PROGRAM
ANDROID SECURITY SYMPOSIUM

8th – 10th March 2017
Vienna, Austria

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

u'smile

https://usmile.at/symposium

FH OBERÖSTERREICH UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

SBA Research

INSTITUTE OF NETWORKS AND SECURITY

JKU JOHANNES KEPLER UNIVERSITÄT LINZ

Welcome

We welcome you to the Second 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 analysis methods, app development, and cloud security.

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 with usable, secure hardware and software in mobile devices with a particular focus on Android smart phones. Five 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 was made possible with the help of our sponsors Energie AG Oberösterreich Telekom, eshard, Google, and Grant Thornton. We are also thankful for support by our three host institutions: University of Applied Sciences Upper Austria in Hagenberg, SBA Research, and Johannes Kepler University Linz with its Institute of Networks and Security.

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.

u'smile

Dr. Michael Roland Prof. Dr. René Mayrhofer Priv.-Doz. Dr. Edgar Weippl

Sponsors

Coffee Break Sponsor

Grant Thornton
An instinct for growth™

Silver Sponsors

ENERGIE AG Telekom
Wir denken an morgen

eshard

Google

Media Partners

concise cybersecurity

Smart Insights

Program

Wednesday	Thursday	Friday
Welcome speech		
Security architectures and security hardening	Developing secure apps	Secure positioning
		Analysis methods
Lunch and networking break		
User identity and cloud security	Developing secure apps	Analysis methods
		Memory attacks
Managing threats	Assessing app security	

Wednesday, 8th March 2017

08:30	**Registration**
09:15	**Welcome speech**
	Security architectures and security hardening
09:30	**Honey, I shrunk the attack surface – Adventures in Android security hardening** Nick Kralevich Google (USA)
10:30	**Coffee break**
11:00	**AT&T efforts to improve the distribution of Android security updates** Patrick McCanna AT&T (USA)
12:00	**Lunch and networking break**
	User identity and cloud security
13:30	**Using threshold crypto to protect single users with multiple devices** Erinn Atwater University of Waterloo (Canada)

14:15	**Privacy with Cryptomator:** **End-to-end cloud encryption – User-friendly and Open Source** Christian Schmickler and Markus Kreusch Skymatic (Germany)
15:00	Coffee break

Managing threats

15:30	**Building threat models for the mobile ecosystem** Joshua M. Franklin NIST (USA) Michael Peck The MITRE Corporation (USA)
16:15	**Lifting all boats: getting developers to improve app security** Hans-Christoph Steiner Guardian Project (Austria)
17:00	Closing of day

Thursday, 9th March 2017

08:30	Registration
09:15	Welcome speech

Developing secure apps

09:30	**An introduction to Android application security testing** Nikolay Elenkov LINE (Japan)
10:30	Coffee break
11:00	**What's NNNNNNew in Android Security?** Scott Alexander-Bown Freelance Android developer (United Kingdom)
12:00	Lunch and networking break
13:30	**Playing with your code: a new approach to avoid potential hackers from doing exactly this!** Hugues Thiebeauld eshard (France)
14:00	**Pinning: Not as simple as it sounds** John Kozyrakis Synopsys (United Kingdom)
14:55	Coffee break

Assessing app security

15:25	**Assessing and improving mobile application security** Michael Peck and Carlton Northern The MITRE Corporation (USA)
16:10	**State of security of Android banking apps in Poland** Tomasz Zieliński PGS Software S.A. (Poland)
17:00	**Closing of day**

Friday, 10th March 2017

08:30	**Registration**
09:15	**Welcome speech**

Secure positioning

09:30	**Secure positioning: From GPS to IoT** Srdjan Capkun ETH Zurich (Switzerland)
10:30	**Coffee break**

Analysis methods

11:00	**Android compiler fingerprinting** Tim Strazzere and Caleb Fenton RedNaga (USA)
12:00	**Lunch and networking break**
13:30	**Statistical deobfuscation of Android applications** Petar Tsankov ETH Zurich (Switzerland)

Memory attacks

14:15	**Drammer: Flip Feng Shui goes mobile** Victor van der Veen Vrije Universiteit Amsterdam (Netherlands)
15:00	**Closing of day**

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 8 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.

