SANS

Mobile Device Security

SUMMIT 2013

The Growing and Constantly Changing Challenge

Program Guide

Agenda

All Summit Sessions will be held in Magic Kingdom Ballroom 1 (unless noted).

All approved presentations will be available online following the Summit at **https://files.sans.org/summits/mobile13** *.*
An e-mail will be sent out within 5 business days once the presentations are posted.

Thursday, May 30

7:45 - 8:45 am

Breakfast & Learr
Presented by

The BYOD Blueprint: How to Securely Onboard Personal Devices to Corporate Networks

Corporate IT departments are struggling to manage and secure the influx of mobile devices on their networks. To ensure the security and integrity of both corporate and employee-owned devices, as well as protect access to your corporate resources and assets, companies should deploy a comprehensive security strategy — the BYOD Blueprint — that encompasses network access control (NAC), mobile device management (MDM) and mobile application management (MAM). This session will showcase the BYOD Blueprint and explain how the different technologies that encompass it complement each other to ensure full visibility and control of the network and mobile devices in this era of IT consumerization.

Michael Killoran, VP Worldwide Sales, Bradford Networks
Rob McLeroy, Channel Manager, AirWatch

7:45 - 9:00 am

Registration

9:00 - 9:10 am

Welcome & Opening Remarks
Kevin Johnson, Senior Instructor, SANS Institute

9:10 - 10:00 am

Keynote Address
Mobile Malfeasance: Exploring Trends in Dangerous Mobile Code

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.

Jason Haddix, Director of Pen Testing, HP

10:00-10:30 am

Networking Break and Vendor Expo
Location: Sleeping Beauty Pavilion

10:30 - 11:30am

User Panel
BYOD: A Real-World Guide to Making it Work

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.

Moderator: Kevin Johnson, Senior Instructor, SANS Institute

Panelists: Waqas Akkawi, Director, IT Security, SIRVA Inc.
Alex Guitman, Head of Global IT Business Continuity, SAP
Aaron Ingold, Association Manager – Mobility Development, NuVasive

---

11:30 am - 12:30 pm

Case Study
Wrapping Your Arms Around Mobile Security in the Enterprise

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.

Nathan King, Senior Manager, IT Security Systems, United Airlines

---

12:30 - 1:40 pm

Lunch & Learn
Presented by

cellebrite
delivering mobile expertise

Smart Phone Forensics

• Cellebrite's current extraction support & the unique R&D challenges faced when developing Physical extraction & Password Bypassing around Android, iOS, & BlackBerry.

• Overview of the Physical Analyzer's decoding support including application data, location data, and malware detection

Sonny Farinas, Director, Forensic Sales, Cellebrite USA
Lee Papathanasiou, Technical & Sales Engineer, Cellebrite USA

1:40 - 2:40 pm

Healthcare to Go: Securing Mobile Healthcare Data

This session will explore the issues and challenges of securing healthcare data and will discuss the implementation of security controls in the mobile space.

Lee Kim, Esq., Chair of mHIMSS Legal and Policy Taskforce, Tucker Arensberg

2:40 - 3:30 pm

Expert Briefing
Social Zombies: Rise of the Mobile Dead

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.

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."

Tom Eston, Manager, Profiling & Penetration Team, SecureState
Kevin Johnson, Senior Instructor, SANS Institute

3:30 - 4:00 pm

Networking Break and Vendor Expo
Location: Sleeping Beauty Pavilion

4:00 - 5:00 pm

Mobile Device Security 2023: Emerging Threats and Trends

This session, Summit Chair Kevin Johnson will draw on research to gaze into the future and predict the next wave of innovation and threats in mobile devices – and what you need to be doing now to stay ahead of the curve.

Kevin Johnson, Senior Instructor, SANS Institute

Please remember to complete your speaker evaluation for today. You may leave completed surveys at your seat or turn them in to the SANS registration desk.

Friday, May 31

7:45 - 8:45 am

Breakfast & Learn
Presented by

BYOD Brings Mobile Security to the Boardroom

Organizations are encouraging employees to bring their own mobile devices into the workplace to be used for work purposes. This trend is shifting how devices are procured, paid for, managed and supported – and most importantly how they are secured. By handling the security issues up front, enterprises can recognize the true value of BYOD, enabling mobility for all. Join SAP, Mocana and NuVasive as we discuss real issues faced when deploying BYOD to thousands of employees. Explore the importance of mobile security when defining your BYOD strategy.

