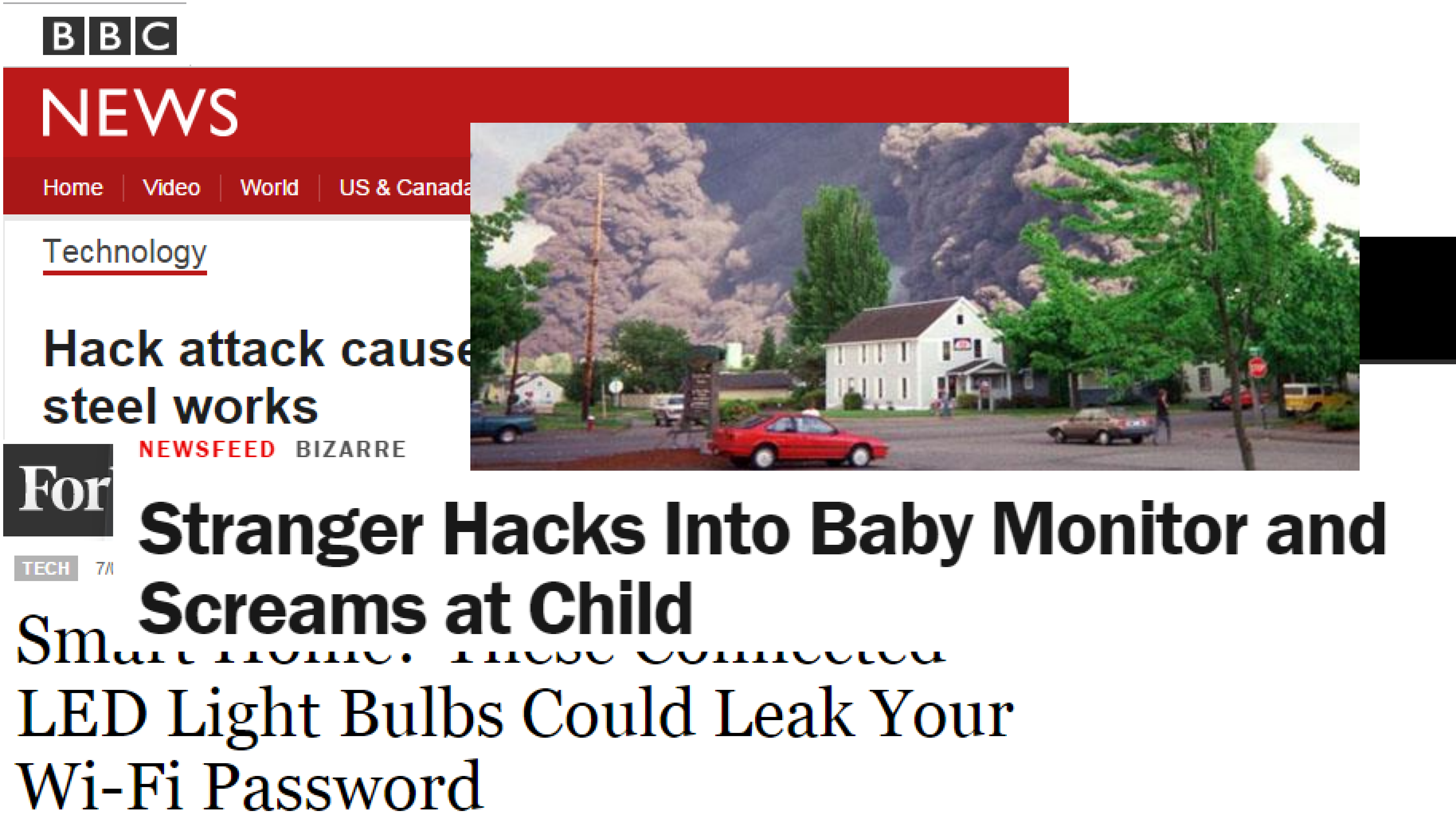
THE UNTRUSTED IOT

A Path to Securing Billions of Insecure Devices

Steve Hanna
Senior Principal, Infineon Technologies
Co-Chair, IoT Sub Group, Trusted Computing Group