Honey, I shrunk the attack surface – Adventures in Android security hardening

Information security is ever evolving, and Android's security posture is no different. Users and application developers have high expectations that their data will be kept safe, private, and secure, and it's the responsibility of the Android Security Team to enable this. To do this, Android has focused on four critical principles of information security: exploit mitigation, exploit containment, attack surface reduction, and safe-by-default features.

In this talk, we will discuss Android's attack surface reduction history, and how that fits into the broader Android security story. We will go into detail on the specific technical strategies used to achieve the attack surface reduction, and explore specific bugs which were made unreachable as a result of the hardening over the last several years. And we will examine the overall result of the hardening, and areas for improvement.

Patrick McCanna

AT&T (Redmond, WA, USA)

Patrick has been responsible for mobile security at AT&T since 2004. Patrick started his employment by establishing security operations teams dedicated to mobility networks & services. He currently supports the Mobile Endpoint Security Team, where he leads efforts to ensure the security of AT&T's portfolio of mobile devices. He is a board member on AT&T's bug bounty. Patrick leads AT&T's sponsorship of r00tz Asylum—a nonprofit dedicated to teaching kids around the world how to love being white-hat hackers. Patrick has a B.S. in Computer Science with a Mathematics minor from Linfield College.

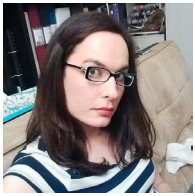
AT&T efforts to improve the distribution of Android security updates

PC's get patches every month. Apple has been very efficient in creating and distributing security patches. The AOSP source is updated regularly. Why was there such a delay in distributing security patches in Android? Should not it be easy to distribute the AOSP source changes as updates to launched devices?

Starting in 2015, AT&T changed it's procedures to enable a rapid distribution of security updates. These changes allowed OEMs to rapidly distribute security updates after the Stagefright discovery. In this talk, we'll discuss what was delaying security updates in the past & the changes that allowed for rapid distribution of security updates during that urgent event. We'll also discuss AT&T's recent 2G sunset and features necessary for the future of secure mobile communication.

Android has provided us with security lessons that are applicable beyond the mobile industry. Industrial IoT, Connected home, Car & city solutions all can benefit in this discussion on the challenge of distributing open source software security updates to proprietary hardware.

Erinn Atwater



University of Waterloo (Waterloo, ON, Canada)

Erinn is currently in the last year of her PhD in Computer Science at the University of Waterloo, where she is a member of the Cryptography, Security and Privacy (CrySP) lab and the Centre for Applied Cryptographic Research.

Her research interests span a variety of topics, mostly revolving around the obstacles that prevent widespread deployment of end-to-end encryption. Her thesis includes work on usable encrypted webmail and protecting keys across multiple devices. In the past, she has also worked on machine learning for behavioural authentication on smartphones, and genetic programming for classification of high-volume online data streams.

Using threshold crypto to protect single users with multiple devices

The average computer user is no longer restricted to one device. They may have several devices and expect their applications to work on all of them. A challenge arises when these applications need the cryptographic private key of the devices' owner. Here the device owner typically has to manage keys manually with a “keychain” app, which leads to private keys being transferred insecurely between devices – or even to other people. Even with intuitive synchronization mechanisms, theft and malware still pose a major risk to keys. Phones and watches are frequently removed or set down, and a single compromised device leads to the loss of the owner's private key, a catastrophic failure that can be quite difficult to recover from.

We introduce Shatter, an open-source framework that runs on desktops, Android, and Android Wear, and performs key distribution on a user's behalf. Shatter uses threshold cryptography to turn the security weakness of having multiple devices into a strength. Apps that delegate cryptographic operations to Shatter have their keys compromised only when a threshold number of devices are compromised by the same attacker. We demonstrate how our framework operates with three popular Android apps (protecting identity keys for Signal and OTR apps, and encryption keys for a note-taking app) in a backwards-compatible manner: only Shatter users need to move to a Shatter-aware version of the app. Shatter has minimal impact on app performance, with signatures and decryption being calculated in only seconds.

Christian Schmickler

Skymatic/Cryptomator (Bonn, Germany)

Christian Schmickler is managing partner at Skymatic and responsible for communications and marketing.

