Should We Trust Mobile Computing, IoT and the Cloud? No, But There Are Solutions

April 20, 2015

9:00AM – 1:00PM

Welcome and Introduction to the Trusted Computing Group (TCG)

Dr. Joerg Borchert

TCG President and Chairman

Principle of Least Privilege Leads to Root of Trust (RoT) Concept

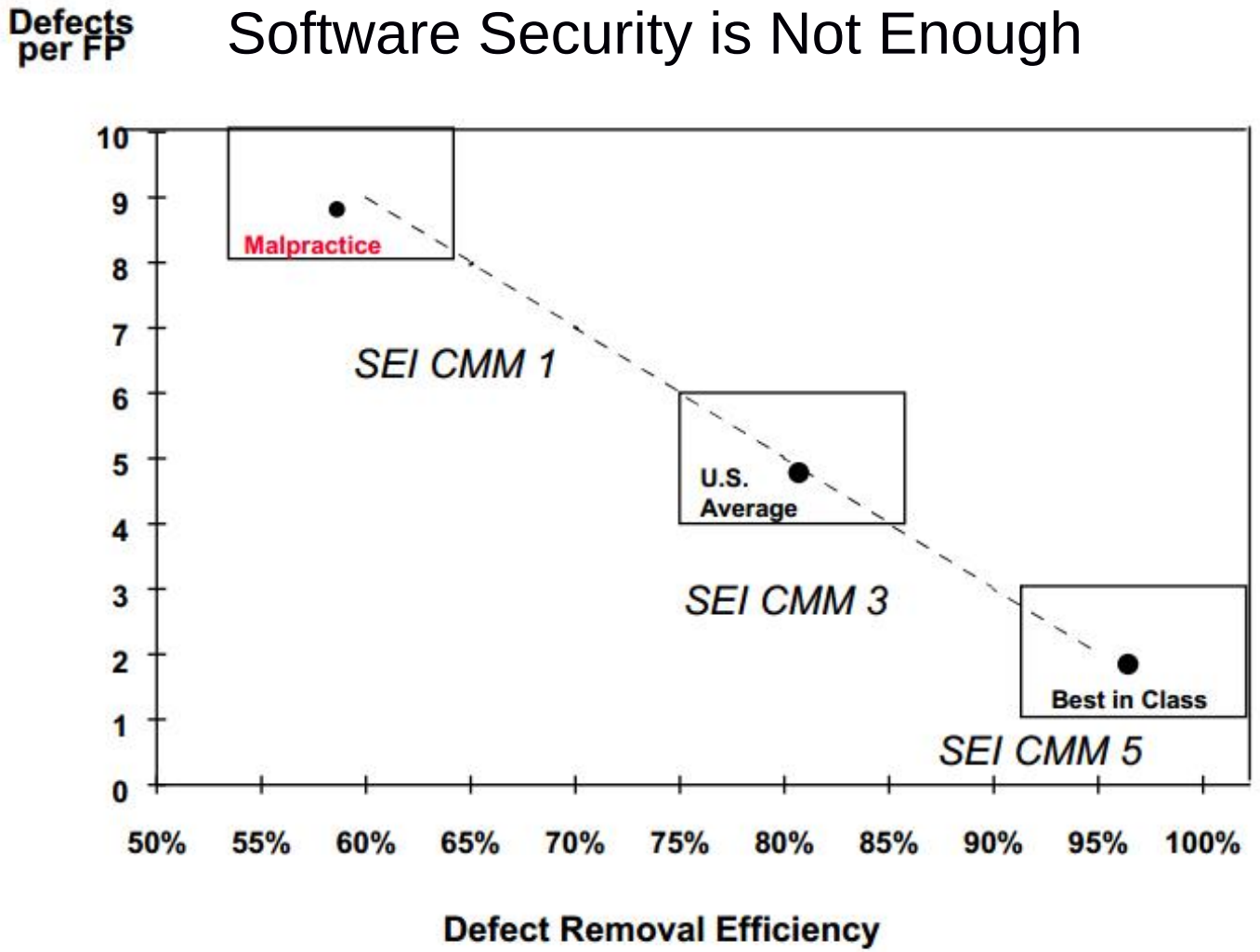
- RoT = Minimized, strongly protected security function

- RoT used for highly security-sensitive functions
  - Generate random numbers
  - Store and use long-term keys
  - Verify system integrity

- Benefits
  - Reduce risks
    - Compromise of long-term keys
    - Undetected system compromise

Why Hardware?

Software Security is Not Enough



Graph used with permission of Capers Jones.

What is a Hardware Root of Trust?

- **Hardware Security**
  - Trusted Platform Module (TPM)
- **Benefits**
  - Foundation for Secure Software
  - Impervious to attacks/hacks
  - Built-in virtual smart card
- **Features**
  - Authentication
  - Encryption