Growing Trend of IoT Security Problems



BBC

NEWS

Home | Video | World | US & Canada

Technology

Hack attack cause
steel works

NEWSFEED BIZARRE

For

TECH 7/

Stranger Hacks Into Baby Monitor and Screams at Child

Smart Home: These Connected
LED Light Bulbs Could Leak Your
Wi-Fi Password

TRUSTED COMPUTING GROUP™

We’ve Been Here Before

Photo of Armagh Rail Disaster, June 12, 1889

Untrusted Systems

Source: S E C Railway Narrow Gauge Museum of Nagpur

Trusted Systems

Source: Bruce Fingerhood
License: CC BY 2.0
Link: http://www.flickr.com/photos/springfieldhomer

What is a Trusted System?

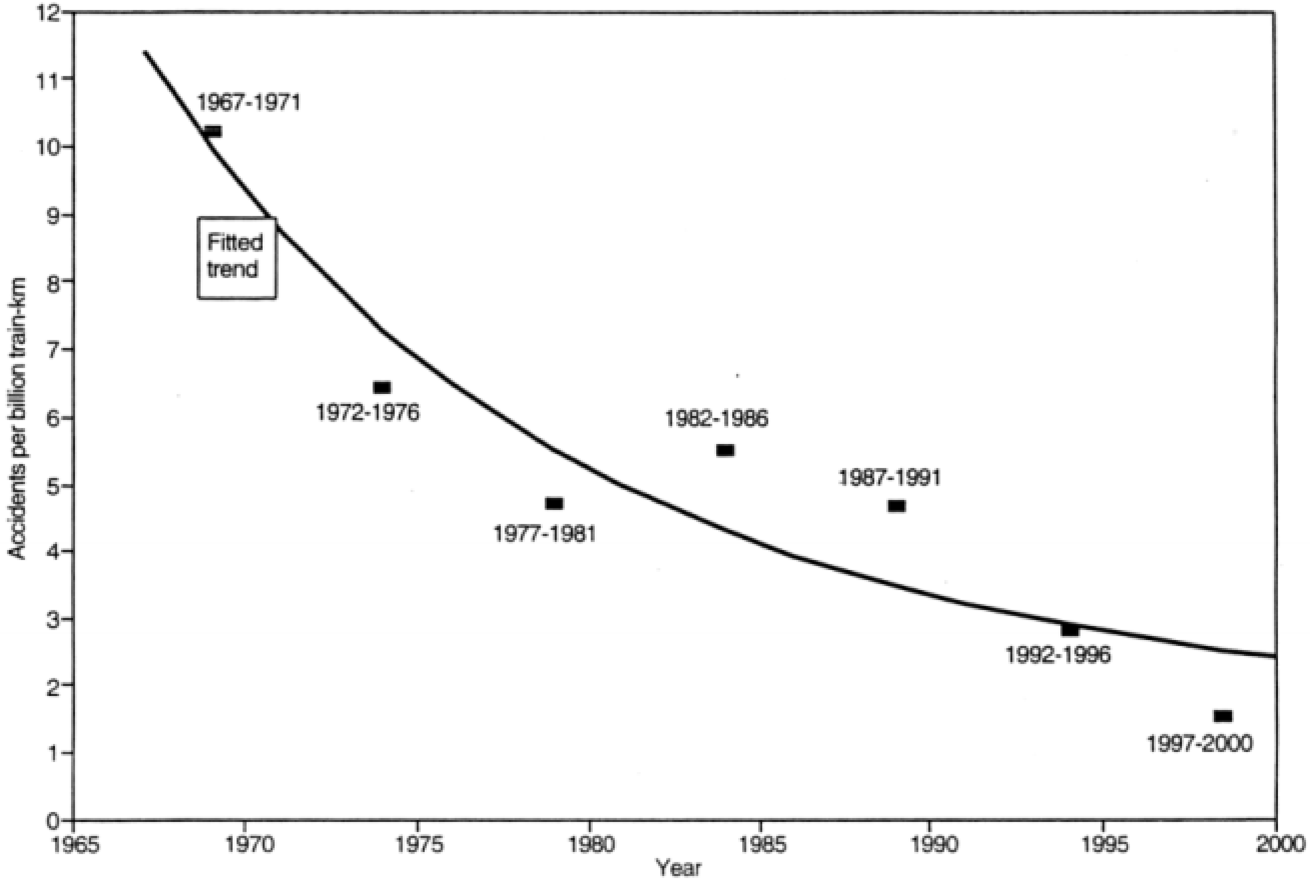
A trusted system is…

designed to be predictable, even under stress

based on fundamental properties

therefore trusted

Benefits of Trusted Systems



Source: Evans, A. W. (2003), Estimating Transport Fatality Risk from Past Accident Data, Accident Analysis and Prevention, Vol. 35, Issue 4.

