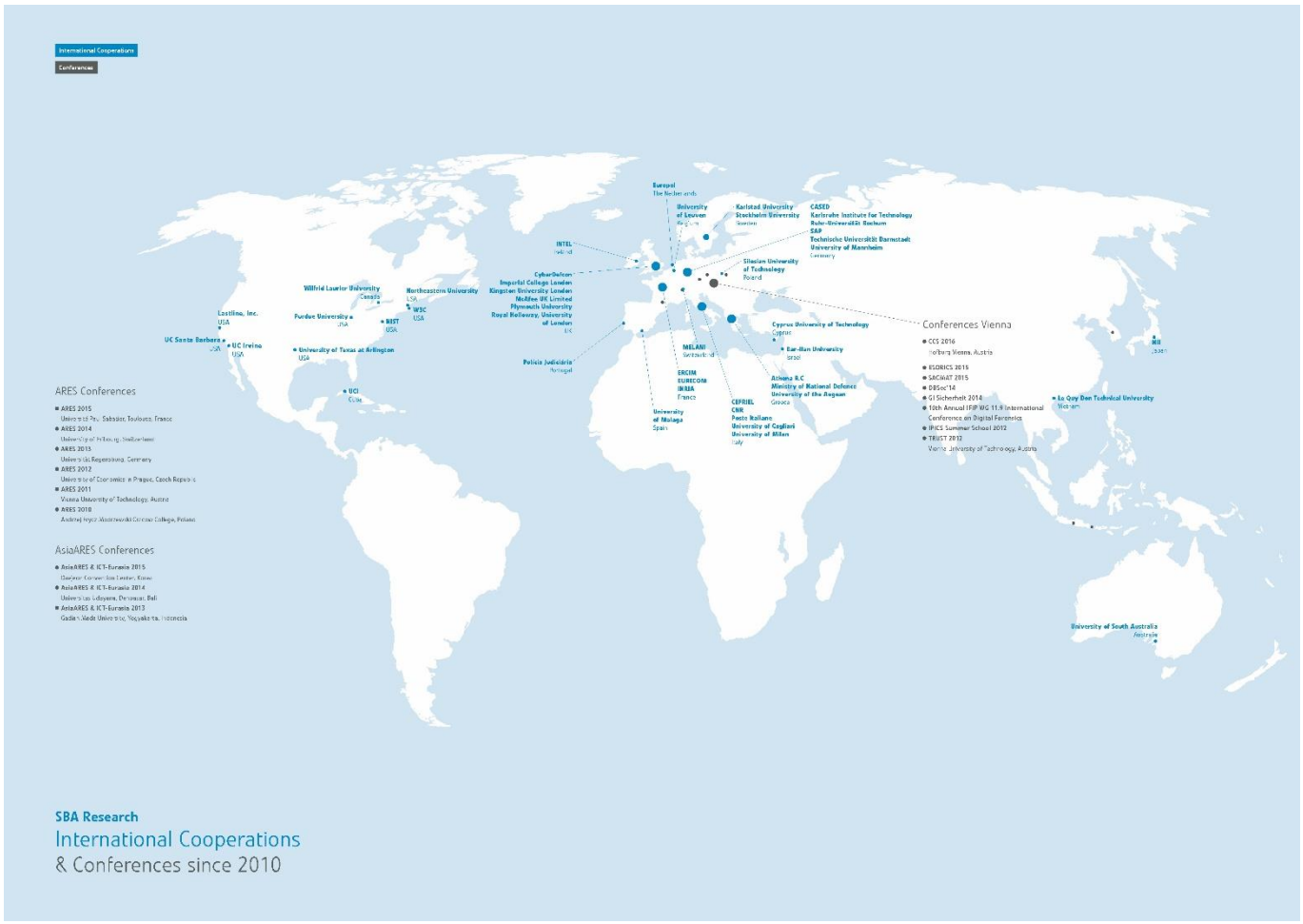
SBA Research

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

Wednesday, Sept 23

	LH C	LH D
08:00 - 17:00	REGISTRATION	
09:00 - 09:15	Opening Leture Hall A	
09:15 - 10:15	Keynote Session *Richard Clayton, University of Cambridge, UK* Lecture Hall A	
10:15 - 10:45	Break	
10:45 - 12:15	Session 1A: Network & Web Security	Session 1B: Cryptography I
12:15 - 13:00	Invited Talk *Afonso Ferreira, European Commission* Lecture Hall A	
13:00 - 14:30	Lunch	
14:30 - 16:00	Session 2A: System Security	Session 2B: Cryptography II
16:00 - 16:30	Break	
16:30 - 18:00	Session 3A: Risk Analysis	Session 3B: Cryptography III
18:00 - 22:00	Mayor's Reception	

Thursday, Sept 24

	LH C	LH D
08:00 - 17:00	REGISTRATION	
09:00 - 10:00	Keynote Session *Sushil Jajodia, George Mason University Fairfax, US* Lecture Hall A	
10.00 - 10:30	Break	
10:30 - 12:00	Session 4A: Privacy I	Session 4B: Signatures
12:00 - 13:30	Lunch	
13:30 - 15:00	Session 5A: Privacy II	Session 5B: Applied Security I
15:00 - 15:30	Break	
15:30 - 17:00	Session 6A: Cloud Security	Session 6B: Protocols & ABE
17:00 - 23:00	Conference Dinner	

Friday, Sept 25

	LH C	LH D	LH E
08:00 - 17:00	REGISTRATION		
09:00 - 10:30	Session 7A: Cloud Analysis & Side-Channels	Session 7B: Crypto Applications & Attacks	PhD Symposium
10:30 - 11:00	Break		
11:00 - 12:30	Session 8A: Authentication I	Session 8B: Policies	PhD Symposium
12:30 - 14:00	Lunch		
14:00 - 15:30	Session 9A: Authentication II	Session 9B: Detection & Monitoring	PhD Symposium
15:30 - 15:45	Break		
15:45 - 17:15	Session 10: Applied Security II		