scademy
secure coding academy

Advanced TPM Security

CL-ATP | Virtual classroom | 3 days

Variant: x86

Audience: System architects, software and firmware engineers, safety engineers
Preparedness: General C/C++ development
Exercises: Hands-on

The course will start with a brief overview of cryptographic principles, symmetric, asymmetric encryption, hash-based authentication, digital signatures, the public key architectures and the use of OpenSSL basic commands as the TPM programming will heavily build on these principles.

TPM chip features form a complex toolset in order to provide root of trust protection, measurement of integrity, secure storage and secure auditing and reporting. All these features are backed with key management, organized into special hierarchies. In order to provide a robust solution for measuring the integrity of software and build a secure boot loading procedure, the TPM chips use so-called Platform Counter Registers (PCR). Several exercises will help to understand the operation of the PCR based hash calculation mechanism. The secure and protected storage is solved by the TPM with the concept of non-volatile memory blocks addressed by NV indexes, which also have special forms, like NV Counters, Bit Fields and NV Extend Indexes. Besides these TPM specific concepts, the usual crypto primitives and how TPM supports their secure execution will also be discussed and demonstrated by hands-on exercises.

The more complex application of TPM based secure solutions will be demonstrated on a sample application framework that was developed for educational purposes. This demonstration application covers the topics of device identification, firmware integrity protection, secure boot loader, chain of trust verification remote attestation and encryption-based solutions. Within this application framework on one hand, we will be able to demonstrate the typical implementation mistakes, pitfalls of past incidents that led to exploitable security weaknesses and on the other hand provide hands-on exercises for the participants to implement their secure solutions based on TPM chip features.

The course is supplemented with real world case studies connected to the explained topics.

Outline:

- IT security and secure coding
- Practical cryptography
- Basic TPM security features

TPM based Cryptographic Operations
Firmware Integrity Protection
Remote Attestation
Principles of security and secure coding
Knowledge sources

Participants attending this course will:

Understand basic concepts of security, IT security and secure coding
Have a practical understanding of cryptography
Learn about various TPM security features
Learn about TPM based Cryptographic Operations
Understand the concept of PKI based device identification
Learn about Firmware integrity protection
Learn about Chain of trust verification
Learn about Remote attestation
Understand the concept of TPM boot loading

Related courses:

- CL-CPI - C and C++ secure coding (x86) (Onsite / Virtual classroom, 3 days)
- CL-CPA - C and C++ secure coding (ARM) (Onsite / Virtual classroom, 3 days)
- CL-CCI - Comprehensive C and C++ secure coding (x86) (Onsite / Virtual classroom, 4 days)
- CL-CCA - Comprehensive C and C++ secure coding (ARM) (Onsite / Virtual classroom, 4 days)
- CL-CMI - C and C++ security master course (x86) (Onsite / Virtual classroom, 5 days)
- CL-CMA - C and C++ security master course (ARM) (Onsite / Virtual classroom, 5 days)
- CL-CTS - Security testing native code (Onsite / Virtual classroom, 3 days)

scademy
secure coding academy

Detailed table of contents

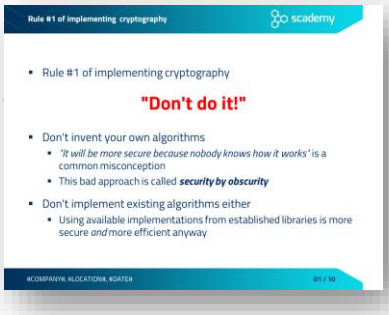
Day 1

IT security and secure coding

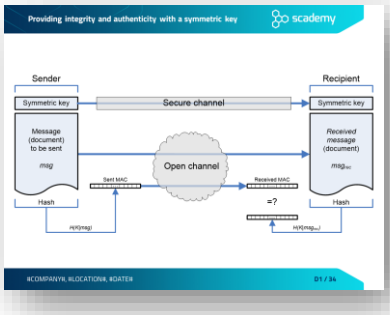
- Nature of security
- What is risk?
- IT security vs. secure coding
- From vulnerabilities to botnets and cybercrime
  - Nature of security flaws
  - From an infected computer to targeted attacks

Practical cryptography

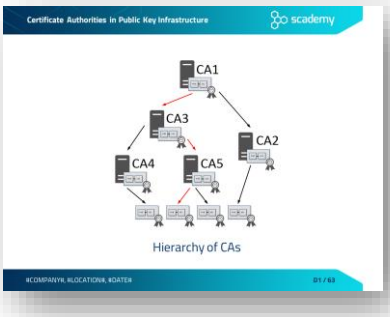
- Rule #1 of implementing cryptography.....