Building Trusted IoT Systems

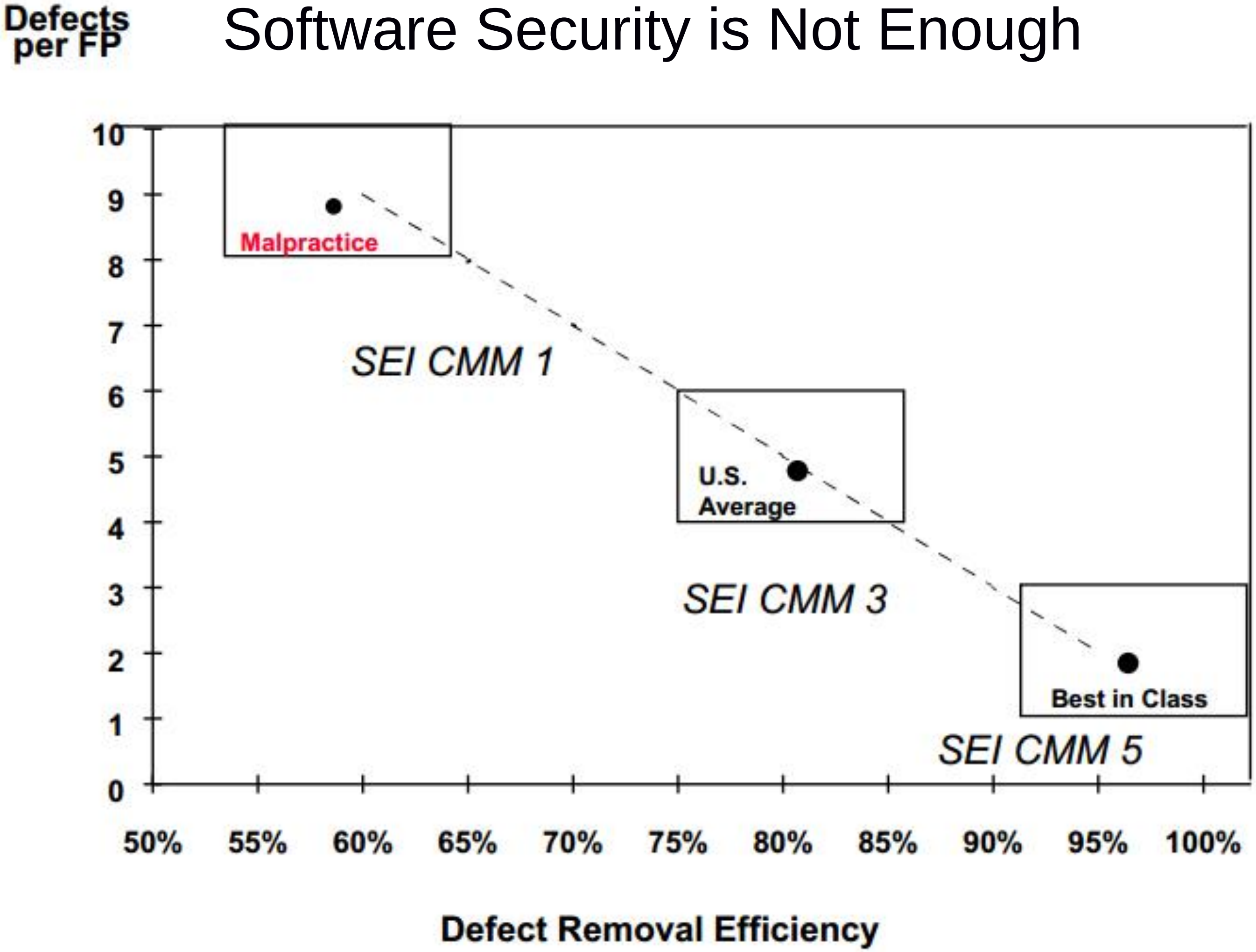
1. Build in a Hardware Root of Trust

What is a Root of Trust (RoT)?

- 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 risk of compromise
    - Compromise of long-term keys
    - Undetected system compromise

Why Hardware?

Software Security is Not Enough



Graph used with permission of Capers Jones.

Trusted Platform Module:
The Standard 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
  - Attestation

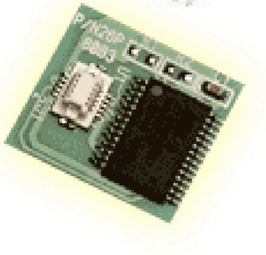
Authentication, Encryption – Identity

Attestation – Integrity

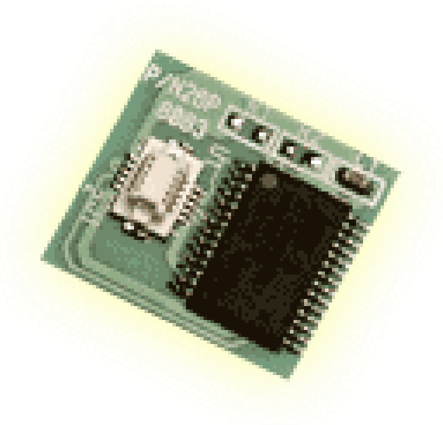
Building Trusted IoT Systems

1. Build in a Hardware Root of Trust

2. Employ Hardware Storage Encryption



Hardware Storage Encryption

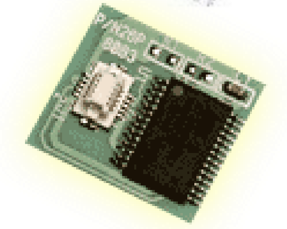


- **Hardware Security**
  - Self-Encrypting Drive (SED)
- **Benefits**
  - Always on encryption
  - No performance impact
  - Protection against Physical Attacks, loss and theft
  - Cryptographic instant erase/Wipe
- **Features**
  - Encryption

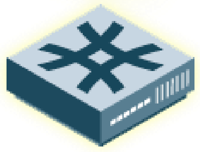
Building Trusted IoT Systems

1. Build in a Hardware Root of Trust

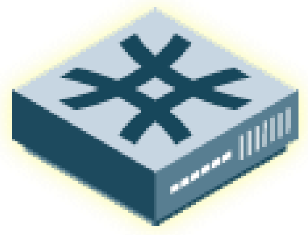
2. Employ Hardware Storage Encryption



3. Add Security Automation



Security Automation

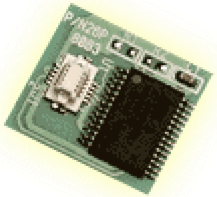


- **Security Automation Standards**
  - IEEE 802.1AR, TNC, TAXII
  - Manage IoT Devices
  - Control Network Access
  - Connect Security Systems
- **Benefits**
  - Automation for All Phases of Cyber
    - Preparation
    - Detection
    - Analysis
    - Response

