TRUSTED® COMPUTING GROUP

Building Trustworthy Embedded Systems

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Agenda

- The Move to IoT
  - Threats & Defenses
  - Managing Risks
- Trusted Computing
  - Embedded Applications
  - Tips and Tricks
- Q&A

©2019 Trusted Computing Group

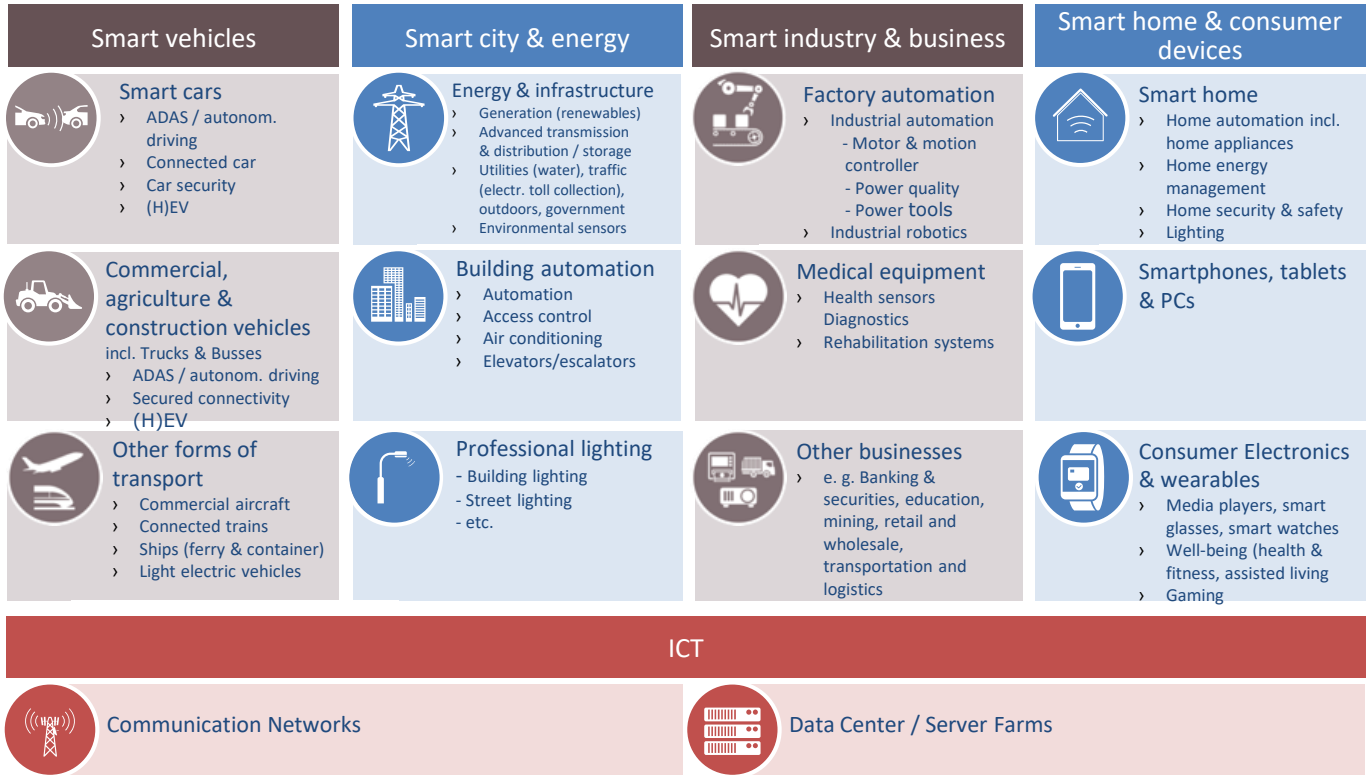
TRUSTED COMPUTING GROUP

The Move to IoT

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

IoT Trend Affects All Markets



Source: Infineon Technologies | graphics are courtesy of Infineon

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Why IoT?

Smart Home	Automotive	Industrial	ICT



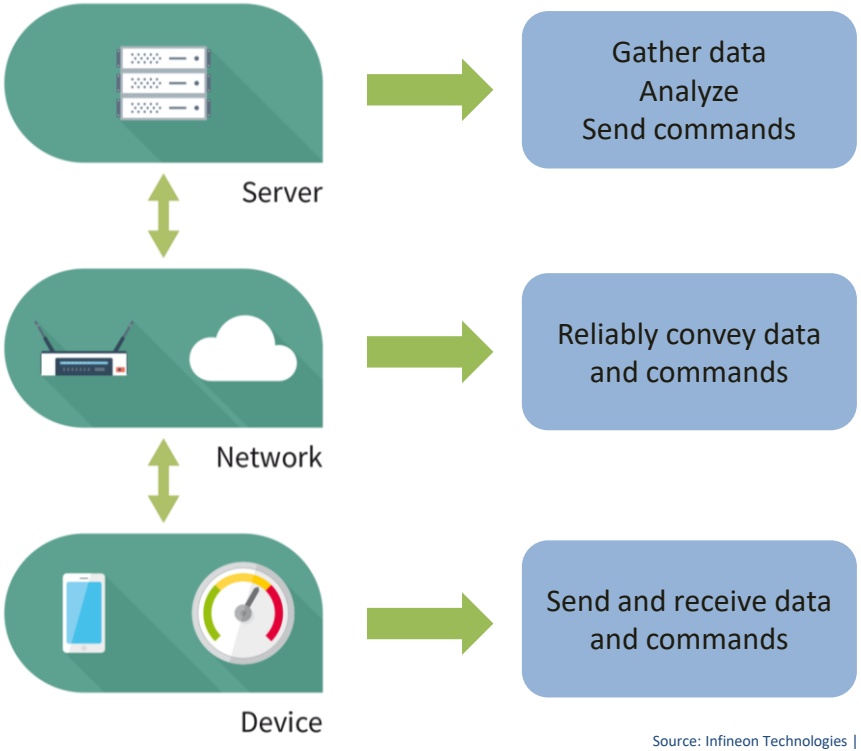
1	New capabilities and services
2	Greater efficiency
3	Increased flexibility and customization