Milja Gillespie, Director – Mobility Product Marketing, SAP
Alex Guitman, Head of Global IT Business Continuity, SAP
Tushar Patel, Director – Product Marketing, Mocana
Aaron Ingold, Association Manager – Mobility Development, NuVasive

---

7:45 - 9:00am

Registration

9:00 - 9:15 am

Research Presentation
SANS Survey on Mobility Usage and Security Practices in the Enterprise

Kevin Johnson, Senior Instructor, SANS Institute

9:15 - 10:15 am

Keynote
SANS 8 Mobile Device Security Steps

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.

Chris Crowley, Certified Instructor, SANS Institute

10:15 - 10:45 am

Networking Break and Vendor Expo
Location: Sleeping Beauty Pavilion

10:45 - 11:30 am

Case Study
School's Out for Summer, But Malware Never Takes a Vacation

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.

Erik Greenwood, Chief Technology Officers, Anaheim Union High School District

---

11:30 am - 1:00 pm

Lunch & Learn
Presented by

BYOD / CYOD Security at the Intersection of NAC and MDM

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.

Scott Gordon, CISSP, Vice President, ForeScout
Clint Adams CISSP, Director of Mobile Technology Solutions, MaaS360 by Fiberlink

---

1:00 - 2:00 pm

Solutions Roundtable

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.

Moderator: Kevin Johnson, Senior Instructor, SANS Institute

Panelists: Clint Adams CISSP, Director of Mobile Technology Solutions, MaaS360 by Fiberlink
Scott Gordon, CISSP, Vice President, ForeScout
Bill Novak, Mobility Solutions, SAP
Tushar Patel, Director - Product Marketing, Mocana

2:00 - 3:00 pm

Mobile Transformation: The Journey of Converting a Concept into Reality

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.

Colin Kibler, Director of Information Security and Compliance, Performance Food Group
Amandeep Lamba, Director, PricewaterhouseCoopers LLP

3:00 - 3:30 pm

Networking Break and Vendor Expo
Location: Sleeping Beauty Pavilion

3:30 - 4:30 pm

Case Study
Authorized Personnel Only: Protecting Against BYOD Party Crashers

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.

Brent Morris, Senior Analyst, VyStar Credit Union

Please remember to complete your speaker evaluation for today. You may leave completed surveys at your seat or turn them in to the SANS registration desk.

Exhibitors

Airwatch
AirWatch is the leader in enterprise-grade mobility management and security solutions. Our highly scalable solution provides a real-time view of an entire fleet of corporate and employee-owned Apple iOS, Android, Windows, BlackBerry and Symbian devices. As the largest MDM provider, AirWatch offers the most comprehensive mobility management solution.

Bradford Networks
Bradford Networks enables secure network access for BYOD. The Bradford Networks solution automatically identifies and profiles all devices and all users on a network, providing complete visibility and control, eliminating the network blind spots that introduce risk.

Cellebrite
Since 2007, the Cellebrite UFED has provided mobile forensics solutions to investigative professionals worldwide. The UFED enables extraction, decoding and analysis of data and passwords from thousands of legacy and feature phones, smartphones, portable GPS devices, and tablets. Visit the Cellebrite exhibit or online at **www.ufedseries.com** to learn more.

HID Global
HID Global is a leader in identity assurance and enables customers to prove and establish trust in a person's identity when accessing resources on the network. HID Global's strong authentication, credential management and converged access solutions provide security and enables compliance for enterprise, government, and financial services customers. **www.hidglobal.com**

Fiberlink
MaaS360 by Fiberlink simplifies mobile device management (MDM), mobile application management (MAM), and secure document sharing in the BYOD era. Trusted by small businesses, government agencies, universities, and large enterprises worldwide, MaaS360 enables mobile policies that boost productivity, protect employee privacy, and secure sensitive data across smartphones, tablets, and laptops.

ForeScout Technologies
ForeScout delivers automated solutions for Network Access Control (NAC), mobile security, endpoint compliance and threat prevention. Because our agentless appliance is easy to deploy, use and scale, over 1300 of the world's most secure enterprises and military installations rely on ForeScout to enable accessibility while protecting networks and sensitive data.

FrontBlade
FrontBlade Systems is an IT System Integrator of Technologies, Services, and Expertise to enable the Adaptive Enterprise. Our portfolio includes only the world's premier technologies with solutions for Network Security, End Point Security, MDM, VDI, BYOD, Thin Client, Zero Client, End Point Discovery / NAC, Server Virtualization, and Storage / DR.

SAP
SAP helps companies of all sizes and industries run better. From back office to boardroom, warehouse to storefront, desktop to mobile device – SAP empowers people and organizations to work together more efficiently. SAP's leading mobile security portfolio addresses an enterprise's need for secure mobile devices, app and content.

Fujitsu
Fujitsu is the 3rd largest IT company globally with revenues of over $53B annually. Fujitsu enables clients to meet their business objectives through integrated including consulting, systems integration, managed services, outsourcing and cloud services for infrastructure, platforms and applications; data center and field services; and server, storage, software and mobile/tablet technologies.