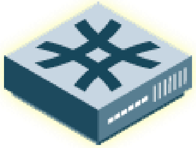
Building Trusted IoT Systems

1. Build in a Hardware Root of Trust

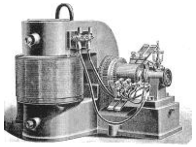
2. Employ Hardware Storage Encryption



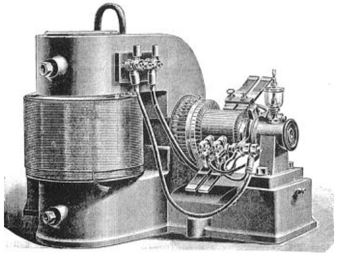
3. Add Security Automation



4. Protect Legacy Systems



Protect Legacy Systems



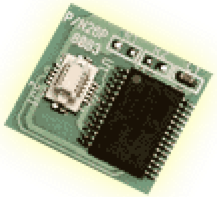
- **Legacy Systems**
  - ICS/SCADA or Old Systems
  - Vulnerable to Disruption or Infection
  - Need Protection

- **Protection**
  - Place into Enclaves
  - Overlay Secure Communications
  - Restrict to Authorized Parties

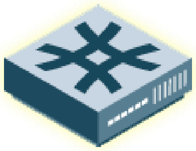
Building Trusted IoT Systems

1. Build a Hardware Root of Trust

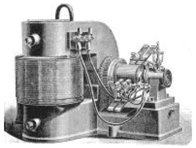
2. Employ Hardware Storage Encryption



3. Add Security Automation



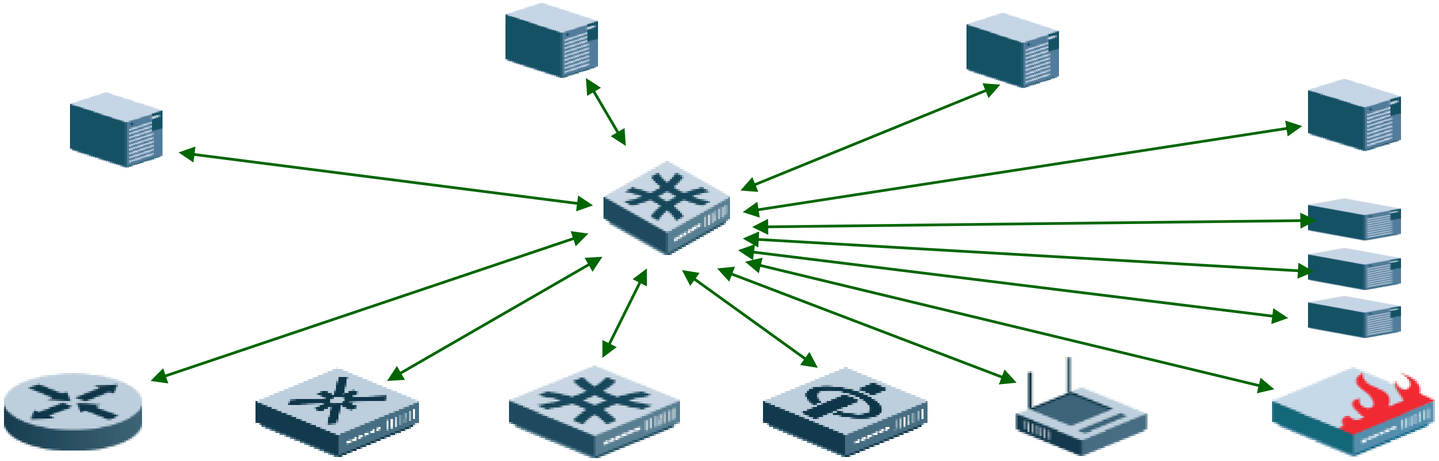
4. Protect Legacy Systems



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 integrated into PCs, servers, printers, kiosks, industrial systems, and many embedded systems
- Trusted Computing is more than TPM
  - Secure storage
  - Security automation
  - Secure mobile devices
  - Secure legacy devices

Why Open Standards?



Interoperability	Vendor Neutrality
Security	Certification
Lower Costs	Ubiquity

Trusted Computing for IoT

- TCG standards have been used in many IoT devices
  - Slot machines, cash registers, network routers, multi-function devices, enterprise printers/copiers, industrial control systems, kiosks, etc.