Before joining the Cryptomator project, he worked as a systemic consultant for a German consultancy. He holds a master's degree in International Business from Maastricht University and bachelor's degrees in economic sciences and psychology.

Markus Kreusch

Skymatic/Cryptomator (Bonn, Germany)

Markus Kreusch is managing partner at Skymatic, the startup behind Cryptomator. At Skymatic he is responsible for the Cryptomator app for Android and supports the development of the desktop application and crypto libraries. Prior to his work at Skymatic he worked as a software architect and IT consultant. In this role he got insights into prominent German companies. He graduated extra-occupational at FOM University of Applied Sciences and currently studies applied computer sciences at University of Hagen.

Privacy with Cryptomator: End-to-end cloud encryption – User-friendly and Open Source

Current and past political events have initiated an extensive discussion on privacy and informational self-determination. The vast majority of consumers states their desire to keep personal data private while in everyday life, they use services and approve privacy agreements that undermine their informational self-determination on a large scale. This contradiction is referred to as the privacy paradox. While there are tools designed to keep personal data private, employing such tools is often associated with reduced functionality and/or usability and new privacy issues resulting from their use. Such deficiencies inhibit their widespread use.

Cloud storages are one example for a privacy-critical infrastructure as personal data is distributed across a broad network while the location of storage is often out of the user's control. Client-side (end-to-end) encryption is a valid way to protect those data independent of security measures taken by the cloud provider and its privacy agreements. However, existing tools—e.g., for disk or file encryption—do not work seamlessly with the cloud.

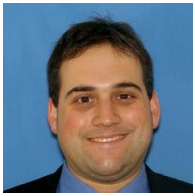
The idea behind Cryptomator is to make cloud encryption as user-friendly, transparent, and understandable as possible to enable everyone to protect their data. In their talk, the developers of Cryptomator emphasize the importance of privacy in our information society in general and the significance of sophisticated and user-friendly tools to empower everyone to safeguard their privacy in particular. The general idea behind Cryptomator, its encryption scheme and challenges when targeting the cloud will be outlined. In addition, the architecture of the app for Android and future development plans will be illustrated.

Joshua M. Franklin

NIST (Gaithersburg, MD, USA)

Joshua M. Franklin is an information security engineer at NIST, focusing on enterprise mobile security, cellular security, and electronic voting. He graduated from George Mason University with an M.S. in Information Security & Assurance, and received a B.S. in Information Systems from Kennesaw State University. Joshua participates in numerous mobile security working groups and standards efforts, such as 3GPP and Communications Security, Reliability and Interoperability Council (CSRIC), part of the Federal Communications Commission (FCC).

Michael Peck



The MITRE Corporation (McLean, VA, USA)

Michael Peck is a security engineer at The MITRE Corporation, where he primarily focuses on mobile device security, mobile application security, and network security protocols and standards. He holds an M.S. in Security Informatics from Johns Hopkins University and a B.S. in Computer Science from the University of Virginia.

Building threat models for the mobile ecosystem

Mobile devices and the surrounding mobile ecosystem face many security threats. This presentation will provide an in-depth discussion and analysis of NIST's National Cybersecurity Center of Excellence's (NCCoE) efforts to enumerate and model these threats, resulting in our Mobile Threat Catalogue and a mobile profile of MITRE's ATT&CK model.

NCCoE's mobile security efforts are dedicated to solving enterprise mobile security challenges. In talking with mobile security stakeholders, we realized there was a need for a comprehensive catalog of threats posed to mobile devices. The resulting Catalogue outlines a taxonomy of threats, including those faced by a mobile device itself as well as the broader mobile ecosystem upon which the device depends. Each Catalogue entry includes a title, exploit examples, countermeasures, and references. The Catalogue resides on GitHub, enabling public collaboration and continuous development.

The NCCoE and MITRE have augmented the Catalogue by building a mobile-specific version of MITRE's ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) model. The mobile ATT&CK model depicts tactics and techniques used by adversaries to gain initial access to a mobile device and then take advantage of that access to accomplish adversarial objectives.

We will discuss how our work can benefit mobile security stakeholders, including enabling stakeholders to depict strategies used in adversarial campaigns, identify defensive gap areas, implement countermeasures, and determine effective security testing strategies.

