Training: SCADEMY
CL-CHS Crypto chip-set security

TRAINING GOALS:

The biggest challenge for professionals working on design and development of crypto chip-sets is to be continuously up-to-date regarding the attack methods and their mitigation. Serving them, this course explains various physical and logical attacks on security chips, possible countermeasures and best practices.

Regarding physical attacks, the passive attacks are detailed through optical reverse engineering and various side channel analysis methods, while active attacks are discussed with special emphasis on fault injection, Focused Ion Beams and hardware Trojans. The very powerful passive and active combined attack (PACA) type is introduced through the practical example of RSA implementations. Discussion of logical attacks not only covers practical attacks against specific cryptographic algorithm implementations, but also the relevant programming bugs and mitigation techniques like buffer overflow or integer problems are introduced.

Finally, a set of guidelines is assembled to follow by engineers working in this field, and the testing methods are presented that can help to find and avoid the discussed security flaws and vulnerabilities.

Participants attending this course will:

- Understand basic concepts of security, IT security and secure coding
- Have a practical understanding of cryptography
- Understand the requirements of secure communication
- Understand essential security protocols
- Understand some recent attacks against cryptosystems

Audience:

Developers, architect and testers of secure hardware components

CONSPECT:

- IT security and secure coding
  - Nature of security
  - What is risk?
  - IT security vs. secure coding

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Nature of security flaws
- Reasons of difficulty

- Requirements of secure communication
  - Security levels
  - Secure acknowledgment
    - Malicious message absorption
      - Feasibility of secure acknowledgment
      - The solution: Clearing Centers
    - Inadvertent message loss
  - Integrity
    - Error detection - Inadvertent message distortion (noise)
      - Modeling message distortion
      - Error detection and correction codes
    - Authenticity - Malicious message manipulation
      - Modeling message manipulation
      - Practical integrity protection (detection)
    - Non-repudiation
      - Non-repudiation
    - Summary
      - Detecting integrity violation
  - Confidentiality
    - Model of encrypted communication
    - Encryption methods in practice
    - Strength of encryption algorithms
  - Remote identification
    - Requirements of remote identification
  - Anonymity and traffic analysis
    - Model of anonymous communication
    - Traffic analysis
    - Theoretically strong protection against traffic analysis
    - Practical protection against traffic analysis
  - Summary
    - Relationship between the requirements

- Practical cryptography
  - Rule #1 of implementing cryptography
  - Cryptosystems

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Elements of a cryptosystem
- Symmetric-key cryptography
  - Providing confidentiality with symmetric cryptography
  - Symmetric encryption algorithms
  - Modes of operation
- Other cryptographic algorithms
  - Hash or message digest
  - Hash algorithms
  - SHAttered
  - Message Authentication Code (MAC)
  - Providing integrity and authenticity with a symmetric key
  - Random number generation
    - Random numbers and cryptography
    - Cryptographically-strong PRNGs
    - Hardware-based TRNGs
- Asymmetric (public-key) cryptography
  - Providing confidentiality with public-key encryption
  - Rule of thumb – possession of private key
  - Combining symmetric and asymmetric algorithms
- Public Key Infrastructure (PKI)
  - Man-in-the-Middle (MitM) attack
  - Digital certificates against MitM attack
  - Certificate Authorities in Public Key Infrastructure
  - X.509 digital certificate

- Security protocols
  - The TLS protocol
    - SSL and TLS
    - Usage options
    - Security services of TLS
    - SSL/TLS handshake
  - Protocol-level vulnerabilities
    - BEAST
    - FREAK
    - FREAK – attack against SSL/TLS
    - Logjam attack
  - Padding oracle attacks

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

        - Adaptive chosen-ciphertext attacks
        - Padding oracle attack
        - CBC decryption
        - Padding oracle example
        - Lucky Thirteen
        - POODLE
    - Simple physical attacks and protections
        - Passive, active and PACA attacks
        - Physical access to the chip
        - Levels of invasiveness
        - Protection principles
    - Passive physical attacks
        - Reverse Engineering
            - Reverse engineering of integrated circuits
            - Decapsulation
            - Decapsulation in practice
            - Deprocessing
            - Removal of the passivation layer
            - Different lasers against different passivation layers
            - Optical reverse engineering
            - Requirements towards the optical microscope
            - Bonding to chip surface
        - Physical protection of the chip
            - Multi-layering
            - Protective layer
            - Examples of protective shields
            - Planarization
            - Confusing attackers
            - Obfuscating the design
            - Shuffling the internal bus lines
            - Internal memory encryption
        - Side channel analysis
            - Power analysis attacks
            - Process of a power analysis attack
            - Modeling power consumption
        - Simple power analysis

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Examples for simple power analysis
- Example power consumption of DES encryption
- SPA against RSA
- Countermeasures against SPA

- Differential power analysis
  - Process of a DPA attack
  - DPA attack – the difference function
  - DPA attack – visible correlation
  - DPA attack – spikes in differential traces
  - Influence of noise and measurement errors on DPA attack
  - DPA against DES
    - DES algorithm
    - Feistel function
    - DPA against DES
  - Improved DPA attacks
    - DPA enhancements
    - Correlation power analysis (CPA)
    - Process of CPA attack

- Protections against power analysis attacks
  - Protection measures against power analysis
  - Hiding techniques
  - Hiding: adding noise, desynchronization
  - Hiding: dual-rail precharge logic (DRP)
  - Hiding, DRP: sense amplifier based logic (SABL)
  - Hiding: current mode logic (CML)
  - Masking: masked dual rail precharge logic (MDPL)
  - Limitations of PA resisting logic styles