- Cryptosystems
  - Elements of a cryptosystem
  - FIPS 140-2
- Symmetric-key cryptography
  - Providing confidentiality with symmetric cryptography
  - Symmetric encryption algorithms
  - Modes of operation
  - Symmetric encryption with OpenSSL: encryption
  - Symmetric encryption with OpenSSL: decryption
  - Decryption with OpenSSL
- Other cryptographic algorithms
  - Hash or message digest
  - Hash algorithms
  - SHAttered
  - Hashing with OpenSSL
  - Message Authentication Code (MAC)
  - Providing integrity and authenticity with a symmetric key.....

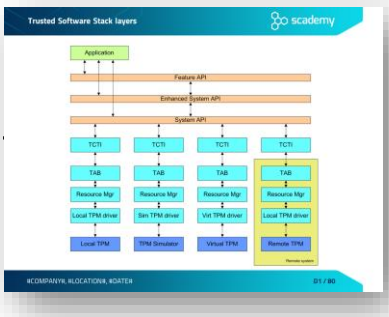


- Random number generation
  - Random numbers and cryptography
  - Cryptographically-strong PRNGs
  - Weak PRNGs in C and C++
  - Stronger PRNGs in C
  - Generating random numbers with OpenSSL
  - Hardware-based TRNGs
- Asymmetric (public-key) cryptography
  - Providing confidentiality with public-key encryption
  - Rule of thumb – possession of private key
  - The RSA algorithm
    - Introduction to RSA algorithm
    - Encrypting with RSA
    - Combining symmetric and asymmetric algorithms
    - Digital signing with RSA
    - Asymmetric encryption with OpenSSL
    - Digital signatures with OpenSSL
- Public Key Infrastructure (PKI)
  - Root of Trust Concept
    - Man-in-the-Middle (MitM) attack
    - Digital certificates against MitM attack
    - Certificate Authorities in Public Key Infrastructure
    - X.509 digital certificate
    - Certificate Revocation Lists (CRLs)
    - Online Certificate Status Protocol (OCSP)
    - Storing Private Keys (PKCS #8)
    - Generate private key with OpenSSL
    - Storing Multiple Cryptographic Keys (PKCS #12)
    - X.509 File Extensions
    - Generate CA certificate
    - View PEM encoded certificate
    - Transform PEM to DER



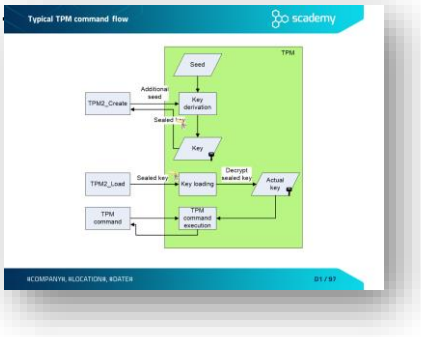
Basic TPM security features

- Introduction to TPM
  - TPM attributes
  - Types of TPM
  - Trusted Software Stack layers
  - TPM Common Criteria certification
  - TPM entities
  - TPM as the Root of Trust



- Root of Trust for Measurement
- Root of Trust for Reporting
- Root of Trust for Storage

- Hierarchies
  - Key hierarchies - common
  - Persistent key hierarchies
  - NULL hierarchy
  - Key hierarchy summary
  - Key hierarchies summary
- Key management
  - Key generation
  - Persistent keys
  - Key loading and offloading
  - Typical TPM command flow .....
  - Exercise: Create and use TPM key
  - Key ladder
  - Key attributes
  - Key attributes - duplications

