
*The agenda for the Mobile Device Security Summit is dynamic and continues to evolve. In order to bring you the most up-to-date information and top rated speakers, the speakers and topics listed on this agenda may change.*

| **Thursday, May 30, 2013** | |
|---|---|
| 8:00-9:00 am | *Registration* |
| 9:00-9:10 am | *Welcome & Opening Remarks*<br>Kevin Johnson, SANS Institute |
| 9:10-10:00 am | *Keynote Address*<br>**Mobile Malfeasance: Exploring Trends in Dangerous Mobile Code**<br>Mobile devices are a hot trend amongst security topics this year. While most cover the angle of the device management, only few go into testing the applications. Since the mobile application vulnerability landscape is still young, there is a need to classify these vulnerabilities so that development teams can focus and root them out of their codebases. Join us as we explore the OWASP Mobile Top 10 classification system and metrics from a large case study of a real enterprise facing the deployment and assessment of a large number of mobile applications. Developers, Managers, and team leads will leave with resources and guidelines to start mobile security both at the process level and code level, including how to handle external mobile development teams them might contract.<br>**Jason Haddix, Director of Pen Testing, HP** |
| **10:00-10:30 am** | **Networking Break** |
| 10:30-11:30am | *User Panel*<br>**BYOD: A Real-World Guide to Making it Work**<br>BYOD can mean decreased equipment expenditures and increased employee productivity; it can also mean BIG headaches for those charged with security, privacy, and access management. These panelists have adopted BYOD and have lived to tell the tale. Don't miss this session to hear their survival strategies and best practices.<br>**Moderator: Kevin Johnson, Senior Instructor, SANS Institute**<br>**Panelists: Waqas Akkawi, Director, IT Security, SIRVA Inc.**<br>**Alex Guitman, Head of Global IT Business Continuity, SAP**<br>**Aaron Ingold, Association Manager – Mobility Development, NuVasive** |
| 11:30 am-12:30 pm | *Case Study*<br>**Wrapping Your Arms Around Mobile Security in the Enterprise**<br>With an average of 5,656 flights a day to 376 airports on six continents, United Airline employees are going places, and their mobile devices are going with them. What are the challenges of securely equipping such a peripatetic workforce? Learn the criteria and step-by-step decision making process United used to select a MDM solution, and put their learning to work in your own organization.<br>**Nathan King, Senior Manager, IT Security Systems United Airlines** |
| 12:30-1:40 p.m. | **Lunch** |

| | |
|---|---|
| 1:40-2:40 pm | **Healthcare to Go: Securing Mobile Healthcare Data**<br>This session will explore the issues and challenges of securing healthcare data and will discuss the implementation of security controls in the mobile space.<br>**Lee Kim, Esq., Tucker Arensberg, Chair of mHIMSS Legal and Policy Taskforce** |
| 2:40-3:30 pm | *Expert Briefing*<br>**Social Zombies: Rise of the Mobile Dead**<br>Just when you thought "bath salts" were turning innocent humans into flesh eating zombies in Florida...mobile devices have begun taken over the world like an infectious zombie virus outbreak. Tablets and mobile phones are being used by everyone today and are more powerful than ever before. The technology implemented in these devices is truly bleeding edge. From new wireless technology like NFC (Near Field Communication) to social networks being integrated directly into mobile operating systems, the times are rapidly changing. These new technology advancements also introduce new privacy and physical security concerns not seen before as well. In addition, with new technology come new responsibilities and challenges for security professionals and consumers alike especially in a world of BYOD.<br><br>In this presentation Tom Eston and Kevin Johnson explore and exploit the new technology being implemented by these mobile platforms. Tom and Kevin have discovered interesting security and privacy issues with Android Jelly Bean, Apple iOS 6, OS X Mountain Lion, NFC and many popular mobile applications. New tools and exploits will be discussed that can be used by penetration testers to exploit these new technologies. Tom and Kevin will also discuss strategies to combat the ensuing mobile device onslaught into the enterprise. This information alone will help you to survive the "Rise of the Mobile Dead."<br>**Tom Eston, Manager, Profiling & Penetration Team, SecureState**<br>**Kevin Johnson, SANS Instructor** |
| **3:30-4:00 pm** | **Networking Break** |
| 4:00-5:00 pm | *Case Study*<br>**Say Cheese: The Evolution of Mobile Devices and Cameras**<br>Remember when cell phones and mobile platforms didn't include cameras? Those days are long gone, yet many people and organizations continue to underestimate the power of the camera. This session will cover the evolution of mobile platforms into mobile devices and how their cameras evolved to potentially impact both personal and professional lives. We'll follow the picture of new attack vectors utilizing QR codes and other mediums to malware and manipulation – including case studies - and finally arrive at mobile device policies and best practices (or lack thereof).<br>**Jim Cossaboom, Senior Manager, Global Information Security Office , Threat Intelligence, Security Operations and Management, Deloitte Touche Tohmatsu Limited** |
| **Friday, May 31** | |
| 9:00-9:15 am | *Research Presentation*<br>**SANS Survey on Mobility Usage and Security Practices in the Enterprise**<br>Kevin Johnson, SANS Institute |
| 9:15-10:15 am | *Keynote*<br>**SANS 8 Mobile Device Security Steps**<br>Every organization is challenged to rapidly deploy mobile device security. The SANS 8 |