Source: Infineon Technologies | graphics are courtesy of Infineon

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

IoT Architecture

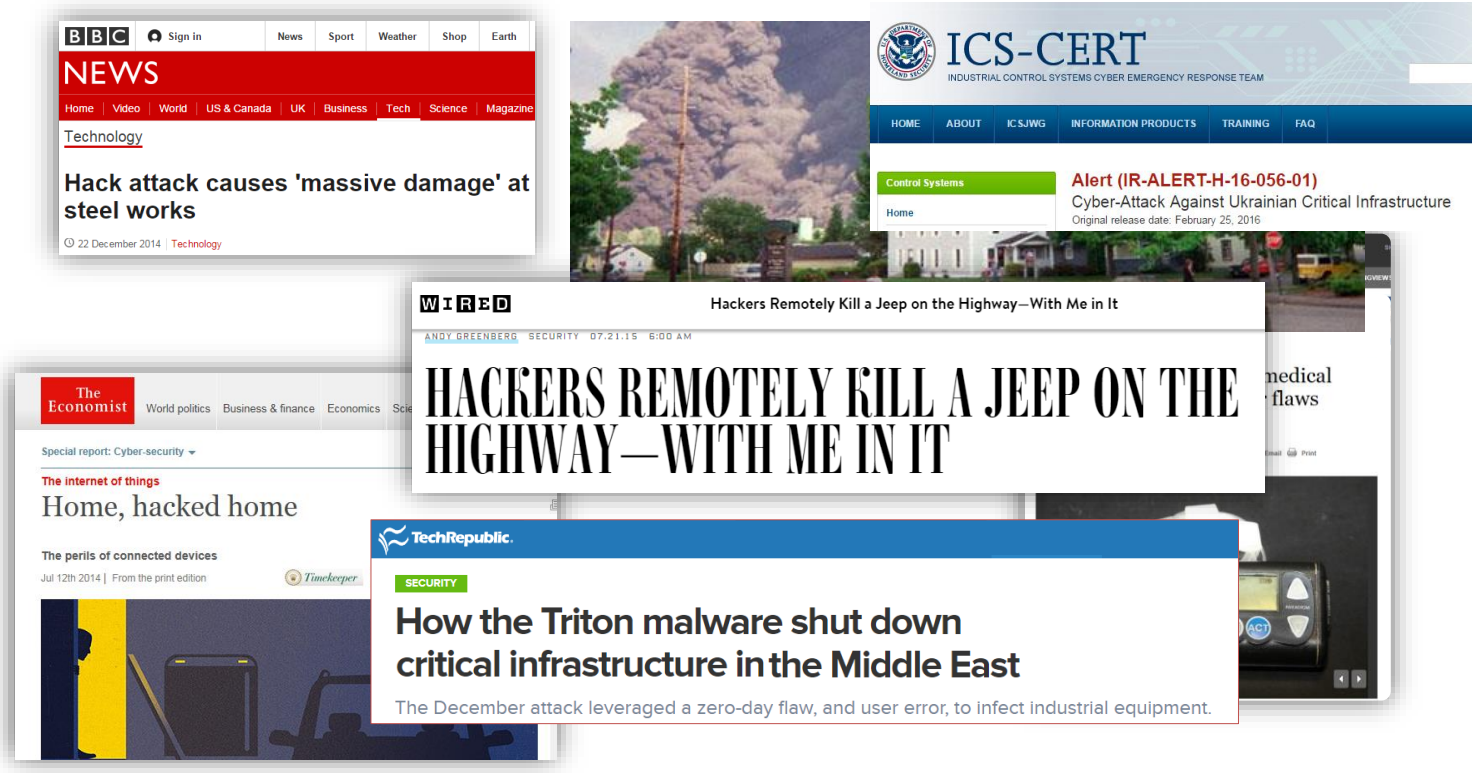


Source: Infineon Technologies | graphics are courtesy of Infineon

©2019 Trusted Computing Group

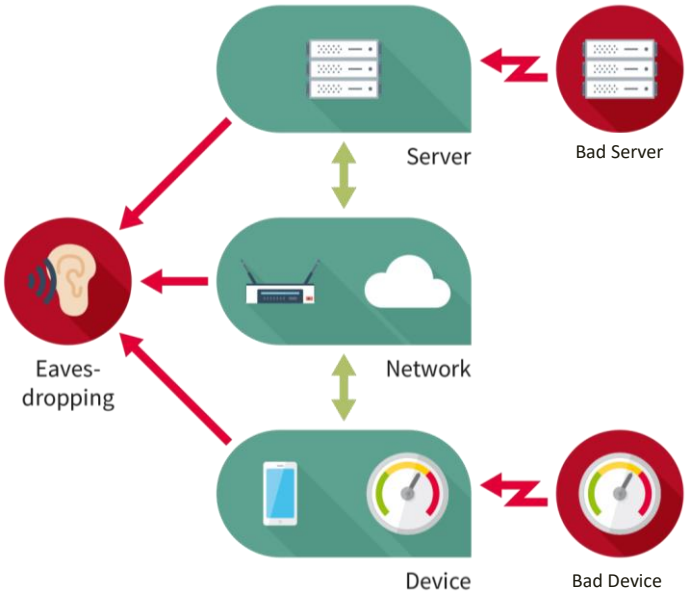
TRUSTED COMPUTING GROUP

IoT Attacks Growing



TRUSTED COMPUTING GROUP

Each Layer can be Attacked



A **Bad Server** sending incorrect commands can be used to trigger unplanned events, to send some physical resource (water, oil, electricity, etc.) to an unplanned destination, and so forth.

