PROGRAM
ANDROID SECURITY SYMPOSIUM

9th – 11th September 2015
Vienna, Austria

Josef Ressel Center for
User-friendly Secure Mobile Environments (u'smile)

u'smile

https://usmile.at/symposium

SBA Research

INSTITUTE OF NETWORKS AND SECURITY

FH OBERÖSTERREICH
UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

Welcome

We welcome you to the Android Security Symposium in Vienna, Austria. Presentations by top speakers from the field of Android security and privacy will provide an in-depth view of Android security architecture, threats to mobile security, and countermeasures. Special focus areas are trusted computing concepts, usable security for everyone, and malware analysis. In addition, a PhD school gives doctoral candidates an opportunity to present their current research and therefore provides a glimpse of upcoming topics in Android security research.

The Josef Ressel Center for User-friendly Secure Mobile Environments (u'smile) started its research activities in 2012 with the driving vision of replacing wallets and key chains by usable, secure hardware and software in mobile devices with a particular focus on Android smart phones. Three years later, we begin to see some of these scenarios becoming mainstream, such as mobile NFC payment, first prototypes for digital identity cards and more wide-spread use of biometric user authentication. Nonetheless, many challenges concerning security and usability remain, and the Android Security Symposium brings together academic and industry researchers to discuss current issues and next steps.

This Android Security Symposium is funded by the Christian Doppler Forschungsgesellschaft (CDG) from funds of the Federal Ministry of Science, Research and Economy (BMWFW) and the Nationalstiftung für Forschung, Technologie und Entwicklung. We are also thankful to support by our three host institutions: University of Applied Sciences Upper Austria in Hagenberg, the Institute of Networks and Security at Johannes Kepler University Linz, and SBA Research.

We are particularly grateful to all our international expert speakers, who freely present their deep insights and latest results to a wide audience without compensation for their time and effort. It is on their shoulders that the Android Security Symposium rests.

bmwfw
Bundesministerium für Wissenschaft, Forschung und Wirtschaft

Prof. Dr. René Mayrhofer Prof. Dr. Edgar Weippl Dr. Michael Roland

Android Security Symposium

Venue

Vienna University of Technology / TU Wien

Room: Festsaal (1st floor)

Karlsplatz 13
1040 Vienna
Austria

www.tuwien.ac.at

Program Overview

Wednesday, 9th September 2015	Thursday, 10th September 2015	Friday, 11th September 2015
Welcome Speech		
Exploring Android Security	Security for Everyone	Incident Handling, Malware and Countermeasures
Lunch and Networking Break		
Exploring Android Security	Trusted Computing	Malware and Countermeasures
PhD School		
	Social Event	

Program
9th September 2015

08:30	Registration
09:15	Welcome speech

Exploring Android Security
Chair: René Mayrhofer

09:30	**Improving mobile security with forensics, app analysis and big data** Andrew Hoog NowSecure (USA)
10:30	Coffee break
11:00	**Android security architecture** Nikolay Elenkov Sarion Systems Research (Japan)
12:00	Lunch and networking break
13:30	**Lessons from the trenches: An inside look at Android security** Nick Kralevich Google (USA)
14:15	**Exploit mitigation at the native level for RISC-based devices** Matthias Neugschwandtner IBM Research Zurich (Switzerland)
15:00	Coffee break

PhD School
Chair: René Mayrhofer

15:30	**Secure copy protection for mobile apps** Nils T. Kannengiesser Technische Universität München (Germany)
16:00	**Human factors in anonymous mobile communication** Svenja Schröder University of Vienna (Austria)
16:30	**Continuous risk-aware multi-modal authentication** Daniel Hintze FHDW Paderborn (Germany) Rainhard Findling, Muhammad Muaaz JRC u'smile (Austria)
17:00	Closing of day

Program
10th September 2015

08:30	Registration
09:15	Welcome speech

Security for Everyone
Chair: Edgar Weippl

09:30	**Assessing Android applications using command-line fu** Pau Oliva Fora NowSecure (Spain)
10:30	Coffee break
11:00	**The quest for usable security** N. Asokan Aalto University / University of Helsinki (Finland)
12:00	Lunch and networking break