Hans-Christoph Steiner

Guardian Project (Vienna, Austria)

Hans-Christoph Steiner spends his time making private software usable, designing interactive software with a focus on human perceptual capabilities, building networks with free software, and composing music with computers. With an emphasis on collaboration, he has worked in many forms, including free software for mobile and embedded devices, responsive sound environments, free wireless networks that help build community, musical robots that listen, programming environments allow people to play with math, and a jet-powered fish that you can ride.

Lifting all boats: getting developers to improve app security

There are many proven techniques for protecting data, providing strong authentication, etc. but actually delivering secure software is often tedious and error prone. On Android it is even worse since most devices rarely get updates, leaving years of open issues across the spectrum of devices that are in use. Guardian Project develops mobile apps for high risk users, such as journalists and human rights activists, that deal with this landscape. Those techniques that we developed are then bundled up into free, easy to use libraries. All of our work is user driven, so we also research the user experience of developers, to learn what are the actual barriers for getting developers to improve app security.

Security is rarely given priority in software development, so in order get developers to use secure practices, the libraries must fit in with their existing knowledge, with minimal technical risk. So our libraries use APIs that developers already know (e.g. android.database.*, java.io.*) so the ramp up time for developers is really fast. This talk will also give a quick overview of our suite of libraries, including SQLCipher-for-Android, private file stores, and hardened network connections. Then short discussion of examples including sample code, real world apps that use these libraries, and UI/UX patterns that work well.

Nikolay Elenkov

LINE (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 Android's initial public release and is the author of Android Security Internals.

He currently works at LINE's Security department.

An introduction to Android application security testing

This presentation will provide a brief introduction to Android application security testing, and highlight some essential tools and methods for analyzing Android applications.

We will cover static analysis, network traffic analysis, different methods for obtaining app data, as well as several techniques for dynamic analysis and method hooking. Finally, we will highlight some of the more common vulnerabilities found in Android applications, and provide hints to help spot them quickly.

Scott Alexander-Bown

Freelance Android developer (Bristol, United Kingdom)

Scott is a consultant Android developer and Google Developer Expert for Android who is passionate about mobile app security. He is co-author of “The Android Security Cookbook”, speaks at various conferences on the subject and has released several security related open source libraries.

In 2011, Scott founded and continues to co-run SWmobile meetup group based in Bristol/Bath (UK). Mobile professionals can meet and share knowledge at the monthly tech talk/social events.

To relax and bug out from the screen Scott enjoys spending time with his wife and children, running, Mexican food, craft beer and science fiction.

What's NNNNNNew in Android Security?

Android N brings a plethora of security enhancements to the platform and the SDK. Including Network Layer Security, Hardware-backed Keystore verification, APK Signing v2, Scoped Directory Access and Direct Boot. Come to this talk to get a concise update on the new features, practical tips and examples of how to implement in your app today! (if your minSDK isn't 24)

Hugues Thiebeauld

eshard (Bordeaux, France)

Hugues Thiebeauld is CEO at eshard, a start-up focusing on security of mobile applications and IoT. Prior to founding the company (in 2015), he worked as security lab manager at UL, where he was responsible for growing the security evaluation lab and manage its accreditations. Using his technical expertise in attack techniques and his knowledge of the industry, he successfully built a team of experts (50+) located in 3 different regions (UK, France and Singapore). Prior to UL, Hugues worked at Oberthur and Thales in various cryptography and security evaluation related roles.

Playing with your code: a new approach to avoid potential hackers from doing exactly this!

eshard, a start-up in the field of mobile security and IoT, provides expert security advice and tools to secure mobile applications and other connected devices. Our aim is to facilitate the development process of mobile applications in order to achieve the right level of security. However, how can you know that the correct security protections have been implemented? How can you gain assurance that no one is able to play with your binary code?

Today, there is no other choice than inspecting codes manually, which takes a lot of time and effort. Also, it seems checking the level of security is always described as an area for experts only. Therefore, many companies choose not to double-check the right implementation of security protections. This may lead to weaknesses in the level of security, which is undesirable.

In this twenty minute presentation, eshard will explain how analyzing binary codes can be done in a more efficient and cost-effective way, and how those questioning the security of an implementation can benefit from this. Furthermore, we explain how we try to ‘break free’ from the established way of looking at security in mobile applications.