An **Eavesdropper** listening in on data or commands can reveal confidential information about the operation of the infrastructure.

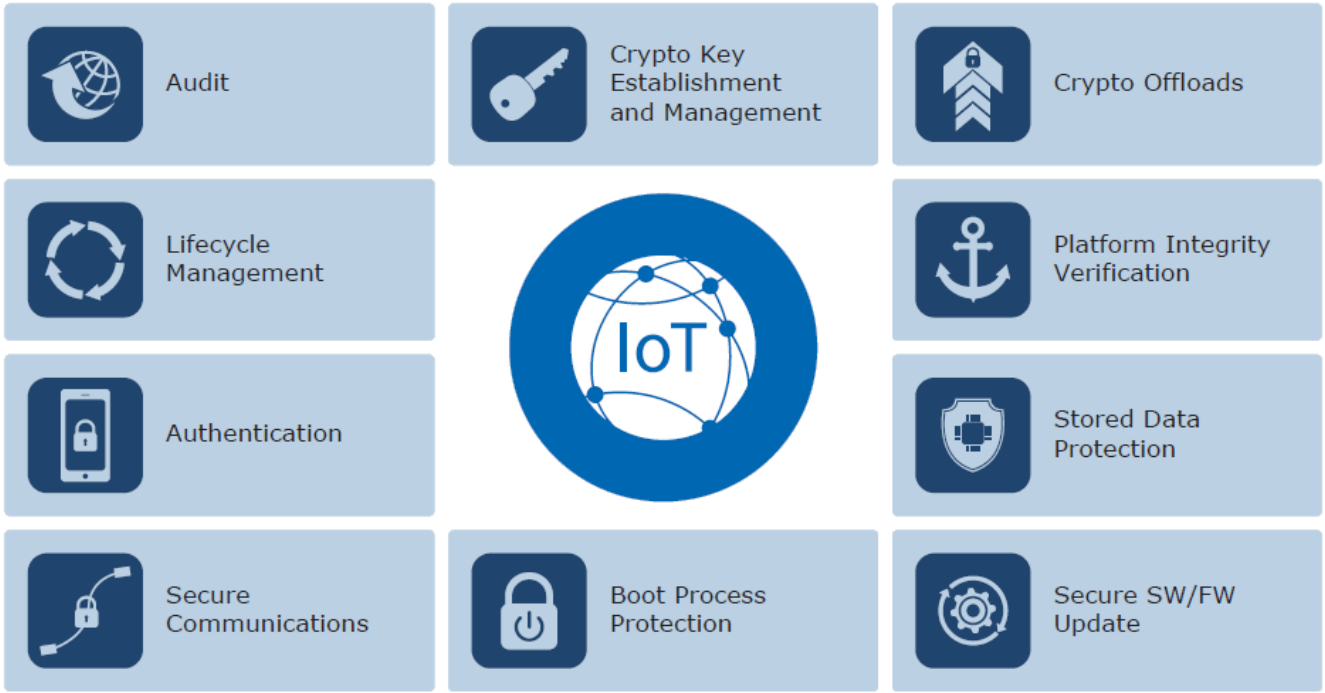
A **Bad Device** injecting fake measurements can disrupt the control processes and cause them to react inappropriately or dangerously, or can be used to mask physical attacks.