Trusted Computing
Chair: Edgar Weippl

13:30	**Android and trusted execution environments** Jan-Erik Ekberg Trustonic Inc (Finland)
14:00	**An infestigation of dragons: Exploring vulnerabilities in the ARM TrustZone architecture** Josh Thomas, Charles Holmes Atredis Partners (USA)
15:00	Coffee break
15:30	**Using Android security for governmental PKI: Opportunities and challenges** Pekka Laitinen Population Register Centre (Finland)
16:00	**Secure elements for you and me: A model for programmable secure hardware in mobile ecosystems** Alexandra Dmitrienko Fraunhofer SIT (Germany)
16:45	Closing of day
17:00	Social event

Program
11th September 2015

08:30	Registration
09:15	Welcome speech

Incident Handling, Malware, and Countermeasures
Chair: René Mayrhofer

09:30	**Mobile threats incident handling** Yonas Leguesse ENISA (Greece)
10:30	Coffee break
11:00	**ANANAS – ANalyzing ANdroid ApplicationS** Dieter Vymazal University of Applied Sciences Upper Austria (Austria)
12:00	Lunch and networking break
13:30	**How Google killed two-factor authentication** Victor van der Veen VU University Amsterdam (Netherlands)
14:00	**A walk through the construction of the first mobile malware tracker** Federico Maggi Politecnico di Milano (Italy)
15:00	Closing of day

Andrew Hoog

NowSecure (Oak Park, IL, USA)

Andrew Hoog is a top industry mobile forensics and security expert, computer scientist and is the CEO and co-founder of NowSecure, a leading mobile security company. Hoog has three patents pending and has authored two books on mobile forensics and security. When not breaking (or fixing) things, he enjoys great wine, science fiction, running and tinkering with geeky gadgets.

Improving mobile security with forensics, app analysis and big data

The velocity of change in the mobile ecosystem requires a new techniques to secure mobile devices. This talk will explain how we can address this challenge by combining global data from mobile devices and app store metadata with static, forensic and dynamic app analysis to create a powerful, data-centric approach to mobile security.

Nikolay Elenkov

Sarion Systems Research (Tokyo, Japan)

Nikolay Elenkov has been working on enterprise security projects for the past 10 years. He has developed security software on various platforms, ranging from smart cards and HSMs to Windows and Linux servers. He became interested in Android shortly after the initial public release and is the author of 'Android Security Internals' (http://www.nostarch.com/androidsecurity).

Android security architecture

This talk will give an overview of Android's security architecture from the bottom up, and present the major Android subsystems and components that relate to device and data security. The talk will cover broader topics that affect all applications, such as package and user management, permissions and device policy, and will also touch on more specific ones such as cryptographic providers, PKI, and credential storage. Some of the changes introduced in the upcoming Android M release will also be explored.

Nick Kralevich

Google (Mountain View, CA, USA)

Nick Kralevich is head of Android platform security at Google and one of the original members of the Android security team. In his 7 years in Android, he led the development of Android's key security features and has been on the forefront of modern operating system security. Nick's expertise is in defensive security technologies with a focus on native code hardening, application containment, and exploit mitigation.

Lessons from the trenches: An inside look at Android security

When Android was first released in 2008, few could have recognized the impact it would have on the mobile world. Today, it is the largest mobile operating system in existence, with billions of users trusting their most sensitive data to Android.

In this talk, Nick will discuss the evolution of Android security from the beginning to today, and give you an inside look into the Android security. What are the things that worked well for Android? What are the things that haven't work? Where will we go in the future? And what are the philosophies that guide our every day decision making?

Matthias Neugschwandtner

IBM Research (Zurich, Switzerland)

Matthias Neugschwandtner is a system security researcher working at the Cloud and Storage Security Group at IBM Research, Zurich. The main focus of his research lies on low-level system security. This encompasses program analysis, vulnerability detection and system hardening. During his academic career he worked at the Vienna University of Technology, Vrije Universiteit Amsterdam and the Northeastern University in Boston.