John Kozyrakis

Synopsys (London, United Kingdom)

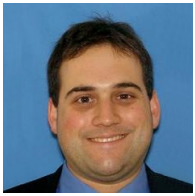
John is a security engineer and researcher in the area of mobile application security. He has helped several large organizations threat model their apps and design or evaluate sophisticated defensive controls such as binary hardening and certificate pinning. He also develops automated static and dynamic analysis solutions for Android applications. John holds an MSc in Information Security from Royal Holloway, University of London and an Electrical and Computer Engineering diploma from University of Patras.

Pinning: Not as simple as it sounds

Certificate pinning trends perennially, coming to the fore with each new SSL hack. Security urges developers to implement pinning and many mobile apps do—some applying pinning to problems it doesn't solve while others do so entirely unnecessarily.

Taking a perspective useful to both developers and testers, this presentation highlights the threats that pinning can tackle and covers the tradeoffs inherent in pinning decisions. The presentation explores several flaws found in real applications and describes changes introduced in recent Android versions.

Expect to leave understanding common implementations mistakes, common misconceptions and key subtleties of pinning that may in fact decrease security or impose undue complexity.



Michael Peck

The MITRE Corporation (McLean, VA, USA)

Michael Peck is a security engineer at The MITRE Corporation, where he primarily focuses on mobile device security, mobile application security, and network security protocols and standards. He holds an M.S. in Security Informatics from Johns Hopkins University and a B.S. in Computer Science from the University of Virginia.

Carlton Northern

The MITRE Corporation (McLean, VA, USA)

Carlton Northern is a mobile security engineer at The MITRE Corporation. While at MITRE he has helped various U.S. DoD and other federal agencies deploy secure mobile solutions over a range of use cases. Carlton has also been an active member of the Trusted Computing Group where he contributed to the TPM Mobile specification. Currently, Carlton is working with the U.S. Army Training and Doctrine Command where he has helped deploy a training and educational app store for the Army, overcoming issues of application security and BYOD.

Building threat models for the mobile ecosystem

Many enterprises are seeking commercial solutions to perform security vetting of mobile applications for exploitable vulnerabilities and suspicious behaviors. We will discuss an analysis performed by MITRE in 2016 of the effectiveness of app security vetting solutions, including discussion of their overall strengths and weaknesses. As part of the analysis, we developed solution criteria based on NIAP's Protection Profile for Application Software, and we created Android and iOS applications with deliberately inserted vulnerabilities and suspicious behaviors. Our work may help others faced with assessing the security of mobile applications.

Next, we'll discuss a MITRE research project into tools and techniques for improving Android application security. We developed static analysis checks for the Android Lint tool built in to Android Studio and the Android Software Development Kit (SDK). The static analysis checks, accepted by the Android Open Source Project, enable app developers and security analysts to identify and eliminate several common Android app vulnerabilities up-front in the software development lifecycle. We'll also discuss our attempt to propose changes to the Android operating system's SELinux mandatory access control policies and other security architecture elements to address application security vulnerabilities and misbehaviors.

Tomasz Zieliński

PGS Software S.A. (Wrocław, Poland)

Tomasz Zieliński—Android team lead at PGS Software. In the past he maintained financial systems at National Bank of Poland, developed Bing at Microsoft, helped in production of Angry Birds and cared for embedded software for trams and buses. He used to be a public data re-use activist, in 2012 he was invited by European Commision to speak in Brussels about his experience of re-use of public transport data in Poland. Graduated from University of Wrocław. Active paraglider pilot.

State of security of Android banking apps in Poland

In the 2nd half of 2016 we reviewed 20 Android banking applications, released and maintained by banks operating in Poland. We found a number of problems, ranging from minor errors in APK packaging, through data loading via insecure connection, lack of certificate pinning, exported activities, debug code present in apps, leak of session token, up to session takeover and user data exposure. Presentation will cover observed vulnerabilities. I will also tell you about the process of contacting bank's security departments and responsible disclosing of sensitive information. If time allows, we will investigate implications of using 3rd party services like Crashlytics or Facebook SDK.

