Crypto Risk

Standard Syllabus

Taught by: Dr Graham Steel

Day 1 - Crypto Risk

Audience

- Security/Risk managers
- Application Security auditors
- Pen-testers
- Security Architects

Required background

The course is for professionals working in application security. Some basic familiarity with cryptography is required to get the most out of the training. There is no practical exercise, so up to date coding skills are not required. Examples will be given in Java.

What you will learn

- When to use crypto and why
- Mistakes to avoid in common operations and protocols
- Best practices for key-management, and common vulnerabilities
- Real-world examples of attacks exploiting crypto flaws to obtain secret data, achieve remote code execution, reset passwords to known values, etc.

Day 1 Syllabus

1. Cryptography recap

- Why (not) use cryptography?
- Not just SSL - how crypto is found everywhere in modern applications

2. Encryption

- Algorithms
- Keylengths
- Modes of operation and padding modes - what to use and why
- Common and not-so-common mode usage errors
- Padding oracle attacks

3. Hashing and Signing

- Hash functions
- HMAC
- Asymmetric signature modes
- Attacks on weak hash functions
- Attacking weak signature modes

4. Password-based key derivation

- Algorithms, parameters, hash functions
- Attacks on weak PBKDFs
- Password-based Encryption

5. Key-Management

- The importance of key management
- Attacks on software keystores
- Alternative key-management techniques

6. Using common protocols

- TLS client and server configuration
- Certificate verification
- Attacks on weak TLS and SSH configurations and how to fix them

---

Day 2 - Crypto Exploits

Audience

- Security/Risk managers
- Application Security auditors
- Pen-testers
- Security Architects

Required background

The course is for professionals working in application security. Some basic familiarity with cryptography is required to get the most out of the training. This part of the training includes practical exercises, so some coding skills are required, and familiarity with crypto APIs will help. The training examples will be given in Java, but developers with good experience of another widely-used high-level language like Python may prefer to use that. Cryptosense trainers will support Java and Python, but can't guarantee support for more exotic languages.

What you will learn

- How to write exploits for vulnerabilities resulting from common crypto errors.

Day 2 Syllabus

1. Warm up

- Attacking a stream cipher using weak IV generation

2. Breaking Encryption

- Attacks on encryption in ECB Mode
- Padding oracle attack on CBC encryption (Vaudenary attack)
- Real-world examples of variations including fixed IV, key as IV

3. Key-management attacks (time permitting)

- Writing a password cracker for a weak proprietary keystore

Detailed Program - Day 1

Cryptography recap (9.00 - 9.30)

Encryption part 1 (9:30 - 10.45)

- Algorithms
- Keylengths
- Modes of operation and padding modes - what to use and why
- Common and not-so-common mode usage errors
- Padding oracle attacks

Coffee Break (10.45 - 11.00)

Hashing and Signing (11.00 - 12.00)

- Hash functions and HMAC
- Asymmetric signature modes
- Attacks on weak hash functions
- Attacking weak signature modes

Lunch Break (12.00 - 13.30)

Password-based cryptography (13:30 - 15.00)

- Password-based Encryption
- Attacks on weak PBKDFs
- Secure password storage

Coffee Break (15.00 - 15.15)

Key-Management (15.15 - 16.30)

- The importance of key management
- Attacks on key generation
- Attacks on weak keystores
- Alternative key-management techniques

Using common protocols (16.30 - 17.30)

- TLS client and server configuration
- Certificate verification
- Attacks on weak TLS and SSH configurations and how to fix them

Detailed Program - Day 2

Warm up (9.00 - 9.30)

Breaking Encryption 1 (9:30 - 10.45)

- Attacks on Encryption in ECB

Coffee Break (10.45 - 11.00)

Breaking Encryption 2 (11.00 - 12.00)

- Vaudenay padding oracle attacks

Lunch Break (12.00 - 13.30)

Breaking Encryption 3 (13:30 - 15.00)

- Vaudenay padding oracle attacks

Coffee Break (15.00 - 15.15)

Key-Management (15.15 - 17.30)

- Password cracking for weak keystores