E-POST

Deutsche Post

Information Security Management - A Hacker's Perspective

Jürgen Pabel

Bochum, 5th of June 2013

Agenda

Information Security Management Systems

A Hacker's Perspective

Focus-Topic #1: Crypto-Toolbox

Focus-Topic #2: Secure Session-Data Storage

Focus-Topic #3: Security Cup

Introduction

Information Security Management Systems

- Purpose
  - Continuous independent organizational control for adequately managing IT-security related risks
- Key aspects
  - Continuous improvement
    - Audits
    - Reviews
  - Artifacts
    - Requirements / Policies
    - Processes / Procedures
    - Reports

Established ISMS Frameworks

- ISO/IEC 27001
  - International standard
  - Process-oriented framework
- BSI IT-Grundschutz
  - German national standard
  - Roughly based on ISO/IEC 27001
  - Technology-specific catalogues

Information Security Management Systems

ISO/IEC 2700x

ISO/IEC 27001: Domains

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

ISO/IEC 2700x: Overview

- ISO/IEC 27002:
  Code of practice for information security management
- ISO/IEC 27003:
  Information security management system implementation guidance
- ISO/IEC 27004:
  Information security management – Measurement
- ISO/IEC 27005:
  Information security risk management
- …

BSI IT-Grundschutz (ISO 27001 according to IT-Grundschutz)

IT-Grundschutz: Artifacts

- Scope definition
- Structure analysis
- Protection requirements
- Modeling
- Baseline security checks
- Risk analysis
- Risk treatment plan

IT-Grundschutz: Standards

- BSI-Standard 100-1:
  Information Security Management Systems
- BSI-Standard 100-2:
  IT-Grundschutz Methodology
- BSI-Standard 100-3:
  Risk Analysis based on IT-Grundschutz
- BSI-Standard 100-4:
  Business Continuity Management

Conceptional and practical issues in real-life

Conceptional issues

- ISO/IEC 27001
  - Gives no technological guidance whatsoever
- IT-Grundschutz is a standard defined by a German federal office
  - Not even formally compliant to ISO/IEC 27001…
  - …and thus not internationally recognized

Practical issues

- Documentation overhead is viewed as cumbersome by most organizations
- IT-Grundschutz catalogues are partially out of date / incomplete
- Classification of protection levels somewhat impractical for most (commercial) environments

Agenda

Deutsche Post

E@POST

Information Security Management Systems

A Hacker's Perspective

Focus-Topic #1: Crypto-Toolbox

Focus-Topic #2: Secure Session-Data Storage

Focus-Topic #3: Security Cup

Complications in most ISMS implementations

Organization

- Independent organizational unit
  - Acceptance / Governance
  - Staffing
  - Budget

Employees

- Usually very process-oriented skill-set…
  - …as required by ISMS idiom
  - …but the technological skill-set of security-management staff is usually very basic

Disclaimer: Personal Oppinion

Systems

- Standard components are often (only) hardened according to vendor standards
- Custom/non-standard components are often not hardened at all

Risk management

- Knowledge of internal staff about risks are often not escalated/prioritized
- External audit results are usually "managed" rather than resolved

Risks in most ISMS implementations

Organization

- Independent organizational unit
  - Acceptance / Governance
  - Staffing
  - Budget

Employees

- Usually very process-oriented skill-set…
  - …as required by ISMS idiom
  - …but the technological skill-set of security-management staff is usually very basic

Disclaimer: Personal Oppinion

Systems

- Standard components are often (only) hardened according to vendor standards
- Custom/non-standard components are often not hardened at all

Risk management

- Knowledge of internal staff about risks are often not escalated/prioritized
- External audit results are usually "managed" rather than resolved

Solutions for most ISMS implementations

Organization

- Unconditional management commitment…
  - …for resolving security issues
  - …for all involved units

Employees

- Hackers in ~~space~~ security management
- Security awareness / trainings
  - Properly handling sensitive information
  - Task-specific security knowledge

Disclaimer: Personal Oppinion

Systems

- Considering security during system planning, development, deployment und operations
- Eye-opening audits

Risk management

- Improvements happen automatically if other aspects are addressed "better"

What else?

