Qualcomm Mobile Security Summit 2015, April 30 & May 1

Sessions on April 30 will be held in Qualcomm Building N at 5775 Morehouse Dr., San Diego, California.
Sessions on May 1 will be held in Qualcomm Building Q at 6455 Lusk Blvd., San Diego, California.

To request an invitation, please contact secsummit@qualcomm.com.

Agenda:

Thursday, April 30, 2015 – Summit Presentations

Attackgraphy

"Think like an attacker. For many people, that's as hard as thinking like a professional chef." - Adam Shostack. The ever-growing requirements of technological innovations in mobile devices have rocketed the growth of the mobile threat landscape for attackers and security researchers. As a result, developers and engineers are pressured into fast-paced release cycles that do not accommodate for in-depth security testing.

A duo of MWR Labs winners of mobile Pwn2Own 2014 aim to engage the audience with a fresh perspective on how attackers are targeting Android devices. Various remote attack vectors will be discussed, ranging from leveraging application vulnerabilities through to advanced attack chains. To illustrate the mindset and methodology employed by attackers, a case study that contained three 0-day vulnerabilities used to achieve full remote code execution on the Amazon Fire Phone from a malicious access point will be displayed.

Speaker Bios

Bernard Wagner is an information security consultant at MWR InfoSecurity and a specialist in mobile security. He was part of the team that won the mobile application category at Mobile Pwn2Own 2014. He is a qualified computer engineer who has contributed to the open-source mobile security testing framework drozer. Outside of security, he has a background in image processing and mechatronics.

Kyle Riley is an information security consultant at MWR InfoSecurity. He has a background in computer engineering. His research interests focus on embedded systems and mobile platforms. He formed part of a team that won the mobile application category of Mobile Pwn2Own 2014 in Tokyo, Japan. He developed an offensive vulnerability search tool that was integrated into Maltego and launched at Blackhat 2013 in Las Vegas, USA.

Digging for Android Kernel Bugs

Since Android 4.4, SELinux is enforced by default and efficiently mitigated threats from user space. However, by attacking the kernel, an attacker can still obtain full system control. In this presentation we are going to discuss tools and methods we used to discover multiple kernel vulnerabilities in commercial

devices. Although Linux kernel is GPL licensed, not all mobile device vendors properly release kernel source code to public. Delayed or incomplete/inaccurate releases are common, especially for our domestic manufacturers. We are going to discuss both situations, so the methods and techniques will be suitable for both device manufactures and external researchers. We will also analyze some of the bugs we found and discuss how to prevent them in further development.

Speaker Bios

James Fang is co-founder and a researcher of Keen Team. He has been working on multiple research projects and for the past year he was mostly focusing on Android kernel vulnerabilities and exploitation. Before founding the team James was working for Microsoft and was involved in vulnerability report responding and Bing safe search initiatives.

Sen Nie is a researcher of Keen Team. His research mainly focuses on program analysis, like symbolic execution and smart fuzzing technology. He's currently a Ph.D Candidate of Shanghai Jiao Tong University.

Mobile Malware: A Network View

Mobile devices are becoming the target of choice for cybercriminals. This presentation will provide an in-depth view on the mobile malware that is currently active on the Internet, how it is monetized and the impact it has on network resources and the user experience. The presentation will draw on network-based malware detection results from deployments in major mobile carriers around the world.

Alcatel Lucent's network-based malware detection system is deployed in major mobile carriers in the U.S., Europe, Asia and the Middle East. It uses DPI technology to detect malware command and control traffic to identify the malware infection. Aggregated statistics on the infection rates for malware in these networks has been reported in regular quarterly malware reports (http://www.alcatel-lucent.com/solutions/malware-reports). This presentation will leverage the most recent aggregated information from these deployments.

Speaker Bio

Kevin McNamee is director of Alcatel-Lucent's Motive Security Labs and is responsible for the security research team that supports Alcatel-Lucent's cloud-based malware detection system. Previously he was director of security research at Alcatel-Lucent's Bell Labs specializing in the analysis of malware propagation and detection. He has recently presented at RSA, BlackHat, (ISC)2 and SECTOR.

Testing WCDMA and LTE Mobile Stacks

With the development of more and more hardware and software projects related to wireless communications, it is becoming always more affordable for auditors to test the implementation of 3G (WCDMA) and LTE mobile stacks and modems. This can lead to interesting findings on how the mobile security procedures are implemented in basebands.