Source: Infineon Technologies | graphics are courtesy of Infineon

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

IoT Defenses



Source: Infineon Technologies | graphics are courtesy of Infineon

©2019 Trusted Computing Group

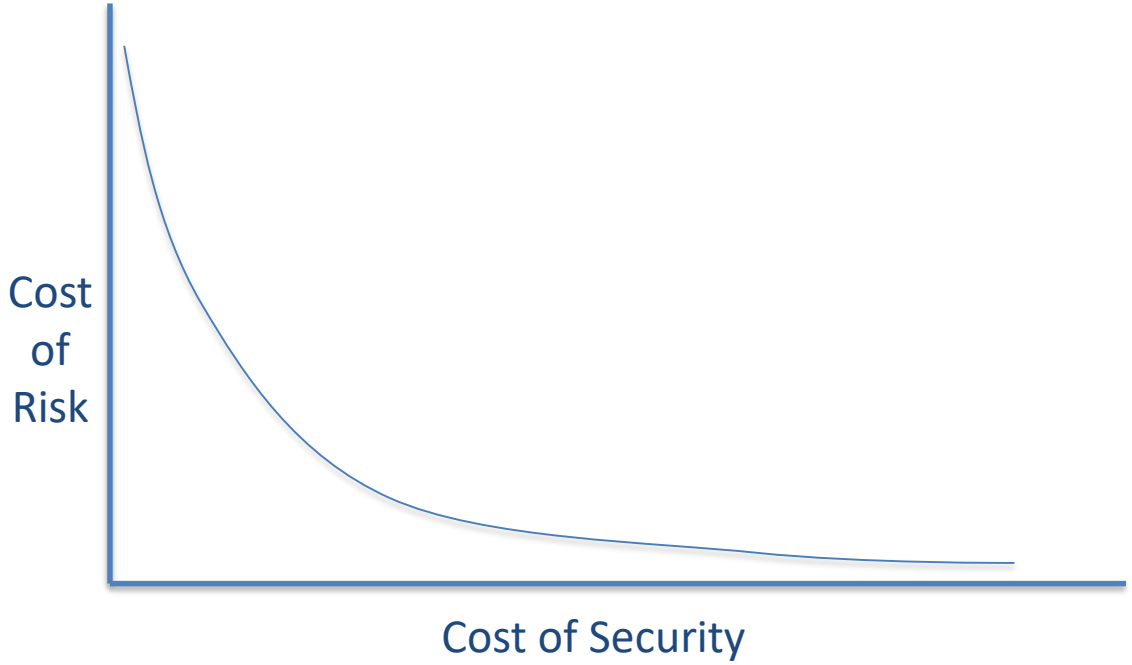
TRUSTED COMPUTING GROUP

Managing Risks

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Balancing Risk and Security



©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Risk Management

- Risk Analysis
  - Identify and assess risks
    - Analyze threats, vulnerabilities, risks (w/ impacts)
- Risk Handling
  - Avoid (e.g. skip activity)
  - Mitigate (e.g. reduce)
  - Transfer (to insurer, customer, …)
  - Accept
- Presentation to management in business terms
- Implementation
- Review risk analysis periodically or as needed

©2019 Trusted Computing Group

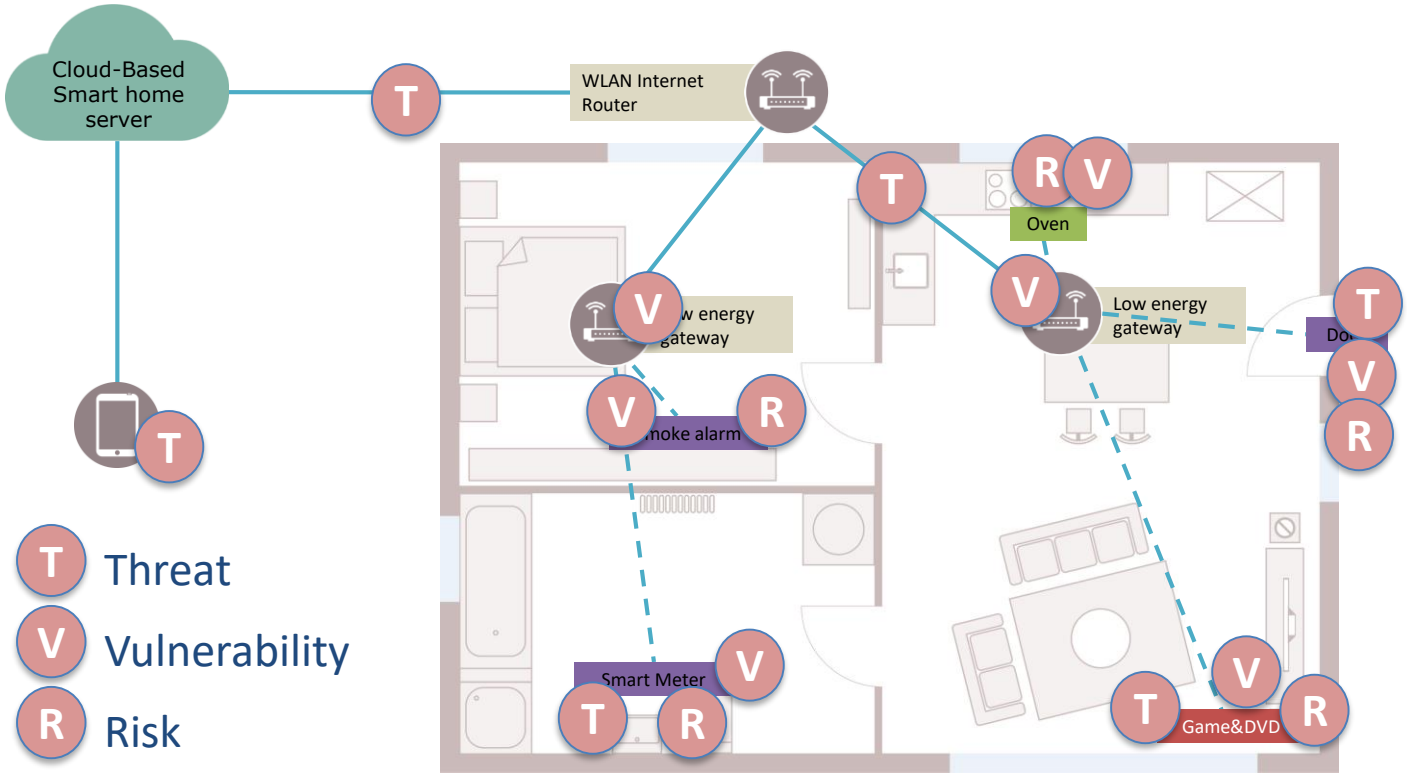
TRUSTED COMPUTING GROUP

Benefits of Risk Management

- Makes business case for IoT security
- Management understands rationale and impact
- Avoids taking on too much risk
- Avoids excessive or inefficient spending on IoT security