Srdjan Capkun

ETH Zurich (Zurich, Switzerland)

Srđan Čapkun is a Full Professor in the Department of Computer Science, ETH Zurich and Director of the Zurich Information Security and Privacy Center (ZISC). He was born in Split, Croatia. He received his Dipl.Ing. Degree in Electrical Engineering / Computer Science from the University of Split in 1998, and his Ph.D. degree in Communication Systems from EPFL in 2004. Prior to joining ETH Zurich in 2006 he was a postdoctoral researcher in the Networked & Embedded Systems Laboratory, University of California Los Angeles and an Assistant Professor in the Informatics and Mathematical Modelling Department, Technical University of Denmark. His research interests are in system and network security. One of his main focus areas is wireless security. In 2016 he received an ERC Consolidator Grant for a project on securing positioning in wireless networks.

Secure positioning: From GPS to IoT

In this talk I will review security issues in today's navigation and close-range positioning systems. I will discuss why GNS systems like GPS are hard to fully secure and will present novel solutions that can be used to improve the robustness of GNS systems to attacks. I will then show how a different design of a positioning system can enable secure positioning, but also that this requires solving a set of relevant physical- and logical- layer challenges. Finally, I will present a design and implementation of a fully integrated IR UWB secure distance measurement (distance bounding) system that solves these challenges and enables secure distance measurement and secure positioning in IoT applications.

Tim Strazzere

RedNaga (Oakland, CA, USA)

Tim “diff” Strazzere is the Security Engineer at Cloudflare, specializing in mobile and linux security. Along with writing security automation software, he specializes in reverse engineering and malware analysis. Some interesting past projects include having reversed the Android Market protocol, Dalvik decompilers and memory manipulation on mobile devices. Past speaking and training engagements have included DEFCON, BlackHat, SyScan, HiTCON and EICAR, QSPI.

Caleb Fenton

RedNaga (Oakland, CA, USA)

Caleb Fenton is a security researcher at SentinelOne and has spent the past 6 years reversing Android apps and researching malware. He's created or maintains several open source Android reverse engineering and anti-malware tools such as Simplify and dex-oracle (Android deobfuscators), smalivm (Smali emulator / virtual machine), and APKiD (PEiD for Android).

Android compiler fingerprinting

Compiler fingerprinting is a technique for identifying the compiler used to create an executable. Executable file formats are usually flexible and different compilers may introduce subtle differences in structure and organization. We have developed a tool called APKiD which can determine the compiler used to create or modify Dalvik executables and Android binary XML files. This allows us to distinguish between apps compiled from the original source code and apps which have been modified using non-standard compilers such as dexlib. We believed the two main reasons for modifying an Android app were for 1.) cracking and piracy and 2.) injecting malicious code. We tested this belief by comparing the compiler profiles of various app markets with different tolerances for cracked or malicious apps to see if the percentage of modified apps was inversely proportional to how strict the store was about policing submissions. We found that strict markets such as Google Play had significantly lower rates of modified apps compared to less strict markets such as Aptoide and BlapkMarket. Additionally, we analyzed ~138,000 benign apps and known malware samples to compare the rates of modification between both groups. We found much higher rates of modification for malware than with benign apps. Thus, knowing if an app is modified seems to be a good signal for maliciousness or software piracy.

This talk presents the history and evolution of various Android compilers, introduces APKiD, summarizes the technical details for how APKiD works, and reviews applications for using compiler fingerprinting to improve detection and classification of malware and pirated apps.

Petar Tsankov

ETH Zurich (Zurich, Switzerland)

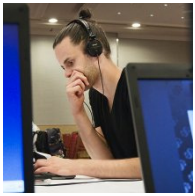
Petar Tsankov is a security researcher at the Software Reliability Lab at ETH Zurich. The goal of his research is to make it easier for developers who are not security experts to build secure and reliable systems. Towards this goal, he combines novel techniques from Programming Synthesis, Machine Learning, and Probabilistic Programming to build new practical systems that solve important problems in Information Security.

Statistical deobfuscation of Android applications

In this talk, I will present DeGuard (www.apk-deguard.com), a new system for deobfuscating Android APKs based on probabilistic learning from large code bases. DeGuard learns a probabilistic model over thousands of non-obfuscated Android applications and uses this model to deobfuscate new, unseen Android APKs. DeGuard effectively reverses the process of layout obfuscation, the most common obfuscation mechanism for Android applications, which renames key program elements such as classes, packages, and methods, thus making it difficult to understand what the application does.