BN **BRADFORD NETWORKS**

the smart edge

ENABLES FLEXIBLE AND SECURE

BYOD

Bring Your Own Device

SC MAGAZINE
BEST BUY

- Know every device on the edge of your network

- Assess the risk of smartphones, tablets, laptops, and edge devices

- Provision secure network access based on user & device policies

- Integrate with the leading security solutions to remediate BYOD threats

www.bradfordnetworks.com

MOBILE MASTERY

Security and flexibility for the BYOD era.
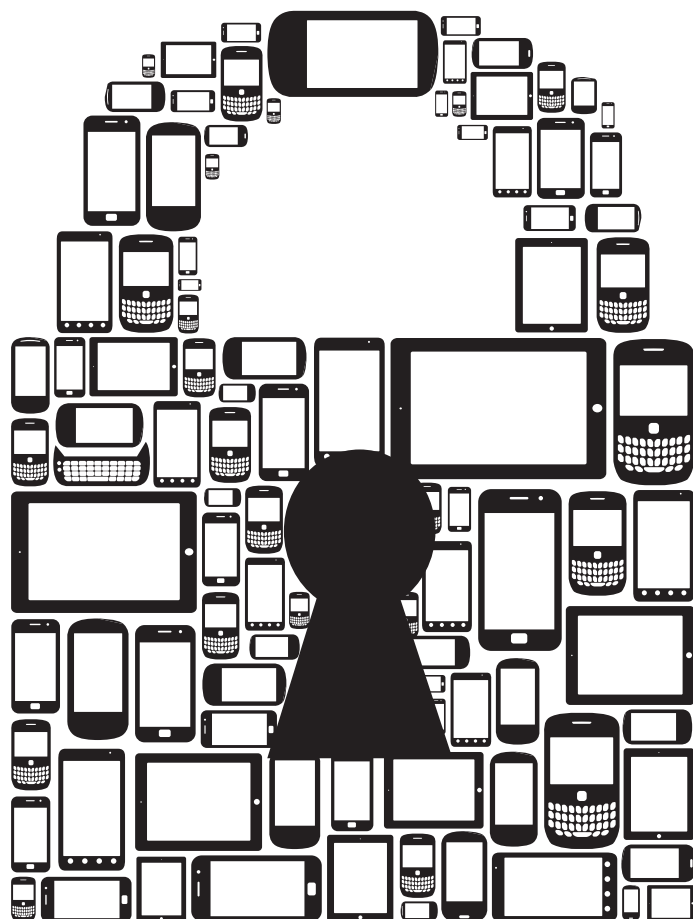
Secure your enterprise mobile apps and devices quickly and easily.

Every day new devices and apps are brought into your enterprise. Now you can implement comprehensive and secure enterprise device, content, and app management for all of your mobile platforms—with the same SAP solution. Used by 200,000 enterprises worldwide, it's fast, easy, and from the proven industry leader.

Learn more at sapafaria.com

SAP **The Best-Run Businesses Run SAP™**

How Are You Protecting Your

➤ Data?

➤ Network?

➤ Systems?

➤ Critical Infrastructure?

Risk management is a top priority. The security of these assets depends on the skills and knowledge of your security team. Don't take chances with a one-size fits all security certification. **Get GIAC certified!**

GIAC offers over 20 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.

"GIAC is the only certification that proves you have hands-on technical skills."
-CHRISTINA FORD, DEPARTMENT OF COMMERCE

"GIAC Certification demonstrates an applied knowledge versus studying a book."
-ALAN C, USMC

Learn more about GIAC and how to *Get Certified* at
www.giac.org

NEW!
GIAC CERTIFICATION

GMOB
GIAC MOBILE DEVICE SECURITY ANALYST

Coming Fall 2013!
GIAC Mobile Device Security Analyst

Registration now open at www.giac.org

2013 UPCOMING SUMMITS & TRAINING COURSES

Digital Forensics and Incident Response Summit & Training
Austin, TX | July 9-16

ICS Security Training
Washington, DC | August 12-16

Critical Security Controls Summit
Washington, DC | August 12-18

Digital Forensics and Incident Response Summit & Training
Prague | October 6-12

Securing the Internet of Things Summit
San Francisco, CA | October 21

Healthcare Summit
San Francisco, CA | October 22-23

Pen Test Hackfest Summit & Training
Washington, DC | November 7-14

Asia Pacific ICS Security Summit
Singapore | December 2-7

For more information on speaking at an upcoming summit or sponsorship opportunities, e-mail SANS at **summit@sans.org**.

Visit **www.sans.org/summit** for detailed summit agendas as they become available.