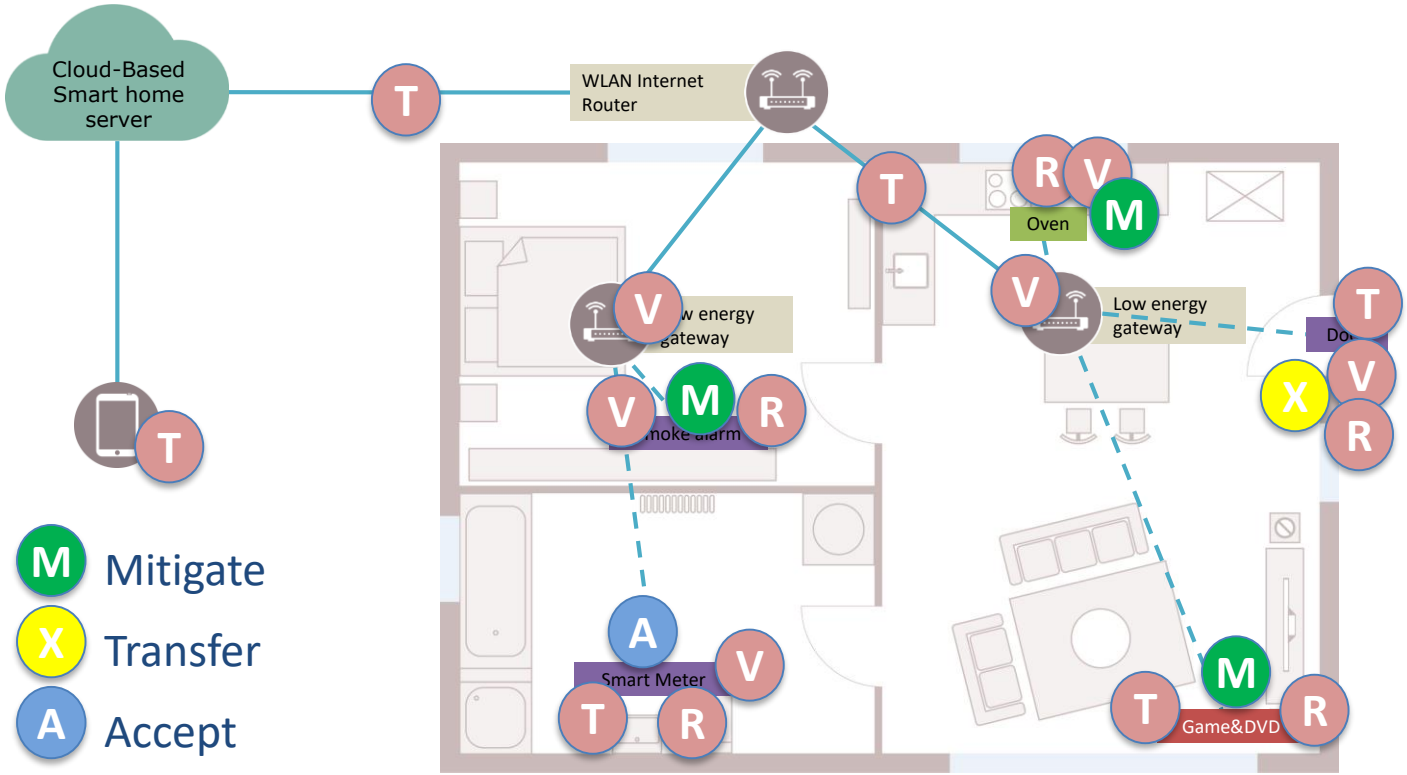
©2019 Trusted Computing Group

Risk Assessment in Smart Home



©2019 Trusted Computing Group

Risk Management in Smart Home



©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Trusted Computing

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

What is a Trusted System?



A trusted system is…

- predictable, even under stress
- trusted based on experience and/or evidence
- based on fundamental properties (identity, integrity)

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

How to Build a Trusted System

- Start with a Root of Trust (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

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Trusted Platform Module (TPM)