In 2013 and 2014, some errors and bugs were discovered while evaluating few terminals against the basic procedures described in 3GPP standards. Some of them could allow the hijacking of the 3G or LTE connection, whereas some other just lead to surprising behaviors. This will be related in the presentation.

Speaker Bio

Benoit Michau works for the French administration, on its secure mobile communication means, after working seven years for France Telecom-Orange and attending 3GPP SA3 for three years.

Practical and Efficient Exploit Mitigation for RISC-based Embedded Devices

We present a novel approach for exploit mitigation that is specifically tailored toward embedded systems that are based on the common RISC architecture. We leveraged architectural features of RISC CPUs to extract a combination of static and dynamic properties relevant to OS service requests from executables, and enforces them during runtime. Our technique borrows ideas from several areas including control flow integrity, system call monitoring, static analysis, and code emulation, and combines them in a low-overhead fashion directly in the operating system kernel. We implemented our approach for the Linux operating system.

Our system is very practical, and restricts the ability of attackers to exploit generic memory corruption vulnerabilities in COTS binaries. In contrast to other approaches, we do not require access to source code, binary modification, or application specific configuration such as policies. Our evaluation demonstrates that our approach incurs a very low overhead—only 2%—and shows that our approach is practical against both code injection and code reuse attacks.

Speaker Bios

Collin Mulliner is a postdoctoral researcher in the Systems Security Lab at Northeastern University. Collin's main interest is the security and privacy of mobile and embedded systems with an emphasis on mobile and smart phones. Since 1997 Collin worked on all kinds of mobile devices and touched most of the mobile platforms for either software development or security work. Collin received a Ph.D. from the Technische Universitaet Berlin in 2011, and a M.S. and B.S. in computer science from UC Santa Barbara and FH-Darmstadt, respectively. Collin has a broad interest in systems security that is somehow connected to mobile devices and cellular infrastructure. He has a specific interest in vulnerability analysis and offensive security. Recently he switched his focus to the defensive side to work on mitigations and countermeasures.

Matthias Neugschwandtner received his D.Sc. degree from Vienna University of Technology in 2014, where he worked at the Secure Systems Lab. He joined the System and Network Security Group at the Vrije Universiteit Amsterdam as a visiting researcher in 2011, and the Northeastern University Systems Security Lab in Boston in 2013. As of April 2015 he is with the Cloud and Storage Security Group at IBM Research, Zürich. The main focus of his research lies on low-level system security. This encompasses program analysis, vulnerability detection and system hardening.

Android App “Protection”

The Android ecosystem is full of interesting types of “protection” for applications; packers, obfuscators, and tools to mangle everything in between. Between Jon Sawyer and myself, we’ve both implemented, and had to defeat, an entire array of these tools; originally we presented Android Hacker Protection Level 0 at DEFCON 2014. Since then, most of these tools have attempted to update themselves to evade the last publication to talk about breaking them. These tools must be understood and handled by the entire ecosystem since they’re used by people releasing malware, exploits, attempting to implement DRM and just simply trying to hide what they are doing. We intend to discuss the characteristics of these protections, how to both implement and defeat them, and the usage and prevalence of these tactics in the wild.

Speaker Bios

Tim "diff" Strazzere is a lead research and response engineer at Lookout Mobile Security. Along with writing security software, he specializes in reverse engineering and malware analysis. Some interesting past projects include having reversing the Android Market protocol, Dalvik decompilers and memory manipulation on mobile devices. Past speaking engagements have included DEFCON, BlackHat, SyScan, HiTCON and EICAR.

Jon "Justin Case" Sawyer is a father of four, and CTO of Applied Cybersecurity LLC. Jon likes to spend his nights with a fine (cheap) glass of wine, writing exploits for the latest Android devices. When not researching vulnerabilities or writing exploits, he dabbles in dalvik obfuscation.

Android Security State of the Union

The world of security is riddled with assumptions and guesses. Using data collected from hundreds of millions of Android devices, we'll establish a baseline for the major factors affecting security in the Android ecosystem. This will include analysis of potentially harmful applications, as well as other exploitation from non-application sources. This will help provide direction for the issues that we think will benefit the most from security community attention and research contributions.

Speaker Bio
Adrian Ludwig

Android Security Modules

Android, iOS, and Windows 8 are changing the application architecture of consumer operating systems. These new architectures required OS designers to rethink security and access control. While the new security architectures improve on traditional desktop and server OS designs, they lack sufficient protection semantics for different classes of OS customers (e.g., consumer, enterprise, and government). The Android OS in particular has seen over a dozen research proposals for security enhancements.