Exploit mitigation at the native level for RISC-based devices

(coming soon)

Nils T. Kannengiesser

Technische Universität München (Munich, Germany)

Nils Kannengiesser is a teaching/research associate at the Technical University of Munich (TUM). His major is Information Technology and he studied in Kiel (Germany) as well as College Station (USA). His current research is about Android Security and Copy Protection using Secure Elements.

Secure copy protection for mobile apps

Highly sophisticated copy protections exist in the desktop world for decades already and were most often used to prevent users from creating illegal copies of CDs or DVDs, while the applications were checking for a valid disc. Instead modern smartphones gather their apps from official markets by default and these apps are bound to a user's account in theory. Of course, it's possible to access the app files and redistribute them to other users and devices. While it might be no issue for free apps, developers of paid apps risk the loss of revenue. For this reason Google provided developers libraries for license verifications (LVL). Nevertheless the provided methods can be easily cracked and many developers seem to be unaware of the risks even nowadays. In this talk we want to present an approach for copy protection using secure elements on smartphones with Android.

Svenja Schröder

University of Vienna (Vienna, Austria)

Svenja Schröder received her Master's degree in Applied Communication and Media Science from the University of Duisburg-Essen in 2008. From 2003 until 2010 she worked—first as student assistant, later as research associate—for the Chair of Collaborative Learning in Intelligent Distributed Environments (COLLIDE) where her research focus was mainly on social network analysis, ontology engineering and human computer interaction.
Since 2014, Svenja Schröder is research assistant at the Cooperative Systems Research Group (COSY) at the University of Vienna and is responsible for the scientific coordination of the cosy:lab which focuses on user trials. Furthermore, her research interest is in the field of usable security and human computer interaction which is also the topic of her PhD thesis.

Human factors in anonymous mobile communications

As the user is shifting more into focus as an essential part of secure systems, the field of usable security is significantly gaining in importance. This is especially true for anonymity networks like Tor, which allow anonymous communication on the Internet. Although a variety of studies have examined the usability of programs to access the Tor network from a traditional PC, research concerning Tor-related apps on mobile devices is extremely sparse. Therefore, this PhD project aims at researching usability and human factors of apps for accessing Tor, starting with Orbot, a Tor proxy app for Android devices.

Our research approach starts from the fact that mobile devices have some limitations compared to full-size computers, notably limited means of user interaction. On the other hand mobile devices also offer features traditional computers lack, like additional sensors and rich context information. HCI as a broad field can help to deal with those limitations and opportunities in order to forge more usable and thus more secure interfaces. Hence, this PhD project aims at systematically identifying all sorts of usability issues in mobile Tor apps. Especially characteristics of mobile context and mobile interactions will be considered in our research, with a strong focus on how mobile context influences usage of Tor apps in the field.

To this end, usability evaluations will take place as controlled laboratory studies as well as field studies. All user studies will be conducted in the COSY user trial lab, which is currently set up and will be fully available at the group's premises by the end of 2015. Based on the results improvements to the user interface will be suggested and implemented. General design guidelines for mobile usable security and privacy apps will be provided.

Daniel Hintze

FHDW University of Applied Sciences (Paderborn, Germany)

Daniel Hintze received a M.Sc. in IT-Management and Information Systems from FHDW University of Applied Sciences, Paderborn, Germany in 2013. Since November 2013 he is enrolled in the PhD program at Johannes Kepler University (JKU) Linz, Austria, with expected date of completion to be end of 2017. His main research interests include authentication on mobile devices, mobile device usage and UI design. Supervisors are René Mayrhofer and Josef Scharinger, professors at JKU Linz, as well as Eckhard Koch, professor at FHDW Paderborn.