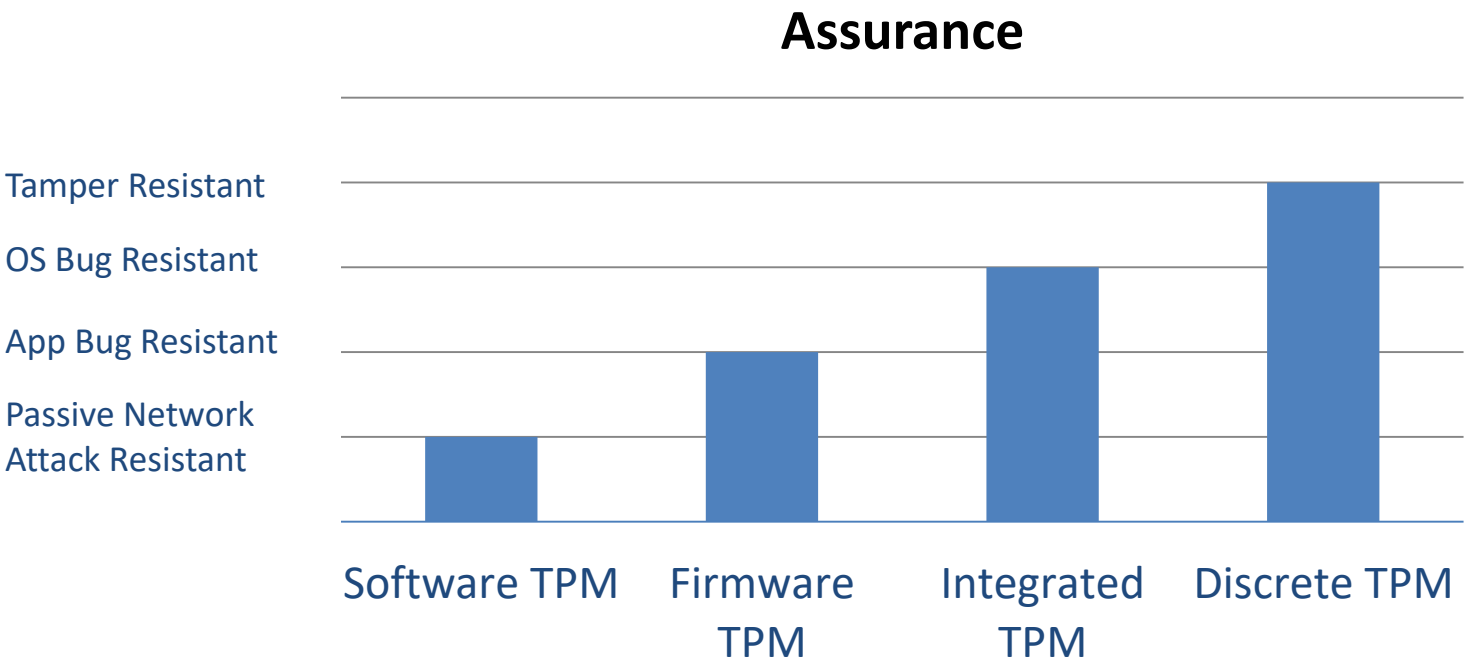


- **Standard Hardware Root of Trust**
  - TPM = ISO/IEC 11889
- **Benefits**
  - Foundation for secure software
  - Resistant to attacks/hacks
  - Built-in virtual smart card
- **Features**
  - Authentication – Identity
  - Encryption – Integrity
  - Attestation

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Levels of Assurance in TPM



©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Why Hardware?

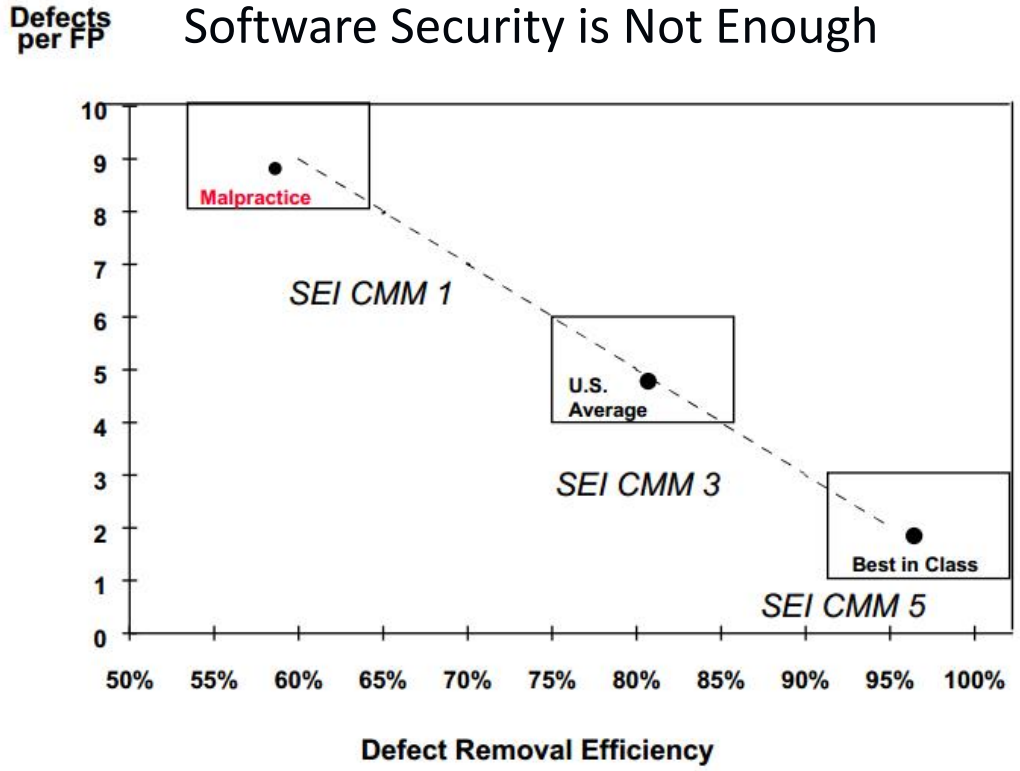


©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Why Hardware?

Software Security is Not Enough



Graph used with permission of Capers Jones.

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

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

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Embedded Applications

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Typical Applications

- Cars
- Financial Services
  - ATMs
  - Cash registers
  - Slot machines
- Industrial Control Systems
- Network Equipment
- IoT Gateways
- Hard Copy Devices

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Trusted Computing for IoT

- Use cases
- Tips and Tricks
- Implementation guidance
- Coming Soon
- IoT Security Resources

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

TCG and IoT Defenses

- Device Identity
- Secure Communication
- Random Number Generation
- Secure Software Update
- Attestation & Measured Boot
- Stored Data Protection
- Tamper Resistance
- Resale and Decommissioning
- Zero Touch Provisioning
- Audit Logging
- Remote Management
- Licensing
- Pay-Per-Use
- Etc.

