SANS

Securing the Internet of Things Summit 2013

Program Guide

Agenda

All Summit Sessions will be held in CA Thayer Ballroom (unless noted).

All approved presentations will be available online following the Summit at ***https://files.sans.org/summits/internet13****.*
You will receive an e-mail within approximately one week of the summit once presentations are posted.

Tuesday, October 22

7:30 am-8:30 am

Registration

8:30 am – 9:15 am

Opening Keynote:
Securing the Internet of Things – Separating Hype from Reality

It's latest Internet evolution: billions of "things" connecting to users, businesses and other "things" using mixtures of wired and wireless connectivity. The "things" include everything from automobiles and home thermostats to airplanes, medical machinery, personal medical devices, windmills, environmental sensors, and natural gas extraction platforms. While this promises new efficiencies and new business models, it will also open up exponentially more attacks paths – if security is not built in. This talk will detail the key security challenges we're facing and opportunities for creating a secure foundation from the start.

Speaker: ***John Pescatore****, Director of Emerging Security Trends, SANS Institute*

9:15 am – 10:00 am

The Internet of Things: Trends and Opportunities

How big will the Internet of Things be in the coming years? Numerous trends all point to this being a massive growth area – one that will have a far-reaching and transformative impact on both our work and personal lives. This presentation will talk thru various scenarios that could play out in the evolution of the Internet of Things, and major trends and opportunity areas.

Speaker: ***Asheem Chandna****, Partner, Greylock Partners*

10:00-10:30 am

Networking Break

10:30-11:15 am

Just Trust Me: Internet-Enabled Devices with Integrity

Trust is an element of cyber security that is often not considered. Trust is based on evidence that a computing device will behave the way it is expected to behave. It implies that the software inventory and configuration is exactly what the owner thinks it is. The Internet of Things is made up of billions of devices that almost universally operate without human supervision. We have to believe that these devices are what they say they are and will do (only) what we expect them to do.

Since there are too many of them for humans to directly supervise (even if all seven billion of us take a hand in doing just that), the Internet of Things must be able to assess their own integrity, be able to detect malicious changes and be able to remediate those changes, ideally without the intervention of a person in the process.

Sound like science fiction? There are devices in the market today that are capable of detecting malicious change and reversing those changes. Sometimes the devices fix themselves, Sometimes the devices work together – the healthy ones helping fix the sick ones. Find out how trusted computing makes this possible and how the systems you design might use these techniques in this session. Examples of different architectures that are currently used in products will be cited and references will be provided.

Speaker: ***Stacy Cannady****, Technical Marketing Manager, Trustworthy Computing, Cisco*

11:15 am – 12:15 pm

Building Security Into the Next Generation of "Things"

If we could go back in time, we would design PCs and servers very differently based on the dangers of Internet-based attacks we are now all too familiar with. Stronger authentications, more secure operating systems, support for encryption, less vulnerable applications are just a few of the things we have a chance to better as we build the Internet of Things.

A panel of industry security experts will explore these issues and highlight the key areas of security that can and should be done better this time around:

Moderator: ***John Pescatore****, Director of Emerging Security Trends, SANS Institute*

Panelists: ***Adam Bosnian****, EVP Americas, Cyber-Ark Software*
Rick Doten*, CISO, Digital Management Inc. (DMI)*
Wolfgang Kandek*, Chief Technical Officer, Qualys*
Billy Rios*, Global Managing Director of Professional Services, Cylance*

12:15-1:30 pm

Lunch on Own

1:30-2:15 pm

Securing the Internet of Everything

Enterprises that embrace elements of the Internet of Things (IoT) in their businesses and for their clients must be prepared to secure and manage this new environment. However, many organizations haven't even yet integrated the security governance in place for traditional IT with the Operational Technology in use on the manufacturing floor, in hospitals or in kiosks, ATM machines and other appliances.

This presentation will detail the key issues around this first necessary phase of IT/OT integration, and seeks to answer such questions as:

- What is cyber security and its role in the IoT?
- What are the cyber security threats that the IoT faces?
- How can enterprises using the IoT secure it?