Rainhard Findling

University of Applied Sciences Upper Austria (Hagenberg, Austria)

Rainhard Dieter Findling received his BSc and MSc degree in Mobile Computing from the University of Applied Sciences Upper Austria in 2011 and 2013 with distinction. Currently, he is researcher with u'smile, the Josef Ressel Center for User-Friendly Secure Mobile Environments, at the University of Applied Sciences Upper Austria at Hagenberg, and works towards his PhD with the Institute of Networks and Security, at the Johannes Kepler University Linz, Austria. His research interests include machine learning, biometrics, and security in the context of mobile environments and ubiquitous computing.

Muhammad Muaaz

University of Applied Sciences Upper Austria (Hagenberg, Austria)

Muhammad Muaaz received a M.Sc. degree in Information and Communication Systems Security from KTH Royal Institute of Technology, Stockholm, Sweden in 2012. Since 2013 he is enrolled in the PhD program at Johannes Kepler University Linz, Austria under the supervision of Prof. Dr. René Mayrhofer and Prof. Dr. Josef Scharinger. His main research interests include information security, biometric authentication on mobile devices, and machine learning.

Continuous risk-aware multi-modal authentication

Nowadays, people own and carry an increasing number of mobile devices, such as smartphones and smartwatches. To protect sensitive data, these devices need authentication mechanisms—which usually don't go beyond point of entry and don't scale well with a growing number of devices and interactions. We present the preliminary design of CORMORANT, an extensible, risk-aware, multi-modal, cross-device authentication framework that enables transparent continuous authentication using different biometrics across multiple trusted devices. With the CORMORANT framework, we aim for user-friendly mobile devices security by reducing the number of authentication attempts and easing the integration of new authentication and risk assessment mechanisms.

Pau Oliva Fora

NowSecure (Barcelona, Spain)

Pau Oliva Fora (@pof) is a Senior Mobile Security Engineer with NowSecure and co-author of the "Android Hacker's Handbook". His passion for smartphones started back in 2004 when he had his first PocketPC phone with the Windows Mobile operating system, and he began reverse engineering and hacking HTC devices. Pau has been actively researching security aspects of the Android operating system since its debut with the T-Mobile G1 on October 2008. He has spoken at a variety of security conferences, such as DefCon and RSA in the US and RootedCon, NoConName and OWASP in Spain.

Assessing Android applications using command-line fu

In this talk we will walk attendees through the process of taking apart an Android application using simple command line tools and bash magic tricks, breaking down awesome one-liners to loop through "adb shell" commands. The session will cover the current state of the art to disassemble Dalvik bytecode, obtain the decompiled Java source, checking the application's certificate, checking for source code obfuscation and easily find vulnerable code such as the SecureRandom bug or testing for the presence of MasterKey exploit in an APK among other fancy stuff you never imagined you could do just using the command line.

N. Asokan

Aalto University / University of Helsinki (Finland)

N. Asokan is a professor at Aalto University and the University of Helsinki. Prior to joining academia, he spent over 15 years at leading industrial research laboratories. His research interests center on understanding how to build systems that are simultaneously secure, easy to use and inexpensive to deploy. More information on Asokan's work is available at his website http://asokan.org/asokan/.

The quest for usable security

Over the last decade or so, the security research community has come to recognize the importance of simultaneously achieving usability and security goals when designing new protocols, applications, and systems for ordinary non-specialist users in the mass market. Often the primary motivation (from the perspective of designers) for usable security arises when lack thereof will lead to a definite cost. The source of such costs can be surprising.

I will use two example problem instances as case studies to discuss the challenges of designing usable and secure systems. The first is the case of secure device pairing, where the research and standardization communities attempted to design and deploy a suite of device pairing mechanisms that are both usable and secure. This effort resulted in the development of several novel key agreement protocols. The second is a recent attempt to design a zero-effort deauthentication scheme. I will then describe a number of current problems in mobile devices that need usable and secure solutions.

On the positive side, mobile devices offer opportunities for security researchers that traditional PCs do not. I will briefly outline some exploratory ideas that my colleagues and I have been investigating on this front.