To make this possible, DeGuard phrases the layout deobfuscation problem of Android APKs as a structured prediction in a probabilistic graphical model. I will describe DeGuard's probabilistic model, along with the rich set of features and constraints for Android that ensure both semantic equivalence and high prediction accuracy. I will present experiments that demonstrate that DeGuard is useful in practice: it recovers 79.1% of the program element names obfuscated with ProGuard, it predicts third-party libraries with an accuracy of 91.3%, and it reveals string decoders and classes that handle sensitive data in Android malware.

Victor van der Veen



Vrije Universiteit Amsterdam (Amsterdam, Netherlands)

Victor is a PhD candidate in the System and Network Security Group (VUSec) at Vrije Universiteit Amsterdam where he also obtained his MSc degree in Computer Science in August 2013. He is currently under the supervision of dr. Cristiano Giuffrida and 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.

Drammer: Flip Feng Shui goes mobile

Rowhammer is a hardware bug that allows attackers to manipulate data in memory without accessing it. More specifically, by reading many times from a specific memory location, somewhere else in memory a bit may flip (a one becomes a zero, or a zero becomes a one). Flip Feng Shui—or FFS—is a technique that allows for reliable exploitation of the Rowhammer vulnerability by combining it with a memory massaging primitive to land sensitive data on a vulnerable location.

In this talk, I present Drammer: a new attack that exploits the Rowhammer hardware vulnerability on Android devices. As an instance of the Flip Feng Shui exploitation technique, it is the first Android root exploit that does not rely on any software vulnerability.

By discussing the requirements for FFS, I first provide an introduction to reliable Rowhammer exploitation. In the second part of my talk, I show how flipping a single bit is enough for Drammer to get root access on an Android device. Note that this will be a highly technical talk: you will learn about page tables and the buddy allocator. **Fun guaranteed!**

u'smile

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 at Hagenberg—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 University of Applied Sciences Upper Austria at Hagenberg, SBA Research, and Johannes Kepler University Linz. The research center is funded through CDG 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, NXP Semiconductors Austria GmbH, and Österreichische Staatsdruckerei GmbH.

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 for User-friendly Secure Mobile Environments (u'smile). Previously, he held a full professorship for Mobile Computing at University of Applied Sciences Upper Austria at 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 70 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.

Michael Roland

University of Applied Sciences Upper Austria (Hagenberg, Austria)

Michael Roland is post-doctoral researcher at the University of Applied Sciences Upper Austria at Hagenberg. There, he is a member of Josef Ressel Center for User-friendly Secure Mobile Environments (u'smile) and the Research Group Embedded Systems. His main research interests are NFC, smartcards and Android with focus on security and privacy. He is the creator of NFC TagInfo, one of the first NFC developer tools for Android devices, and co-author of the book "Anwendungen und Technik von Near Field Communication (NFC)". He has a B.Sc. and an 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).

Edgar Weippl

SBA Research (Vienna, Austria)

After graduating with a Ph.D. from the 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, General Chair of ACM CCS 2016, and PC Chair of ACM SACMAT 2017.

Venue

Vienna University of Technology
Technische Universität Wien

Room: Kuppelsaal (3rd floor)

Karlsplatz 13
1040 Vienna
Austria

www.tuwien.ac.at

Wi-Fi

SSID: tuguestnet

You find the username and the password for access to the Wi-Fi network on your participant badge.

Passwords consist of digits and lower-case letters only.

ANDROID SECURITY SYMPOSIUM

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

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

SBA Research gGmbH

Favoritenstraße 16
1040 Vienna | Austria
www.sba-research.org
/sbaresearch

Johannes Kepler University Linz
Institute of Networks and Security

Altenberger Straße 69
4040 Linz | Austria
www.ins.jku.at
www.jku.at
/jku.edu

FH OBERÖSTERREICH UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA
SBA Research
INSTITUTE OF NETWORKS AND SECURITY
JKU JOHANNES KEPLER UNIVERSITÄT LINZ