Speaker: ***Earl Perkins****, Research VP, Gartner*

2:15-3:00 pm

Riot Control: The Art of Managing Risk and the Internet Of Things (Riot)

Connected devices, machine-to-machine (M2) communications and smart-everything are transforming IP networks into a system of things providing data like never before. Many of these represent the interface between the logical world and the real world where emotional decisions can unknowingly facilitate risky reactions. This session explores the question will IoT change the way we need to think about security or will it be more of the same we are dealing with today.

Speaker: Greg Brown, CTO, Intel Networking

3:00-3:30 pm

Networking Break

3:30-4:30 pm

Solutions Session presented by

TREND MICRO™

Securing Your Journey to the Cloud

Internet of Everything: Insecurity Case Studies and Insights

The Internet of Things is turning quickly into the Internet of Everything and will only gain momentum with devices from all worlds, from many different industries, with many different reasons connecting to it. This presentation will focus on a number of insecurities that we are finding as part of this phenomenon and will share a number of case studies we've identified within our customer base as well as some unique research data developed by some of our forward-looking threat researchers. From ICS/SCADA attacks to some non-traditional infections, insights will be given around the insecurity of the Internet of Everything and best practices for improving security of this environment.

Speaker: ***Jon Clay****, Senior Manager, Trend Micro*

4:30-5:15 pm

Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts

Homes and offices inspired by concept of Internet of Things (IoT) are here and so are the related high impact attack vectors. Your next door lock, sprinkler system, light bulb, pet feeder, door sensor, thermostat, and baby monitor are likely to be vulnerable to attack. Remotely.

In this talk, we will break open emerging home automation products to build a solid threat model and see actual examples of vulnerabilities: from how an attacker can remotely cause blackout at your home (or your high-rise condo or office) and exploit various physical sensors that you will come to depend on. These aren't vulnerabilities you can just patch with a software update.

We know the implications of critical infrastructure vulnerabilities that are based on traditional protocols. It is time to talk about next-generation infrastructure that is destined to empower our future and our safety.

Speaker: ***Nitesh Dhanjani,*** *Researcher & Author*

5:15-5:30 pm

Closing Remarks

John Pescatore*, Director of Emerging Security Trends, SANS Institute*

Thank you for attending Securing the Internet of Things Summit.

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

Exhibitors

Codenomicon

Codenomicon finds product security vulnerabilities others can't find. Companies and their supply chains rely on Codenomicon DEFENSICS and APPCHECK to discover vulnerabilities in software/firmware/hardware that cause Denial of Service (DoS) and data leakage, and to provide detailed reporting to help developers remove the vulnerabilities. For more information, go to **www.codenomicon.com**.

Securing Your Journey to the Cloud

Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information. With more than 25 years of experience, we're recognized as the market leader in server security, virtual security, and small business content security. Trend Micro enables the smart protection of information, with innovative security technology that is simple to deploy and manage, and fits an evolving ecosystem. Our solutions are powered by the cloud-based global threat intelligence of the ***Trend Micro™ Smart Protection Network™*** infrastructure, and are supported by over 1,200 threat experts around the globe.

SANS
ICS
Industrial Control Systems

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

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

NEW!
GIAC CERTIFICATION

GIAC MOBILE DEVICE SECURITY ANALYST
GMOB

Coming Fall 2013!
GIAC Mobile Device Security Analyst

Registration now open at www.giac.org

UPCOMING SUMMITS & TRAINING COURSES

2013

Healthcare Summit
San Francisco, CA | October 23-24

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

Asia Pacific ICS Security Summit
Singapore | December 2-7

2014

AppSec Summit & Training
Austin, TX | February 3-8

Cyber Threat Intelligence Summit & Training
Washington, DC | February 2014

Digital Forensics & Incident Response Summit & Training
Austin, TX | June 3-10

Industrial Control Systems Security Summit & Training
Orlando, FL | March 12-18

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.