- Electromagnetic analysis
  - Electromagnetic emanation
  - Simple electromagnetic analysis (SEMA)
  - Electromagnetic analysis countermeasures

- RSA timing attack
  - Implementation of encoding/decoding in RSA
  - Fast exponentiation
  - Differences in execution times
  - RSA timing attack

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Measurements
- RSA timing attack – principles
- Correlation of total and partial execution times
- RSA timing attack – in practice
- Example – RSA measurements
- Example – Partial execution times are calculated for first i bits
- Example – Candidates are ordered according to the variance
- The RSA timing attack algorithm
- Practical exploitation using the RSA timing attack
- Attacking SSL/TLS servers
- Protection against timing attacks
  - Hiding: RSA timing attack countermeasures
  - Masking: using blind signature
  - Real RSA implementations
  - Summary – lessons learnt from side channel attacks
  - Security evaluation of side-channel protections

- Active physical attacks
  - Manipulating the circuit layout
    - Focused ion beam (FIB) workstation
    - Milling and cutting using FIB
    - Creation of test points
    - FIB accessibility
  - Hardware trojan horses
    - Hardware trojan horse (HTH) risk factors
    - Taxonomy of trojans
    - Physical characteristics
    - Prevention – dead space removal
    - Design facilitated logic testing
    - Transparent mode
    - IC fingerprint / transient power-based analysis
    - IC fingerprint / timing-based analysis
    - Detection and correction using DEFENSE methodology
  - Fault injection attacks
    - Fault injection attacks (FIA)
    - Fault injection models
    - Practical attacks

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Microprobing
- Microprobe station parts
- Case study – reading the memory using chip surgery
- Light, X-Ray, electromagnetic radiation
- UV light attack – resetting the fuse
- UV attack – locating the fuse
- Effect of UV light on EEPROM and floating gate devices
- Optical fault injection – white light
- Pulsed laser
- Tampering with temperature – data remanence
- Tampering with temperature – cooling
- Localized heating
- Clock glitch attack
- Execution of the attack
- A sample attack against a Motorola microcontroller
- Assembly code of the attack
- Power glitching
- Power glitch examples – attack on Motorola microcontroller
- Power glitch examples – microchip PIC16F84 microcontroller

- Fault injection into RSA with CRT optimization
  - Chinese Remainder Theorem
  - RSA using CRT – mathematical background
  - RSA using CRT – the algorithm
  - Bellcore attack on RSA with CRT
  - Bellcore attack algorithm
  - Lenstra attack on RSA with CRT
  - Non permanent bit-flip attack on RSA without CRT
  - RSA non permanent bit-flip attack
  - Detection of fault injection attacks

- Passive and active combined attacks
  - PACA against RSA with blinding and doublechecking
  - SPA/DPA resistant RSA blinding
  - Power traces before and after fault injection
  - Fault injection – word by word multiplication
  - PACA resistant RSA with CRT and Montgomery’s Ladder
  - Montgomery’s Ladder: improved square and multiply always

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- FA-SPA resistant modular exponentiation
- FA-SPA resistant RSA with CRT
- PACA protection – detect and derive
- DnD example – protecting the secret key
- Fault injection into ECC
  - Elliptic Curve Cryptography (ECC)
  - Elliptic curves
  - Addition and multiplication operations over elliptic curves
  - Discrete Logarithm Problem (DLP)
  - ECC fault injection attack
  - ECC attack method
- DES final round attack
  - DES algorithm
  - Feistel function
  - DES final round with permutation compensation
  - DES final round attack principle
  - DES final round attack algorithm
  - Completing the DES attack
- AES fault injection attacks
  - Advanced Encryption Standard (AES)
  - AES operation
  - AES algorithm
  - AES final round differential injection attack principle
  - Giraud's differential fault analysis attack
  - Blömer-Seifert fault attack on AES-128
  - AES pre-whitening step attack principle
  - Blömer-Seifert fault attack on AES
  - Assessment of the Blömer-Seifert fault attack on AES

- Special security functions – Requirements and solutions
  - Physically unclonable functions
    - Main PUF properties
    - PUF types
    - Secret key generation with PUFs
    - Further PUF applications
  - JTAG attacks and protections
    - JTAG overview

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- JTAG based attacks
- Defending against JTAG attacks

- Miscellaneous protection measures
  - Keeping the memory programming method secret
  - Unique chip ID
  - Bus scrambling
  - Sensors
  - Further design guidelines

- Principles of security and secure coding
  - Matt Bishop’s principles of robust programming
  - The security principles of Saltzer and Schroeder

REQUIREMENTS:

Professional

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by SCADEMY (course completion).

TRAINER:

Authorized SCADEMY Trainer

ADDITIONAL INFORMATION:

Training come with a number of easy-to-understand exercises providing live hacking fun. By accomplishing these exercises with the lead of the trainer, participants can analyze vulnerable code snippets and commit attacks against them in order to fully understand the root causes of certain security problems. All exercises are prepared in a plug-and-play manner by using a pre-set desktop virtual machine, which provides a uniform development environment.

SCADEMY together with online application security educational platform AVATAO (more about AVATAO www.avatao.com) for each of participant SCADEMYs authorized training adds the 30 days business AVATAO trial holds the following package:

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- 30-day customized free trial

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007