Jan-Erik Ekberg

Trustonic Inc. (Helsinki, Finland)

Jan-Erik Ekberg is Director of Advanced Development at Trustonic. His background is in the telecom industry, where he worked for 18 years at Nokia Research Center. His primary interests are with issues related to platform security, TPMs and TEEs, but he has also background in (securing) network protocols and telecom systems, as well with short-range communication technologies like NFC, BT-LE and WLAN. In his latest role his main focus is in trusted execution environments for Android, but also in OS security aspects such as SEAndroid. Jan-Erik received his doctorate in Computer Science from Aalto Uni-versity.

Android and trusted execution environments

Over the last years, third-party provisionable Trusted Execution Environments (TEEs) have seen increasing market presence, one estimate is that 0.5B handsets have been shipped with one, at least 350M of these are Android handsets. Interface standards in the field are also maturing.

My talk will focus on the deployed TEE ecosystem with an Android perspective—outlining what a TEE architecturally is, which components and services it typically contains and which processing / processor services form the fundament of the TEE security argument. I will briefly touch on recent platform alternatives for TEE development and research, as well as which directions in which we see TEEs evolving in the near future. I will round up by motivating TEE usefulness through a few selected use-cases like mobile payments and identity, as well as a few architecture and application results we have recently reached in the new domain of TEEs in servers (Cloud), primarily in collaboration with Aalto University, Helsinki.

Josh Thomas

Atredis Partners (Houston, TX, USA)

Josh Thomas is a founding member of Atredis Partners, a niche consulting shop performing reverse engineering and security assessments of hardware and software products for vendors and end customers. Previously, he was a Senior Research Scientist with Accuvant's Applied Research team, and has worked as a Senior Research Engineer at The MITRE Corporation. Josh specializes in mobile, embedded systems, protocol and architecture analysis and has a deep history with malware and advanced rootkit research. Josh has written for multiple journals and industry publications over the past years and he has open sourced the entirety of his work for the DARPA Cyber Fast Track program.

Charles Holmes

Atredis Partners (Boston, MA, USA)

Charles Holmes has spent nearly the last decade working on sensitive projects for various US government and research organizations. Charles specializes in mobile security, malware and rootkit development, and advanced software engineering.
Prior to joining Atredis, Charles was a Senior Research Lead with The MITRE Corporation. In that role, Charles led research into a variety of mobile platforms including Apple, Android, Telematics, and Blackberry.
Before shifting focus to mobile security, Charles worked on a variety of projects for the Department of Defense. These projects included the next generation software for the dis-mounted soldier, tactical radio networking, RFID card readers, nuclear threat modeling, and mission planning systems.

An infestigation of dragons: Exploring vulnerabilities in the ARM TrustZone architecture

ARM TrustZone is being heavily marketed as a be all solution for mobile security. Through extensive marketing promising BYOD, secure PIN entry, and protection against APT and the prevalence of ARM devices on mobile platforms, millions of devices now contain an implementation of TrustZone. However, the current drivers for TrustZone adoption primarily relate to vendor lock and Digital Rights Management (DRM), rather than increasing the difficulty in compromising user data. Further, due to TZ architecture, the inclusion of DRM protections provide a net reduction in real world security provided to the device owner.

In this talk, we provide an overview of the ARM TrustZone architecture as utilized by modern Android, Blackberry, and Windows phones. We discuss its potential, its current use cases, its shortcomings, and its impact on the security of modern phones. At this point, we dive into the details of the Qualcomm implementation, which is utilized on the flagship mobile devices from each major vendor, excluding Apple. Specifically, we cover vulnerabilities in codebases from Qualcomm, OEM Vendors, and 3rd Parties, as well as attack surface, exploitation pathways, difficulties, and successes.

Pekka Laitinen

Population Register Centre (Helsinki, Finland)

Pekka Laitinen is a Senior Analyst in Development and Production team of Certification Authority Services group at Population Register Centre (PRC). He joined PRC in February 2013 and is responsible for research and development in the mobile PKI area. Prior his work at PRC, he worked 16 years as a researcher at Nokia Research Center, Helsinki. At Nokia, Pekka was a member of the security research group, which succeeded in effecting several technology transfers to Nokia business units.