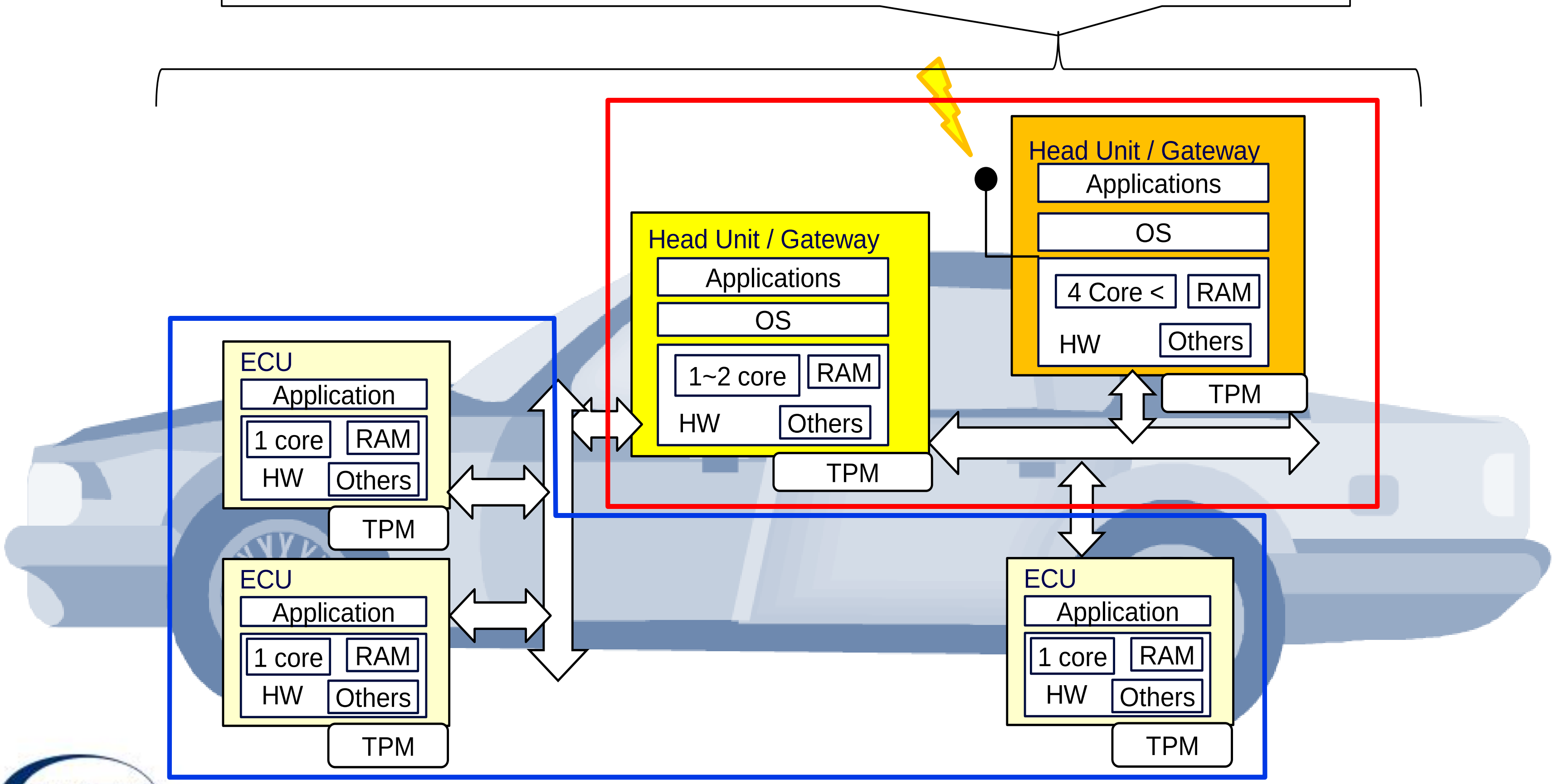
- Based on this experience, TCG has developed
  - TCG Guidance for Securing IoT
  - TCG Architect's Guide for Securing IoT
  - Demonstrations of Trusted Computing in IoT