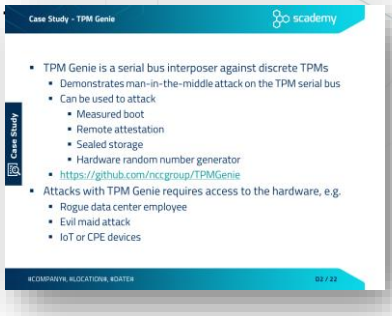


Day 2

Basic TPM security features

- Platform Configuration Register (PCR)
  - PCR value
  - Exercise: Using PCRs
  - Exercise: Calculate extended PCR value
  - Boot with PCR
  - Authorization with PCR
  - Attestation with PCR
  - Typical PCR allocation
- NV Indexes
  - NV Indexes overview
  - NV Ordinary Index
  - Storing a root public key
  - Exercise: Use NV indexes
  - NV Counter Index
  - Exercise: Use NV Counter indexes
  - NV Bit Field Index

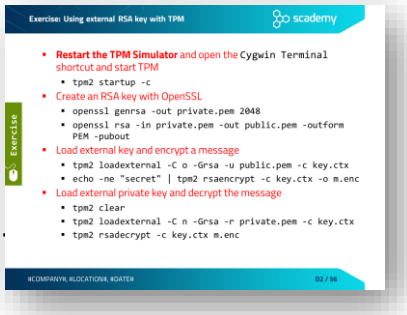
- NV Extend Index
- Hybrid Index
- TPM Genie
  - Case Study - TPM Genie
  - Case Study - TPM Genie results
  - Case Study - TPM Genie mitigations



- TPM Sessions and Authorization
  - Session and authorization overview
  - Session variations and modifiers
  - Password authorization
  - Exercise: Use NV Counter with password authorization
  - HMAC session
  - Policy session (Extended Authorization)
  - Policy authorization lifecycle
  - Exercise: Use NV Counter with policy authorization
  - Session type summary
  - Authorizations and sessions
  - Context management
- Auditing TPM Commands
  - TPM audit
  - Audit TPM command with audit session
  - Exclusive audit
- Password management
  - Password management with TPM

TPM based Cryptographic Operations

- Symmetric encryption with TPM
  - Symmetric encryption algorithms
  - Modes of operation
  - Comparing the modes of operation
  - Symmetric-key encryption with TPM
  - Exercise - TPM communication
- Asymmetric (public-key) cryptography
  - Providing confidentiality with public-key encryption
  - Rule of thumb - possession of private key
  - RSA variations in TPM 2.0
  - Exercise: Using external RSA key with TPM



  - ECC variations in TPM 2.0

- Dynamic data protection
  - Integrity protection with HMAC
  - Exercise - HMAC validation
  - Certification based verification
  - Exercise: Certify that a key is generated by the TPM
  - Exercise: Verify the generated signature
  - Hands-on PKI with TPM
  - Exercise - OpenSSL
- PKI based device identification
  - Root of trust concept
  - Loading or generating root values
  - Endorsement key certificate
  - Designing, manufacturing and personalization processes
  - Different stakeholders, manufacturer, platform owner, application developer
  - Certification process

Firmware Integrity Protection

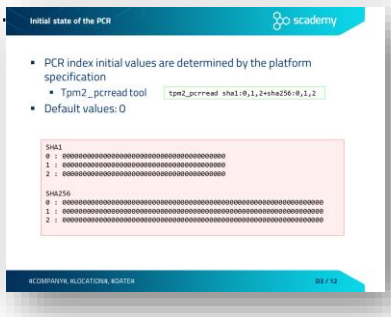
- Software Integrity Concepts
- Code Signing
- Trust on first use
- Extendible Hashing
  - Extendible hash during bootloading
- Firmware update mechanisms
  - Firmware update introduction
  - Over-the-air updates
  - Firmware update challenges
- Downgrade Attack
  - Anti-rollback protection
  - BYOvD – Bring Your Own Vulnerable Driver
- Security Counter
  - Security counter requirements
- Chain of trust verification
  - Public Key Infrastructure (recap)
  - Certificate Authorities in Public Key Infrastructure
  - Certificate handling
  - Certificate provisioning
  - TPM key attestation