Using Android security for governmental PKI: Opportunities and challegens

The talk provides a view of a governmental CA provider on Android's hardware based security. Can it be used for governmental PKI? What are the opportunities and challenges? How to do the registration, enrollment, and usage of the credential securely but still user friendly way? There are a lot of issues to be solved but we are getting there.

Yonas Leguesse

ENISA (Athens, Greece)

Yonas Leguesse is an Expert in Network and Information Security at ENISA. He has a background in the field of Law Enforcement, and is currently preparing and delivering training courses to Computer Emergency Response Teams within the EU.

Mobile threats incident handling

This presentation will demonstrate how the application of an incident handling procedure can simplify the process of incident handling. This will be validated through a case study, where the incident handler will cover certain critical steps such as incident reporting, mitigation, and the closing of an incident. The incident handling procedure will be based on ENISA's framework for incident handling:
https://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process

Alexandra Dmitrienko

Fraunhofer SIT (Darmstadt, Germany)

Alexandra is a researcher at the Fraunhofer Institute for Secure Information Technology since 2011. Starting from January 2015 she leads the Mobile Services group of the Cyber-Physical Systems Security department of Fraunhofer SIT. Recently Alexandra obtained her PhD in Information Security from TU Darmstadt. Her academic achievements within a PhD program were awarded with an Intel Doctoral Student Honor Award. Her research is mainly focused on security aspects of mobile operating systems, such as Android, and security architectures for security sensitive mobile applications (such as online banking, access management, mobile payments and ticketing).

Secure elements for you and me: A model for programmable secure hardware in mobile ecosystems

Today, most smartphones feature different kinds of secure hardware, such as processor-based security extensions (e.g., TrustZone) and dedicated secure co-processors (e.g., SIM-cards or embedded secure elements). Unfortunately, the secure hardware is almost never utilized by commercial third party apps, although its usage would drastically improve their security. The reasons are diverse: Secure hardware stakeholders such as phone manufacturers and mobile network operators (MNOs) have full control over the corresponding interfaces and expect financial revenue; and the current code provisioning schemes are inflexible and impractical since they require developers to collaborate with large stakeholders.

To address these shortcomings, we propose a new code distribution model for mobile ecosystems which allows distribution of apps and their security sensitive subroutines realized in a form of Java applets. Our model leverages market-based code distribution environments (well-accepted for the distribution of mobile apps) to distribute Java applets. By leveraging market-based environments for the distribution of Java applets our scheme provides not only an easy way for third party developers to get their Java applets verified and signed by the secure element stakeholders, but also enables secure element stakeholders to allow installation of the applet against a fee, providing financial incentives to deploy our scheme. Further, our solution provides mechanisms to maintain dependencies between apps and their corresponding applets and to automatically configure OS-level access control to secure element APIs, eliminating dependency on OS vendors and phone manufacturers. These mechanisms are compatible with Global Platform (GP) specifications and can be easily incorporated into existing standards.

Dieter Vymazal

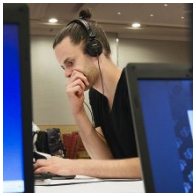
University of Applied Sciences Upper Austria (Hagenberg, Austria)

Dieter Vymazal is an Assistant Professor at the University of Applied Sciences Upper Austria. His main research interest is the analysis of malware especially focused on malware on mobile devices. Dieter gives courses on operating systems, networks, malware analysis and reverse engineering, and supervises several bachelor and master theses on malware analysis. As part of the Department for Secure Information Systems at the University of Applied Sciences Upper Austria he runs the Malware Lab Hagenberg that develops and maintains ANANAS, a framework for analyzing Android applications.

ANANAS – ANalyzing ANdroid ApplicationS

Android is an open software platform for mobile devices with a large market share in the smartphone sector. The openness of the system as well as its wide adoption lead to an increasing amount of malware developed for this platform. ANANAS is an expandable and modular framework for analyzing Android applications that takes care of common needs of dynamic malware analysis and provides a simple to use plugin interface. Six plugins representing well-known techniques for malware analysis have been developed for ANANAS. Five of the six plugins implement dynamic analysis methods, such as system call hooking and network traffic analysis.