| | |
|---|---|
| | Mobile Device Security Steps is a community driven project to provide the most up to date information on the most effective strategies for securing mobile infrastructure. Chris Crowley will discuss the guidance provided in the 8 Steps, including: User authentication and restricting unauthorized access, OS and Application management, device monitoring, and key operational components for mobile device management.<br>**Chris Crowley, Certified Instructor, SANS Institute** |
| 10:15-10:45 am | **Networking Break** |
| 10:45-11:30 am | *Case Study*<br>**School's Out for Summer, But Malware Never Takes a Vacation**<br>The Anaheim Union High School District is comprised of 21 schools and serves more than 33,000 students and teachers – making it critical for the school district to know who and what was connecting to its network at all times. Over summer break, the school district enables staff to take home the laptops and portable devices they use during the school year. However, when staff returns, the devices are often out of date with respect to software and anti-virus patches. To prepare to deal with the malware introduced into its network when its staff returned, Anaheim Union needed to find a way to add a layer of security to its endpoint, while ensuring a secure pathway for students and staff to connect their consumer devices to the network. This session will stimulate conversation through a review of a particularly demanding case study and show attendees how Anaheim Union High School District took a layered approach to security that leveraged a comprehensive network access system to provide its IT team with complete visibility and control over the users and devices on its network.<br>**Erik Greenwood, Director of Information Systems, Anaheim Union High School District** |
| 11:30 am-1:00 pm | **Lunch & Learn , Presented by ForeScout & FiberLink**<br>**BYOD / CYOD Security at the Intersection of NAC and MDM**<br>You've got the green light to speed up your enterprise mobility initiatives. You are well informed about the threats and risk. You've been deluged with tool options. So what critical control mechanisms should you consider in order to achieve successful BYOD / CYOD adoption while enforcing policy. This luncheon session pinpoints where, when and how Network Access Control and Mobile Device Management effectuates controls across device, user, network, application and data. Gain insight into uncommon capabilities, advantages and constraints with regards to how NAC and MDM can be applied to rapidly implement and safeguard personal and mobile device use at your company.<br>**Scott Gordon, CISSP, Vice President, ForeScout**<br>**Clint Adams, Director of Mobile Technology Solutions, Fiberlink** |
| 1:00-2:00 pm | **Solutions Roundtable**<br>MDM, BYOD, OMG! Your workforce wants access to everything they need to work from anywhere on any device of their choosing; your management wants a tight rein on proprietary data and apps. How do you power an efficient yet secure mobile enterprise? In this roundtable, we'll examine what's happening now and what's next in mobile device security, and you'll have a chance to get your questions answered and your opinions heard by some of the leading vendors in this space.<br>**Moderator: Kevin Johnson, Senior Instructor, SANS Institute**<br>**Panelists:** |

| | |
|---|---|
| | **Scott Gordon, CISSP, Vice President, ForeScout**<br>**Clint Adams, Director of Mobile Technology Solutions, Fiberlink**<br>*Additional Panelists to be Named* |
| 2:00-3:00 pm | **2:00-3:00 p.m.**<br>**Mobile Transformation: The Journey of Converting a Concept into Reality**<br>Increasingly, enterprises are embracing the bring-your-own-device (BYOD) phenomenon to support growing mobile workforces and increase productivity. The push for change is taking place from the Board room with the C-suite and senior management asking for "i" devices. The need for mobile transformation is inevitable for most organizations, and as such, it is imperative to strategically map this journey in order to successfully navigate today's mobile threats and vulnerabilities. This presentation will walk through the mobile transformational journey, using a real case study to outline a comprehensive roadmap for converting a vision into reality. Specifically, we will discuss the key ingredients to a successful BYOD implementation, including strategy, governance and policy, technology architecture, security and compliance, and mobile device lifecycle management processes.<br>**Colin Kibler, Director of Information Security and Compliance, Performance Food Group**<br>**Amandeep Lamba, Director, PricewaterhouseCoopers LLP** |
| **3:00-3:30 pm** | **Networking Break** |
| 3:30-4:30 pm | *Case Study*<br>**Authorized Personnel Only: Protecting BYOD Party Crashers**<br>So, you've agonized over your BYOD policy and selected an MDM product to manage employees authorized to use their smart phones at work. But what about everyone else – the employees who aren't authorized but who still have smart phones, and are going to use them. In this case study, you'll learn which Windows GPOs and other tools you can implement to stop unauthorized personnel from exfiltrating or bypassing web filtering through tethering.<br>**Brent Morris, VyStar Credit Union** |