Training: SCADEMY
# CL-ANW Network security and secure communication

## TRAINING GOALS:

Implementing a secure networked application can be difficult, even for developers who may have used various cryptographic building blocks (such as encryption and digital signatures) beforehand. In order to make the participants understand the role and usage of these cryptographic primitives, first a solid foundation on the main requirements of secure communication – secure acknowledgement, integrity, confidentiality, remote identification and anonymity – is given, while also presenting the typical problems that may damage these requirements along with real-world solutions.

As a critical aspect of network security is cryptography, the most important cryptographic algorithms in symmetric cryptography, hashing, asymmetric cryptography, and key agreement are also discussed. Instead of presenting an in-depth mathematical background, these elements are discussed from a developer's perspective, showing typical use-case examples and practical considerations related to the use of crypto, such as public key infrastructures. Security protocols in many different areas of secure communication are introduced, with an in-depth discussion on the most widely-used protocol families such as IPSEC and SSL/TLS.

Finally, as XML technology is central for data exchange by networked applications, the security aspects of XML are described. This includes the usage of XML within web services and SOAP messages alongside protection measures such as XML signature and XML encryption – as well as weaknesses in those protection measures and XML-specific security issues such as XML injection, XML external entity (XXE) attacks, XML bombs, and XPath injection.

Participants attending this course will:

- Understand basic concepts of security, IT security and secure coding
- Understand the requirements of secure communication
- Learn about network attacks and defenses at different OSI layers
- Have a practical understanding of cryptography
- Understand essential security protocols
- Understand some recent attacks against cryptosystems
- Learn about typical coding mistakes and how to avoid them
- Get information about some recent vulnerabilities in the Java framework
- Learn about XML security
- Get information about some recent related vulnerabilities
- Get sources and further readings on secure coding practices



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

Audience:

Network engineers and developers

## CONSPECT:

- 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
    - Reasons of difficulty
    - From an infected computer to targeted attacks
    - The Seven Pernicious Kingdoms
    - OWASP Top Ten 2017
- 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



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

- 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

- Network security
  - Overview
    - The TCP/IP stack
  - Data Link layer
    - Sniffing attacks
      - What is a sniffer?
      - A revision on hubs and switches
      - MAC flooding
    - Spoofing
      - Spoofing attacks
      - Address Resolution Protocol (ARP)
      - ARP spoofing
      - Dynamic Host Configuration Protocol (DHCP)
      - DHCP starvation
    - Man-in-the-Middle
      - Man-in-the-Middle
      - Man-in-the-Middle with ARP poisoning
      - Rogue DHCP server
    - Attacks against VLANs
      - VLANs, Native VLANs, DTP
      - VLAN hopping, Switch spoofing
      - Double tagging
    - Data Link layer protections
      - Segmentation
      - Detecting sniffing tools
      - VLAN security



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

- Port Security
- DHCP snooping
- Dynamic ARP Inspection (DAI)
- Private VLANs

- Network security
  - Network layer
    - IP address spoofing
    - Maximum Transmission Unit
    - Fragmentation attack
    - ICMP attacks
      - Internet Control Message Protocol (ICMP)
      - Smurf attack
      - Ping of death
      - Route hijacking
    - Network layer protections
      - Ingress filtering, Egress filtering
      - IP Source Guard
      - Firewalls
      - Packet filtering firewalls
      - Intrusion Detection/Prevention Systems
  - Transport layer
    - Transmission Control Protocol (TCP)
      - Transmission Control Protocol
      - SYN flood
      - TCP session hijacking
    - User Datagram Protocol (UDP)
      - User Datagram Protocol
      - UDP flooding
    - Routing protocols
      - Routing protocols
    - Fingerprinting and service detection
      - connect() scan
      - SYN scan
      - FIN scan
      - X-mas scan
    - Transport layer protection