ANANAS is integrated in a scalable analysis infrastructure that allows analysts to upload samples and to get a report which contains filtered analysis results gathered by the used analysis plugins within a few minutes. The ANANAS analysis infrastructure is operated by the malware lab at the University of Applied Sciences in Hagenberg and is used by an Austrian antivirus vendor who gives feedback on the practical usefulness of the system.



Victor van der Veen

VU University Amsterdam (Amsterdam, Netherlands)

Victor is a PhD candidate in the System and Network Security Group at the VU University Amsterdam where he also obtained his MSc. degree in Computer Science in August 2013. He is currently under the supervision of prof. dr. ir. Herbert Bos.
His research focuses on—but is not limited to—malware on smartphones and is part of the Dutch-American Project Arrangement about cooperative research and development on cybersecurity. Besides mobile malware, Victor is also interested in low-level system topics that enhance system security, as well as reverse engineering and analyzing malicious code. His previous work involves an in-depth analysis on trends in the field of memory errors.

How Google killed two-factor authentication

Exponential growth in smartphone usage combined with recent advances in mobile technology is causing a shift in (mobile) app behavior: application vendors no longer restrict their apps to a single platform, but rather add options that allow users to conveniently switch from mobile to PC or vice versa in order to access their services. This essentially removes the gap between multiple platforms. Many two-factor authentication (2FA) mechanisms, however, heavily rely on the existence of such separation. They are used in a variety of segments (such as consumer online banking services or enterprise secure remote access) to protect against malware. For example, with mobile-phone (TAN-based) 2FA in place, an attacker should no longer be able to use his PC-based malware to instantiate fraudulent banking transactions.

In this talk, I discuss how the ongoing integration and desire to increase usability results in violation of key principles for 2FA. In particular, I discuss the BAndroid vulnerability and show how it can be used to elevate a Man-in-the-Browser attack to takeover the user's mobile devices and, as a consequence, bypass the chain of mobile phone 2FA mechanisms as used by many financial services.

Federico Maggi

Politecnico di Milano (Milano, Italy)

Federico Maggi is a Assistant Professor at Dipartimento di Elettronica e Informazione, Politecnico di Milano in Italy, working at the NECST Laboratory. Specifically, his research interests are in analysis of malicious activity, Internet measurements and mobile malware. He is also actively involved in research projects funded by the European Union.
During his doctorate he studied and made contributions in the field of intrusion detection: he developed and tested anomaly-based tools to mitigate Internet threats by (1) avoiding their spread via vulnerable web applications, (2) detecting unexpected activities in the operating system's kernel (sing of malware infections or compromised processes), and (3) dealing with high number of alerts using alert correlation. Federico is instructor of the graduate-level course of computer security at Politecnico di Milano and has been invited in several venues to give lectures about his research work.

A walk through the construction of the first mobile malware tracker

In this talk I will start presenting the practical problem of analyzing the botnet activity of Android malware, describing how an Android bot typically works and which network primitives and transport they normally use. Next, I will introduce a little bit of the basics (theory and practice) necessary to start a simple static analysis to obtain the information that we need to analyize the botnet activity of a suspected bot. Then, I will show you how TraceDroid (presented in the previous talk) can be used to collect the very same information at runtime. After this, I will show you how we constructed a simple intelligence tool to correlate such collected information to provide a first, high-level ranking of the network endpoints that are potentially interesting C&C servers. I will conclude with a demonstration of the resulting tool, which our lab has recently released to the public as a web service. Remarkably, this tool has allowed us to discover malware-spreading campaigns targeting Chinese- and Korean-speaking bank customers.

Josef Ressel Center
for User-friendly Secure Mobile Environments

The Josef Ressel Center for User-friendly Secure Mobile Environments (u'smile) was founded in 2012 at the University of Applied Sciences Upper Austria, Hagenberg Campus—as the first JR Center serviced by the Christian Doppler Forschungsgesellschaft (CDG).