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Device Identity

- Many embedded devices are ‘remote’
  - Difficult to protect or identify reliably
- Provision them with a TPM-based cryptographic identity
  - Typically, a private key and certificates stored in TPM
- Use that identity for many purposes
  - Secure communications
  - Access control
  - Remote management
  - Anti-counterfeiting
  - Licensing

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Secure Communications

- Remote communications must be protected
  - Confidentiality
  - Authentication & Authorization
  - Integrity Protection
  - Replay Protection
  - Perfect Forward Secrecy
- Use TPM-based identity with TLS, DTLS, Cloud, P2P, etc.
  - Device can prove its identity
    - Using private key and certificate stored inside the TPM
  - Device can authenticate other parties
    - Using trusted CA certificate stored in TPM

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Random Number Generation

- Protocols like TLS need high-quality random numbers
  - For cryptographic keys, nonces, initialization vectors, etc.
  - Typically generated within the embedded device itself
  - These random numbers are like passwords:
    - *If you can guess the numbers, you can break the protocol.*

- Random numbers are hard to get in embedded systems
  - Software algorithms can only generate pseudo-random sequences
  - Hardware is needed for truly random numbers

- Most TPMs contain a physical source of randomness (aka entropy) that can be used to generate good keys

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Secure Software Update

- Software needs regular updates
  - To add features, fix bugs, and repair security vulnerabilities
  - An unpatched system is highly vulnerable
    - Once a patch is released, attackers quickly develop and deploy exploits
- But software updates can cause problems
  - Reliability issues, failed updates, or incompatibilities
  - Compromise if the update mechanism is weak
- So every system needs a **secure** update mechanism

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Phases of Secure Update

- Secure Development
- Secure Update Signing
- Robust Distribution
- Secure Update Installation
- Post-Update Verification and Attestation

Trusted Computing can help with all of these!

To learn how, read our forthcoming document “TCG Guidance for Secure Update of Software and Firmware on Embedded Systems”

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

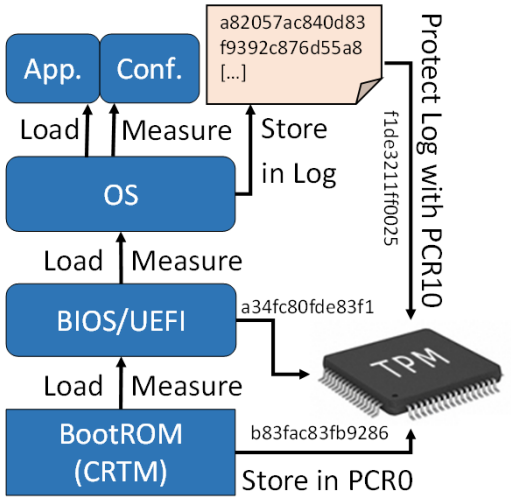
Attestation & Measured Boot

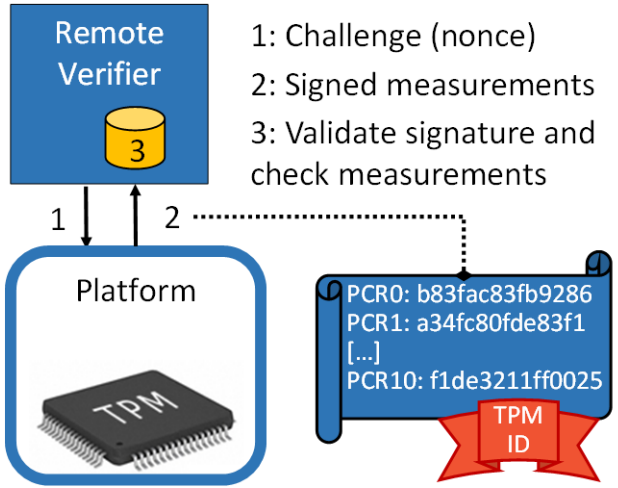
- Purpose: verify software on device
  - Cannot trust software alone to report its status
- Measured Boot
  - Securely record integrity measurement of each loaded code module
- Attestation
  - Verify loaded firmware and software
  - Can verify locally or remotely

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Attestation & Measured Boot





©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Measured Boot vs. Secure Boot

- Secure Boot works well for *deterministic* early stages of boot
  - Multi-core processors tend to be less predictable once the OS layer starts.
  - Doesn't provide evidence: is it XYZv3 or XYZv4 that was loaded?
- We want to prove exactly which firmware & software was loaded
  - Before we trust it to do something else we need to trust
- Who checks code and when?
  - With Measured Boot, verifier checks code hash during attestation
  - With Secure Boot, loader checks code signature during boot

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Stored Data Protection

- The TPM can be used to protect secrets like:
  - Passwords
  - Authentication keys
  - Disk Encryption keys or other decryption keys
  - Non-cryptographic data (formulas, configuration, code, etc.)

- Configure the TPM so it will only decrypt the secrets for use when the platform is in a specified state:
  - Known, unmodified firmware or OS
  - Specific platform configuration
  - User password entered
  - Etc.

