TEMET
end-to-end IT security

Trusted Boot

About and Beyond PKI 2019

Gregor Walter

10.04.2019

About the speaker

Gregor Walter

Bachelor Business Informatics
CompTIA Security+

Associate Security Consultant
Working in IT Security since 2015

Specialties
IT Service Management
Data protection
Risk Management

Contact
Tel: +41 76 730 39 00
Email: gregor.walter@temet.ch

About TEMET AG

TEMET
end-to-end IT security

Mission

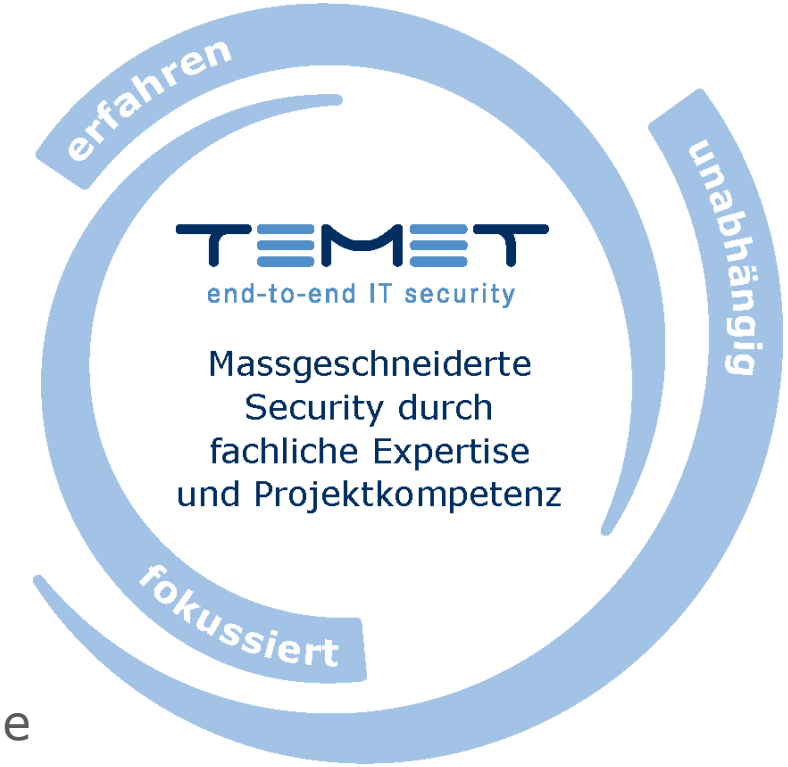
- We plan, design, and implement security projects

Unique selling propositions

- We combine technical expertise with project competence
- We concentrate on tailor-made security
- We are neutral and only committed to our customers

Company

- Founded in March 2010
- Owner-operated stock corporation
- 15 Security Consultants
- 100 customers who have a very high demand on their sustainable guarantee regarding their security



What is Trusted Boot?

- Have a safe trip! But where are we actually?
- Trust is a Strategy

© Washington Post

Trusted Boot and its flavours

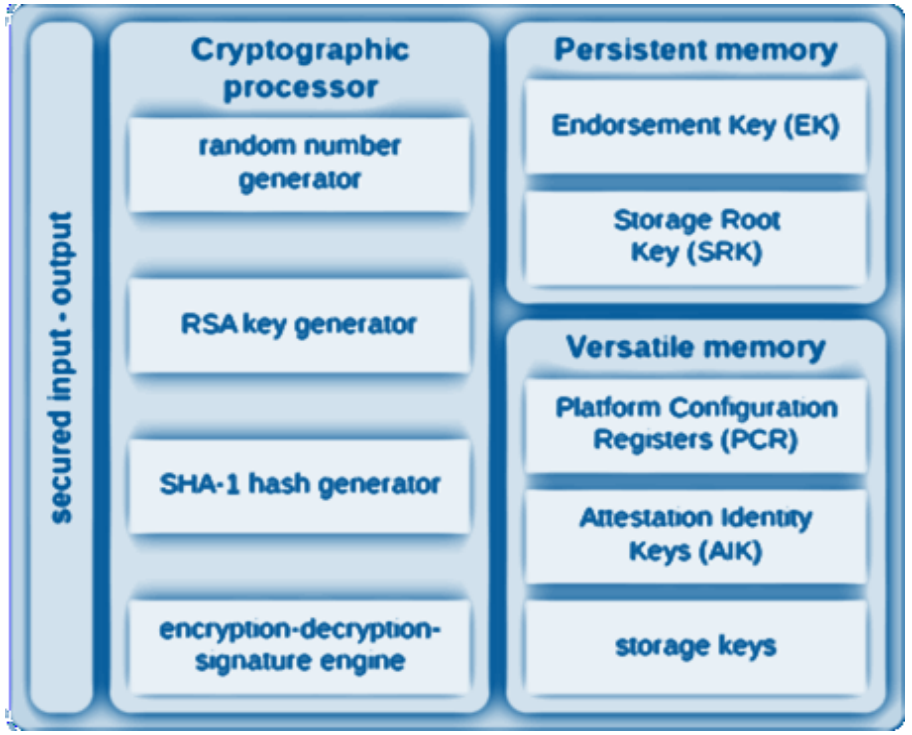
- Secure Boot for x86 & ARM
  - Requires UEFI 2.3.1 Errata C or higher
    - TPM for PC
    - T2 Chip for MAC
- Verified Boot
  - Android
- Bootchain (Secure Boot Chain)
  - iPhone

Trusted Boot Example: Secure Boot

Trusted Platform Module 2.0 Specs

- TPMs are a basic building block used in most other specifications, for providing an anchor of trust.
- They can be used for validating basic boot properties before allowing network access (TNC), or for storing platform measurements (PC Client), or for providing self-measurement to provide anchors of trust to hypervisors (Virtualization).

https://trustedcomputinggroup.org/work-groups/trusted-platform-module/



Why do we need it?

- We want to trust our platform/device…
  - …because we can’t trust the environment or we have to protect the environment
    - Integrity
    - Safety Environment
    - Critical Systems
  - …because we can’t trust the user
    - Embedded Systems
    - Commercial products

- We want to secure a Chain of Trust
  - PSE/CA/RA -> PKI

Based on trust

Where trust truly begins

- Where Trusted Boot is used (in reality)
  - IoT
  - Smart Devices
  - Next-generation mission-critical electronics (and there's a lot of them)
- RFCs / Standards & Implementations
  - Mac
  - Windows
  - Linux
  - Android
  - Vmware & Citrix / Hyper-V
  - iPhone

Trust by Design

- Incidence Vector
- Criticism
- Trusted rootkit (Boot Kit)
- Other Vulnerabilities
  - Fault Injection
  - Buffer Overflow
  - Week Cryptography

Outlook and Challenges

TEMET
end-to-end IT security

- Third Party?
- Key/Certificate Import/Export for Trusted Boot?
  - CMS(PKI)
  - IAM
- How to overcome known vulnerabilities?
  - Combination with physical security?
  - Hardware based TPM Check?

Q&A