This talk motivates OS security extensibility in the Android OS. We propose the Android Security Modules (ASM) framework, which provides a programmable interface for defining new reference monitors for Android. We drive the ASM design by studying the authorization hook requirements of recent security enhancement proposals and identify that new OSes such as Android require new types of authorization hooks (e.g., replacing data). We describe the design and implementation of ASM and demonstrate its utility by developing reference monitors called ASM apps. Finally, ASM is not only beneficial for security researchers. If adopted by Google, we envision ASM enabling in-the-field security enhancement of Android devices without requiring root access, a significant limitation of existing bring-your-own-device solutions.

Speaker Bio

William Enck is an assistant professor in the Department of Computer Science at NC State University. Dr. Enck's research efforts centrally focus on systems security, addressing challenges in smartphones and mobile applications, operating systems, cloud services, telecommunications, and hardware architectures. In particular, his work in mobile application security has led to significant consumer awareness and changes within the space.

Dr. Enck was awarded the National Science Foundation CAREER Award and has served on many program committees including several top conferences in security such as USENIX Security, IEEE Security and Privacy, ACM CCS, and NDSS. Prior to joining NC State, Dr. Enck earned his Ph.D., M.S., and B.S in Computer Science and Engineering from the Pennsylvania State University in 2011, 2006, and 2004, respectively. He is a member of the ACM, IEEE, ISSA, and USENIX.

Friday, May 1, 2015 – Device Security Update Presentations and Breakout Sessions

An Update on Android Security Updates

The Android Security Team has been doing extensive analysis of CTS and device data to understand which Android devices are updated and how often. We want to share our findings and suggest changes to the current patch management process that may improve the responsiveness of the Android ecosystem to security issues.

Speaker Bio

Jon Larimer is a senior security engineer on the Android Security Team.

Let's Patch: An Analysis on Android Challenges in Distributing Open Source Patches on Proprietary Hardware

PC's get patches every month. Apple has been very efficient in creating and distributing security patches. The AOSP source is updated regularly. Why is Android patch distribution so delayed? Shouldn't it be easy to distribute the AOSP source changes as updates to launched devices?

This talk is of benefit for anyone working on mobile security. The primary function of this presentation is to provide a map of the reefs that have distributing updates to the end user difficult. Android has provided us with 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 embracing open source software on proprietary hardware.

Speaker Bio

Patrick McCanna has been defining what "mobile security" means at AT&T since 2004. Patrick launched the initial network security audits for the mobility production network. He later created the security review processes for all new mobile service offerings at AT&T. Patrick later helped develop AT&T's mobile endpoint security program. He is also a board member on AT&T's bug bounty program—the first of its kind for the ISP industry. Patrick also leads AT&T's sponsorship of r00tz Asylum—a non-profit dedicated to teaching kids around the world how to love being white-hat hackers.

Xiaomi Device OTA Update for Security Patches

Device security update is one of the most critical steps to address security vulnerabilities in end-user devices. Thanks to Xiaomi's "living OS" concept and practice, Xiaomi is able to do device update more frequently than lots of smartphone brands in the market place. Recently, Xiaomi and the Qualcomm product security team started a pilot program to regularly patch security vulnerabilities in Xiaomi smartphones. We pick a Xiaomi flagship phone for this pilot program, gather security vulnerability information mainly from Qualcomm security bulletins and Google Android Security bulletins, figure out the applicability, integrate and test the patches, and release OTA device update. In this talk, we will introduce Xiaomi device update mechanism and process, share some statistics on the scope and timeline of security-related device updates, and discuss lessons learned in this pilot program.

Speaker Bios

NIE Juhu and **ZHANG Yang** are security researchers in Xiaomi. They mainly focus on Android framework development, exploit research, reverse engineering and program analysis.

Breakout Session: Patching

Patching is an important component of securing software & devices. This session will focus on patching security vulnerabilities in the mobile ecosystem. It will build on last year's session and likely touch:

- The state of patching in the mobile ecosystem
- Understanding the challenges & opportunities specific to mobile ecosystem
- Exploring steps to make patching more streamlined & ubiquitous

Moderator: **Arun Balakrishnan**

Breakout Session: Open Source and Security

Use of open source code & libraries is ubiquitous in today's projects. We have been seeing the impact of security vulnerabilities in popular open source libraries on product security. This session will likely touch on:

- The role of open source
- Initiatives to secure core libraries
- Approaches to working with open source community

Moderators: **Renwei Ge** and **Neil Lofland**