- How does TPM key attestation work?
- Endorsement hierarchy
- Revocation
- Timestamps
- TPM timekeeping
- Attacks against Timestamps

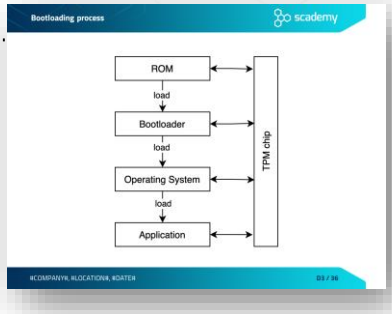
Day 3

Remote Attestation

- Attestation definition
- Main roles in attestation
- Identity checking
- Privacy considerations
- Hypothetical example
- Ways to resolve privacy issues
- TPM attestation
  - TPM attestation / Platform configuration registers
  - Platform configuration registers
  - Initial state of the PCR
  - Extending PCR indices
  - Golden or reference PCR
  - Calculating the golden PCR - 1
  - Calculating the golden PCR - 2
  - Requirements for remote attestation
  - Entities in the attestation process
  - Service registration
  - Service request – Platform Anonymous Identity Validation
  - Service request – Platform Software State Validation
  - Service delivery
  - Remote attestation application
  - Remote attestation application diagram
  - Remote attestation
  - Exercise – Remote attestation
  - Exercise – Calculate pcrDigest value



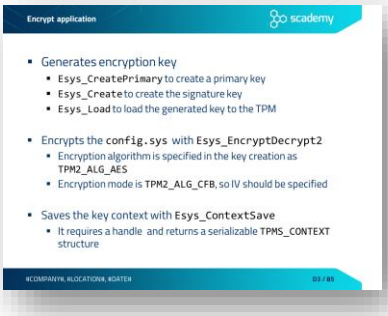
- Secure bootloading process
  - The goal of secure bootloading
  - TPM and secure bootloading
  - Apple's iOS secure bootloading
    - Apple's Secure Bootloading process explioted
  - Typical secure bootloading process
    - Bootloading process
    - Description of the Bootloading process



- Example bootloading process
  - Sources of the parts of Bootloading process
  - Executing the example bootloading process
  - Exercise – Start bootloading process
  - Exercise – TPM provisioning
  - Exercise – Start an application
  - Output of the bootloading process
  - ROM
    - Description of the ROM – Public key integrity check
    - Description of the ROM – Checking bootloader's signature
    - Description of the ROM – Measure bootloader code
    - Description of the ROM – Signature verification diagram
    - Altering the signed bootloader
    - Exercise - Altering the signed bootloader
    - Bypassing protections in ROM
    - Exercise – bypassing protection in ROM
    - Exercise – bypassing protection in ROM (TOCTTOU)
  - Apple's macOS secure bootloading
    - macOS Secure Bootloading Process
  - Bootloader
    - Description of the Bootloader
  - Operating System
    - Description of the OS
    - Buffer overflow exploit
    - Exercise - Buffer overflow
  - What do you use to get elevated privileges on Linux?
  - Imagine what would happen if they found a bug in sudo…
    - Case Study – Sudo bug
    - Exploiting the Sudo bugCVE-2021-3156
    - Exercise – Sudo bug

- Firmware Update Application
  - Firmware update application
  - Firmware update application diagram
  - Firmware update
  - Exercise - Firmware update
  - Exercise – Downgrade protection

- Encrypt/Decrypt Applications
  - Encrypt application
  - Encrypt application diagram
  - Decrypt application
  - Encrypt/Decrypt with the TPM chip
  - Exercise – Encrypt with TPM
  - Exercise – Decrypt with TPM
- NV Indexes Application
  - NV Indexes application
  - NV Indexes application diagram
  - Using NVIndexes
  - Exercise – Write and read NV-Indexes



Principles of security and secure coding

- Matt Bishop's principles of robust programming
- The security principles of Saltzer and Schroeder

Knowledge sources

- TPM 2.0 Library specification
- TPM 2.0 Library specification - References

- References
- Recommended books - TPM 2.0