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

Stored Data Protection

- Use an Opal drive
  - Create multiple sections with different access controls
    - Read-only
    - Read-only unless a certain key is presented
    - Inaccessible unless a certain key is presented
    - Etc.
- Consider protecting Opal keys with a TPM
  - Restrict access to those keys using TPM policies
    - Require an authorization value
    - Require certain PCR values
    - Or many other combinations

©2019 Trusted Computing Group

TRUSTED COMPUTING GROUP

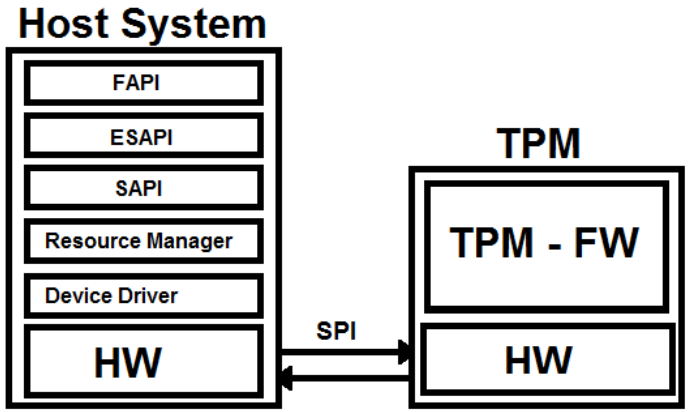
Tips & Tricks

- TPM Software Support Options
  - TCG Software Stack (TSS)
  - Mocana TrustPoint
  - WolfSSL
- Dev Boards and Other Tools
  - http://developer.trustedcomputinggroup.org

©2019 Trusted Computing Group

Why Host Software

- Host system communicates with the TPM via software
  - At various abstraction levels

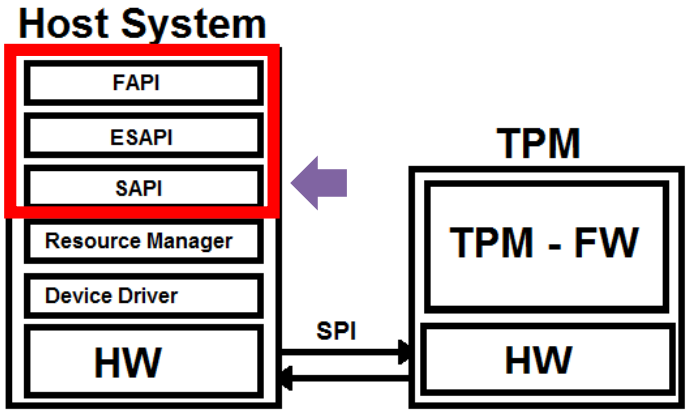


©2019 Trusted Computing Group
Copyright © Infineon Technologies AG 2019. All rights reserved. - draft -

TSS Definitions

TCG TSS working group defines the following working packages:

- **System API (SAPI)** Lowest level interface to build command byte streams and decompose response byte streams

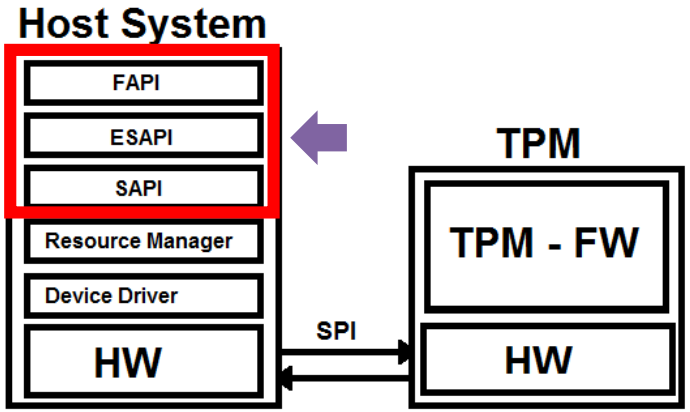


©2019 Trusted Computing Group
Copyright © Infineon Technologies AG 2019. All rights reserved. - draft -

TSS Definitions

TCG TSS working group defines the following working packages:

- **Enhanced System API (ESAPI)** sits directly above the System API to reduce the complexity of individual "system level" calls to the TPM, but allows crypto operations on the data

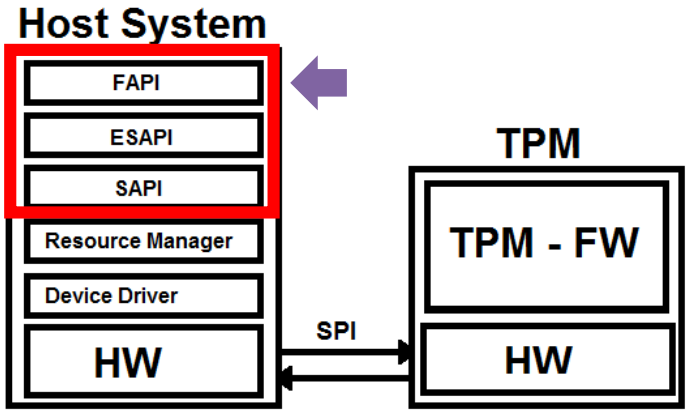


©2019 Trusted Computing Group
Copyright © Infineon Technologies AG 2019. All rights reserved.

TSS Definitions

TCG TSS working group defines the following working packages:

- **Feature/environment API (FAPI)** Provides a higher level software abstraction to application developers



©2019 Trusted Computing Group
Copyright © Infineon Technologies AG 2019. All rights reserved. - draft -

TRUSTED COMPUTING GROUP

Implementation Help

- TCG IoT Architect's Guide
  - https://trustedcomputinggroup.org/resource/architects-guide-iot-security-2/
- TCG Guidance for Securing the IoT
  - https://trustedcomputinggroup.org/resource/tcg-guidance-for-securing-iot-2/

©2019 Trusted Computing Group