TCG and Auto Security Initiative

- Initial focus on two key areas
  - Electronic Control Unit (ECU) integrity
  - Secure data communications
    - to manufacturer
    - to third parties
    - to other vehicles

Secure Automotive Architecture

Vehicle
- Works as a heterogeneous cluster with ECUs
- Internal communication: on-chip bus, system bus, Controller Area Network (CAN), Media Oriented Systems Transport (MOST), FlexRay.
- External communication directly or via Gateway



Which TCG Technologies for Auto?

- **TPM and TNC**
  - Create, store, and manage cryptographic keys in the ECU
  - Measure and report on the integrity of firmware and software used in the ECU
  - Provide attestation and assurance of identity of the ECU
  - Support secure firmware and software updates in the ECU
  - Provide anti-rollback protection and secure configuration memory for the ECU

- **TCG TPM 2.0 Automotive Thin Profile**
  - Addresses unique automotive requirements
    - temperature, vibration, acceleration, reliability
    - limited processing, power, and memory
    - long lifecycle (20 years+)

Secure Update Process

1. Securely verify software configuration

2. Initiate, verify, and perform software updates

3. Gather and securely store audit logs

TCG IoT Demos

- Industrial control systems (SCADA) network with a TNC interface and TPM (Artec IT Solutions)
- Securing IoT sensors and actuators managed by a cloud application over the public network with TCG TNC standards and the TPM: Cisco, HSR, Infineon, Intel
- Near real-time network security with an IF-MAP-based SIEM to enable various components to monitor, evaluate and visualize the network state: Decoit and the University of Hannover
- Establishing trust in embedded systems in the IoT with a TPM 2.0 and TPM Software Stack 2.0 to determine firmware and software state: Fraunhofer SIT

More TCG IoT Demos

- A remote firmware update with integrity enabled by the TPM for automotive electronic control units: Fujitsu
- Trusted computing in a network device using the TPM for measured boot for detection of tampering of software: Huawei
- Managed IoT security from silicon to cloud with separation of hardware, software and data security capability from operational applications: Intel
- Trusted device lifecycle management for IoT devices, using enterprise key management structures for industrial controllers and vehicles: Integrated Security Services
- A secure overlay network for M2M connectivity and communications, including process control networks: Tempered Networks and PulseSecure

Product Availability

- TPMs available from four chip manufacturers
  - SPI, LPC, and I^2C interfaces
  - Support in Microsoft Windows and Linux
- SEDs available from every drive maker
  - HDD, SSD, enterprise, and USBs
  - No need for OS support
  - Extensive ISV support for management
- TNC supported by most network vendors
  - Switches, routers, wireless access points
  - Support in Microsoft Windows and Linux

TCG Collaborating with IoT Industry

- Formal liaison relationship with ETSI, international telecoms standards body, for work on secure networking protocols
- Formal liaison relationship with Mobey Forum to help enable trusted mobile transactions, etc.
- Working with SAE Vehicle Electrical Hardware Security Task Force, a sub-committee of the SAE Vehicle Electrical System Security Committee re auto security requirements and solutions
- Regular input to NIST, NHTSA and other agencies and government groups
- Relationships with information assurance agencies worldwide

IoT Resources

- TCG IoT Architect’s Guide: http://bit.ly/1RzLRa6
- TCG Guidance for Securing IoT: http://bit.ly/1J0SBZ2
- IoT Demos: http://bit.ly/1GmmNrk
- Secure auto update prototype: http://bit.ly/1Hv8On3
- Auto Thin TPM profile: http://bit.ly/1J0SWL9
- 6 ways to Boost IoT Security article: http://ubm.io/1LahjI4
- IoT Security Groundswell article: http://ubm.io/1K7MOPW
- Practical Tips to Securing the IoT article: http://bit.ly/1K7WUTH

Questions?