The goal of u'smile is the analysis of security issues in current and future mobile applications; the design, development, and evaluation of concepts, methods, protocols, and prototypical implementations for addressing them; and communication and co-ordination with industry partners and standardization organizations towards establishing globally accepted standards for secure, interoperable, mobile services.

Academic partners of u'smile are the Johannes Kepler University Linz (JKU) and SBA Research, a joint research institute operated by the Vienna University of Technology, the Vienna University of Economics, the University of Vienna, the Graz University of Technology, and the St. Pölten University of Applied Sciences.

The research center is funded through the Christian Doppler Forschungsgesellschaft from funds of the Federal Ministry of Science, Research and Economy (BMWFW) and the National Foundation for Research, Technology and Development, as well as by competent corporate partners: A1 Telekom Austria AG, Drei-Banken-EDV GmbH, LG Nexera Business Solutions AG, and NXP Semiconductors Austria GmbH. In 2015, Österreichische Staatsdruckerei GmbH joined the u'smile consortium—adding their long standing experience and knowledge of secure electronic documents.

René Mayrhofer

Johannes Kepler University (Linz, Austria)

René Mayrhofer heads the Institute of Networks and Security (INS) at Johannes Kepler University Linz (JKU), Austria, and the Josef Ressel Center on User-friendly Secure Mobile Environments (u'smile). Previously, he held a full professorship for Mobile Computing at University of Applied Sciences Upper Austria, Campus Hagenberg, a guest professorship for Mobile Computing at University of Vienna, and a Marie Curie Fellowship at Lancaster University, UK. His research interests include computer security, mobile devices, network communication, and machine learning, which he brings together in his research on securing spontaneous, mobile interaction. René has contributed to over 60 peer-reviewed publications and is a reviewer for numerous journals and conferences. He received Dipl.-Ing. (MSc) and Dr. techn. (PhD) degrees from Johannes Kepler University Linz, Austria and his Venia Docendi for Applied Computer Science from University of Vienna, Austria.

Edgar Weippl

SBA Research (Vienna, Austria)

After graduating with a Ph.D. from TU Wien, Edgar worked in a research startup for two years. He then spent one year teaching as an Assistant Professor at Beloit College, WI. From 2002 to 2004, while with the software vendor ISIS Papyrus, he worked as a consultant in New York, NY and Albany, NY, and in Frankfurt, Germany. In 2004 he joined the TU Wien and founded the research center SBA Research together with A Min Tjoa and Markus Klemen. Edgar R. Weippl (CISSP, CISA, CISM, CRISC, CSSLP, CMC) is member of the editorial board of Computers & Security (COSE), organizes the ARES conference and is General Chair of SACMAT 2015, PC Chair of Esorics 2015 and General Chair of ACM CCS 2016.

Michael Roland

University of Applied Sciences Upper Austria (Hagenberg, Austria)

Michael Roland is a post-doc researcher at the Josef Ressel Center for User-friendly Secure Mobile Environments (u'smile) of the University of Applied Sciences Upper Austria at Hagenberg, Austria. His main research interests are NFC, security and Android. He is the creator of NFC TagInfo, one of the first and most successful NFC developer tools for Android devices, and co-author of the book 'Anwendungen und Technik von Near Field Communication (NFC)'. He holds a B.Sc. and a M.Sc. degree in Embedded Systems Design (University of Applied Sciences Upper Austria, 2007 and 2009) and a Ph.D. (Dr. techn.) degree in Computer Science (Johannes Kepler University Linz, Austria, 2013).

HAGENBERG | LINZ | STEYR | WELS

FH OÖ Forschungs & Entwicklungs GmbH
Josef Ressel Center u'smile

u'smile

Softwarepark 11
4232 Hagenberg | Austria
Phone: +43 50804-27149
Fax: +43 50804-27199
office@usmile.at
www.usmile.at
www.fh-ooe.at
/fhooe.at

FH OBERÖSTERREICH
UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

Forschungsland OBERÖSTERREICH