Organization

- Don't over-do it
  - Escalate to management only if really necessary

Employees

- Don't over-do it
  - Guide and support instead of criticize and "punish"
- Help by suggesting solutions for non-security related issues

Disclaimer: Personal Oppinion

Systems

- Don't over-do it
  - (Security) Resource management

Risk management

- Don't over-do it

Agenda

Information Security Management Systems

A Hacker's Perspective

Focus-Topic #1: Crypto-Toolbox

Focus-Topic #2: Secure Session-Data Storage

Focus-Topic #3: Security Cup

Focus-Topic #1: Crypto-Toolbox

Visualization of cryptographic basics

Even within IT, most people don't understand basic cryptographic concepts. Thus, a simple to understand analogy helps to build an understanding for cryptographic basics:

- Symmetric encryption
- Asymmetric encryption
- Hashing
- Digital signatures

Focus-Topic #1: Crypto-Toolbox

Crypto-Toolbox explains cryptographic basics

Symmetric encryption

- The key is required for locking and unlocking the lock.

Asymmetric encryption

- Locking the lock is possible without the key; unlocking requires the key.

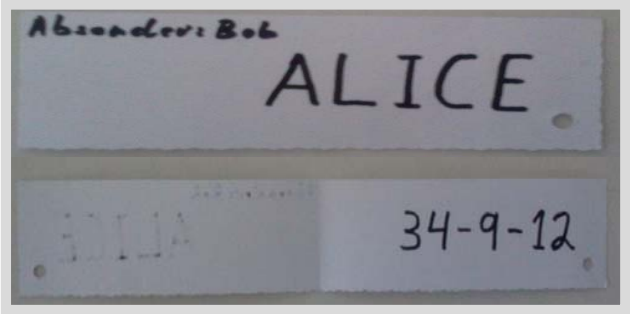
Hashing

- The sum of all numbers represents a hash-algorithm for easy explanations.

Digital signatures

- The specific cutting pattern of crafting-scissors represent digital signatures.

Visualize „encrypting“ and „signing“



Message creation

- Sender and recipients are written on the message envelope.
- Message contents are on the inside of the envelope.

Message encryption

- Envelope is locked using a (randomly selected) symmetric lock.
- The key of the symmetric lock is attached to the recipients asymmetric lock.

Message signing

- The hash of the message is calculated and written on a separate note.
- The note is marked using the sender’s scissor and attached to the message.

Agenda

Deutsche Post

E@POST

Information Security Management Systems

A Hacker's Perspective

Focus-Topic #1: Crypto-Toolbox

Focus-Topic #2: Secure Session-Data Storage

Focus-Topic #3: Security Cup

Focus-Topic #2: Secure Session-Data Storage

Most web-applications handle sensitive data

Commonly employed security measures

- Encrypting the transport channel from web-browser to web-server with HTTPS.
- Encrypting the transport channel from web-server to backend-systems using TLS.
- Encrypting or access-restricting persisted data by application-specific means.