  – Identity
  - Attestation

  – Integrity

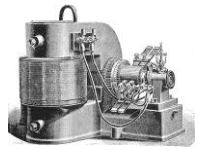
Building Trusted Systems

1. Build a Hardware Root of Trust into each device or use the ones you have in PCs, servers, other systems

2. Employ Hardware Storage Encryption

3. Add Security Automation

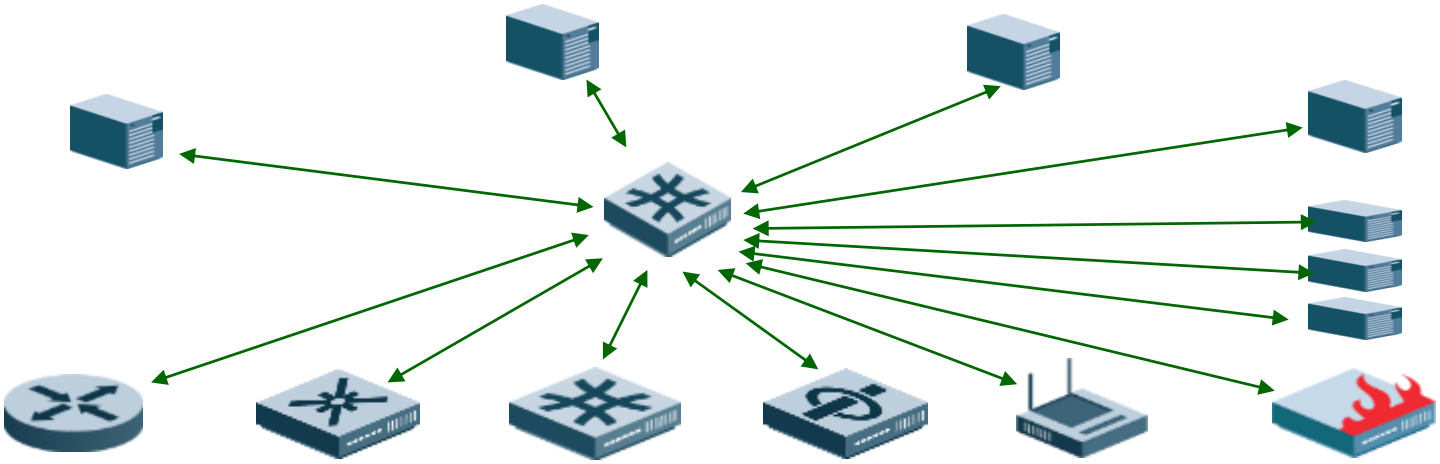
4. Protect Legacy Systems



TCG = Open Standards for Trusted Computing

- TCG is the only group focused on trusted computing standards
- TPM specification implemented in more than a billion devices
  - Chips, PCs, servers, printers, kiosks, industrial systems, and many embedded systems
- Trusted Computing is more than TPM
  - Secure Storage
  - Security Automation
  - Secure Cloud
  - Secure Mobile Devices
  - Secure Legacy Devices

Why Open Standards?



Interoperability	Vendor Neutrality
Security	Certification
Lower Costs	Ubiquity

TCG Evolving: Join Us

- Classic work groups, such as TPM, remain active
  - TPM Software Stack, PC Client specifications for 2.0 emerging
  - Storage releasing significant updates this summer
  - TNC doing significant architectural updates
- Mobile: new relationship to collaborate with ETSI; existing relationships with GlobalPlatform and others
- Embedded: new automobile thin specification released to enable secure remote software updates to vehicles, this week at SAE World Congress with SAE committee input.
- Internet of Things: new guidelines for securing IoT published as implementation guidance with more to follow

TCG Appoints Executive Director

Mark Schiller to lead membership and strategic initiatives as TCG continues to evolve to increasingly important computing and security applications, including cloud services, mobile computing and Internet of Things.

Contact: Mark@TrustedComputingGroup.org

Meet Mark in the Demonstration Showcase Room 2006 to learn more about TCG and its efforts!

TRUSTED COMPUTING GROUP™

Driving Adoption of Standards

- Join the TCG in the quest to develop and promote trusted computing technologies
  - Research; Standards writing; Published studies; and Continuing education
- Join to help influence developers and enterprise end-users

Technologies In Action:

Security Automation

Embedded Systems

Opal & Enterprise Drives

TPM Mobile

TPM Software Stack

Industrial Control Systems (ICS)

Trusted Platform Module (TPM)

Internet of Things (IoT)

Open-source Network Security

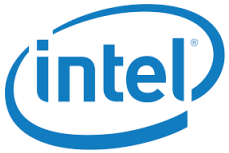
Self-encrypting Drive (SED)

Endpoint Compliance

Virtualized Systems

Demonstration Showcase

Over 25 member and partner companies showcasing TCG technology usage



Session Schedule

9:20	**20-Story Snowcastle: Why We Need a New Foundation for the Internet of Things**	Paul Roberts, Founder, Editor-in-Chief, Security Ledger
9:45	Panel: **Security and the Root of Trust: Leveraging the Root of Trust and TPM in the Enterprise**	Moderator: Paul Roberts – Founder, Editor-in-Chief, Security Ledger Panelists: • Amy Nelson – Engineering Technologist, Dell • David Bossio – Group Program Manage, OSSG Enterprise and Security R&D, Microsoft
10:45	Refreshment Break – Room 2006	
11:00	Panel: **The Insecure Internet of Things and How to Secure It**	Moderator: Rich Nass, Executive Vice-President, Embedded-Computing.com, OpenSystems Media Panelist: • Stacy Cannady, Senior Principal Cisco Systems • Darin Andersen, Founder, CyberUnited • Chuck Benson, Assistant Director of IT, Facilities Service, University of Washington
12:00	Panel: **Mobile is King, But Security Must Be a Priority**	Moderator: Jai Vijayan; Technology Editor/Writer Panelists: • Gil Bernabeu, Technical Director, GlobalPlatform • Lee Neely, Senior Cyber Analyst, Lawrence Livermore National Laboratory (LLNL) • Jon Geater, Chief Technology Officer, Trustonic
13:00	**End of Session Live Raffle Drawing**	Products Donated by: • Infineon Technologies • Samsung Electronics

20-Story Snowcastle: Why We Need a New Foundation for the Internet of Things

Paul Roberts

Founder and Editor-in-Chief,
Security Ledger