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

        - SYN proxy
        - SYN cookies
        - Stateful firewalls
        - Routing protocol security
    - Application layer
        - Domain Name System
        - DNS Spoofing
        - Application layer protections
            - Application-level firewalls
            - Application layer security solutions
            - Secure protocols
- Practical cryptography
    - Rule #1 of implementing cryptography
    - Cryptosystems
        - Elements of a cryptosystem
        - Java Cryptography Architecture / Extension (JCA/JCE)
        - Using Cryptographic Service Providers
    - Symmetric-key cryptography
        - Providing confidentiality with symmetric cryptography
        - Symmetric encryption algorithms
        - Modes of operation
        - Private (symmetric) key cryptography in Java
    - Other cryptographic algorithms
        - Hash or message digest
        - Hash algorithms
        - SHAttered
        - Hashing in Java: MessageDigest class
        - MAC and password-based encryption in Java: Mac class
        - Message Authentication Code (MAC)
        - Providing integrity and authenticity with a symmetric key
        - Random number generation
            - Random numbers and cryptography
            - Cryptographically-strong PRNGs
            - Weak and strong PRNGs in Java
            - Hardware-based TRNGs
            - Exercise RandomTest



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

- Using random numbers in Java – spot the bug!
- Testing random number generators
- Exercise – Testing random number generators

- 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
    - Exercise Sign
- 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
  - The Java Keystore (JKS)
  - Java Certification Path (CertPath)
- Web of Trust (WoT)
  - Web of Trust (WoT) – introduction
  - WoT example
  - Challenges of Web of Trust

- Security protocols
  - Secure network protocols
  - Specific vs. general solutions
  - IPSEC protocol family
    - IPSEC standards
    - Security Association (SA)
    - Message formats
    - AH packet structure
    - ESP packet structure
    - Protected channels
    - More complex set-ups
    - Traffic control
    - SA structure



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

- Key management
- The TLS protocol
  - SSL and TLS
  - Usage options
  - Security services of TLS
  - SSL/TLS handshake
  - Java Secure Socket Extension (JSSE)
- Cryptographic vulnerabilities
  - Protocol-level vulnerabilities
    - BEAST
    - FREAK
    - FREAK – attack against SSL/TLS
    - Logjam attack
  - Padding oracle attacks
    - Adaptive chosen-ciphertext attacks
    - Padding oracle attack
    - CBC decryption
    - Padding oracle example
    - Lucky Thirteen
    - POODLE
- Common coding errors and vulnerabilities
  - Input validation
    - Input validation concepts
    - XML security
    - XML injection
      - (Ab)using CDATA to store XSS payload in XML
      - Exercise – XML injection
      - Protection through sanitization and XML validation
    - Abusing XML Entity
      - XML Entity introduction
      - XML bomb
      - Exercise – XML bomb
      - XML external entity attack (XXE) – resource inclusion
      - XML external entity attack – URL invocation
      - XML external entity attack – parameter entities
      - Exercise – XXE 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

- Preventing entity-related attacks
- Case study – XXE in Google Toolbar
- Integer problems
  - Representation of negative integers
  - Integer overflow
  - Exercise IntOverflow
  - What is the value of Math.abs(Integer.MIN_VALUE)?
  - Integer problem – best practices
- Improper use of security features
  - Typical problems related to the use of security features
  - Password management
    - Exercise – Weakness of hashed passwords
    - Password management and storage
    - Special purpose hash algorithms for password storage
    - Argon2 and PBKDF2 implementations in Java
    - bcrypt and scrypt implementations in Java
    - Password audit
    - Exercise – using John the Ripper
    - Case study – the Ashley Madison data breach
    - Typical mistakes in password management
    - Exercise – Hard coded passwords
- Some well-known implementation problems
  - Case study – Heartbleed
    - TLS Heartbeat Extension
    - Heartbleed – information leakage in OpenSSL
    - Heartbleed – fix in v1.0.1g
- Knowledge sources
  - Secure coding sources – a starter kit
  - Vulnerability databases
  - Java secure coding sources
  - Recommended books – Java
  - Recommended books – cloud security

## REQUIREMENTS:

Network engineering, general software development



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

## 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:

- 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