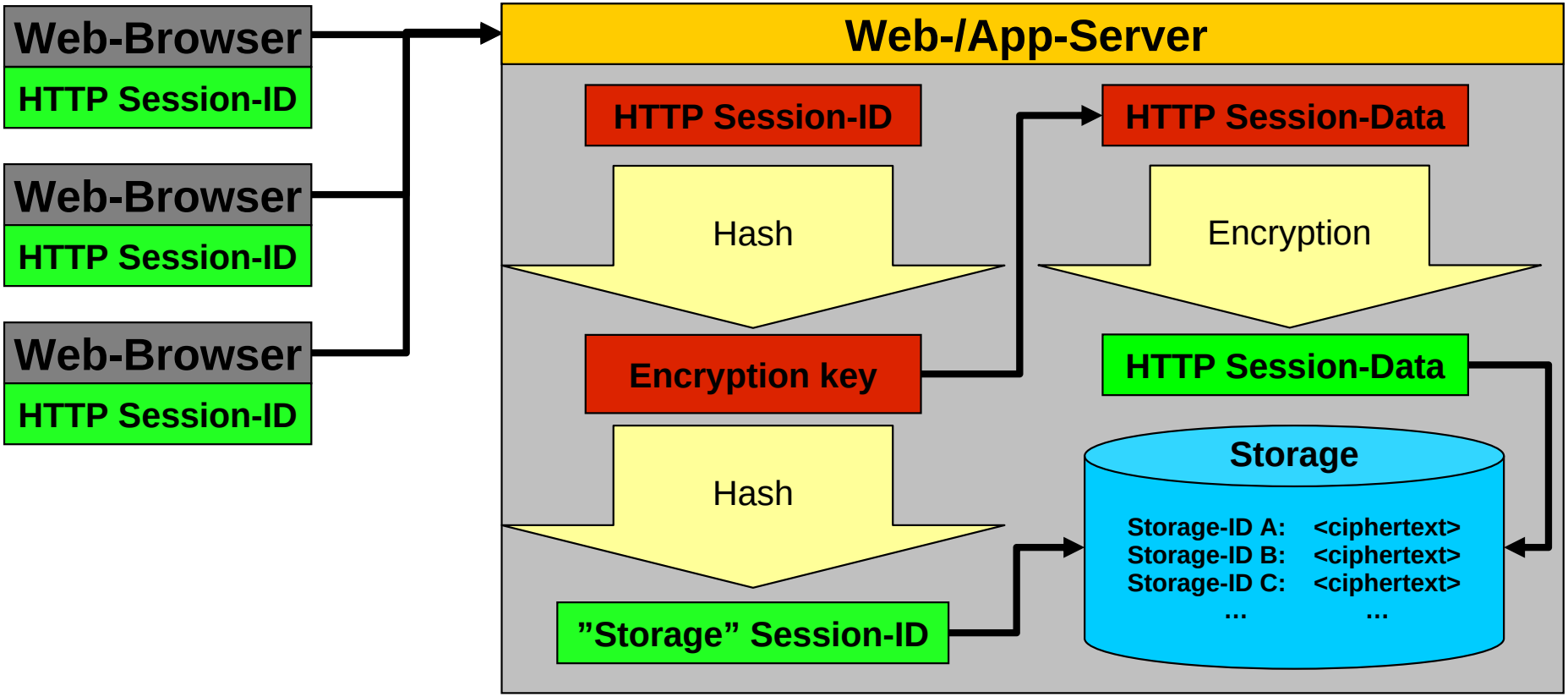
HTTP Session-Data left unprotected

- HTTP Session-Data is usually stored in storage systems (like memcached).
- The HTTP Session-ID is usually the primary key for the stored HTTP Session-Data.
- HTTP Session-ID and Session-Data are usually – due to a lack of generally available solutions – stored unencrypted.

Focus-Topic #2: Secure Session-Data Storage

Secure Session Data-Storage (SSDS) encrypts session-data on the server

- Hashes of the HTTP Session-IDs are stored as the primary keys (instead of Session-IDs themselves).
- HTTP-Session-IDs are used as keys for encrypting HTTP Session-Data



Focus-Topic #2: Secure Session-Data Storage

PHP-SSDS: Cryptographic details

- A non-deterministic initialization-vector is important for most block cipher modes
  - Randomly generating initialization-vectors would probably drain the server's entropy pool.
  - Initialization-vectors are calculated in php-ssds using the original Session-ID and the current time:
    `IV = hash( concat( NOW, HTTP SESSION-ID ) )`

- All employed cryptographic algorithms are configurable
  - `key_hash` Hashing algorithm for deriving the encryption key from the HTTP Session-ID
  - `sid_hash` Hashing algorithm for deriving the Storage-ID form the encryption key
  - `iv_hash` Hashing algorithm for deriving the initialization-vector using Session-ID and time
  - `data_cipher` Encryption cipher for encrypting Session-Data using the calculated encryption-key

Agenda

Information Security Management Systems

A Hacker's Perspective

Focus-Topic #1: Crypto-Toolbox

Focus-Topic #2: Secure Session-Data Storage

Focus-Topic #3: Security Cup

Thank you for your attention!

Q & A

Jürgen Pabel
Information Security Officer E-POST

Moltkestrasse 14
53173 Bonn

Büro: (0228) 182 32123
juergen.pabel@deutschepost.de