

# Script generated by TTT

Title: Pretschner: SecEngSS19 (29.04.2019)

Date: Mon Apr 29 12:22:53 CEST 2019

Duration: 43:33 min

Pages: 6

0:27:22 12:39

## Relevance and Challenges

New security-sensitive applications

- eVoting, car2car communication, internet banking and payment, DRM, ...

Security technologies are **enablers and drivers**

Fight against

- Vulnerabilities, vulnerabilities, vulnerabilities, ...
- Increasing threats and potential damages
- Potential cyber crime, hooliganism, terrorism

National interests and secret services

Privacy issues

Lack of standards; lack of products/solutions

Lack of understanding

Prof. Alexander Pretschner (I4) | Security Engineering | Sommer 2019 12

Nächste Folie

### Relevance: Known incidents/vulnerabilities

We have seen all kinds of attacks and serious vulnerabilities in the wild, increasingly over the years! Think of:

- Heartbleed: late 2014
- Heartbleed 2014: 60% of the internet under threat!
- NBA 2013: E. Snowden revealed espionage on citizens and governments
- Bony 2011: PlayStation network, private data of millions of user stolen
- Stuxnet 2010: Attack to particular critical infrastructure using Stuxnet PLCs
- Political statements constantly made by Anonymous
  - Goal: against commercial banking and governmental sites
- Zeus malware: world-scale cyber-crime operation
- ... Etc.

Keine Notizen.

0:44:11 12:56

## What to do?

**Technically**

- Software and Systems Engineering
- Cryptography
- Physical at macro-level: access to buildings, secured areas (like computer centers), shielding against electromagnetic radiation, etc.
- Physical at micro-level: e.g. tamper-resistant devices, smart-cards
- Biometric technology
- Processor technology
- Language security
- Operating system security

**Organizationally**

- Security policies, classification of information, defining responsibilities, etc.

**People-related**

- Selection, motivation, education, etc.

**Legally**

- Liability regulations, insurances, etc.

Prof. Alexander Pretschner (I4) | Security Engineering | Sommer 2019 17

Nächste Folie

## Humans in the loop

Social Engineering

- Don't hack system, "hack" people

Keine Notizen.

0:49:36 13:01

## ...and system vulnerabilities

**Password Management Flaws**

- Weak passwords
- Passwords easily accessible
- Heavy re-use of passwords

**Fundamental Operating System Design Flaws**

- Default permit policies
- Race conditions

**Software Bugs**

- Security holes as consequence of flawed design or implementation

**Unchecked User Input –**

- Buffer overflow attacks
- SQL injections

Badly set-up and managed IT infrastructures that combine the above

Prof. Alexander Pretschner (I4) | Security Engineering | Sommer 2019 20

Nächste Folie

### OWASP 2017 Top Ten Vulnerabilities

Top 10 2013	Top 10 2017
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting
A4 – Insecure Direct Object References	A4 – Broken Access Control
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control	A7 – Insufficient Attack Protection
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and forwards	A10 – Unprotected APIs

See [https://www.owasp.org/index.php/Top\\_10-2017\\_Top\\_10](https://www.owasp.org/index.php/Top_10-2017_Top_10)

Keine Notizen.

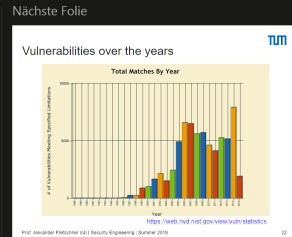
0:51:01 13:03

## OWASP 2017 Top Ten Vulnerabilities

Top 10 2013	Top 10 2017
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting
A4 – Insecure Direct Object References	A4 – Broken Access Control
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control	A7 – Insufficient Attack Protection
A8 – Cross-site Request Forgery (CSRF)	A8 – Cross-site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	A10 – Unprotected APIs

See [https://www.owasp.org/index.php/Top\\_10-2017\\_Top\\_10](https://www.owasp.org/index.php/Top_10-2017_Top_10)

Folie 21 von 58



Keine Notizen.

0:52:05 13:04

## Vulnerabilities over the years

<https://web.nvd.nist.gov/view/vuln/statistics>

Prof. Alexander Pretschner (14) | Security Engineering | Summer 2019

Folie 22 von 58

Nächste Folie

### Security Engineering

Security Engineering = Software Engineering + Information Security

Software Engineering is the application of systematic, quantifiable approaches to the development, operation, and maintenance of software; i.e., the application of engineering to software.

Information Security focuses on methods and technologies to reduce risks to Information Assets.

More refined (adopted from Anderson, Security Engineering)

- Security Engineering is about building systems that remain dependable in the face of malice, error, or mischance. As a discipline, it focuses on the tools, processes, and methods needed to design, implement, test, and evolve systems.

Security Engineering is not a mature discipline yet!

Prof. Alexander Pretschner (41) | Security Engineering | Summer 2019

Keine Notizen.

0:52:08 13:04

## Security Engineering

Security Engineering = Software Engineering + Information Security

Software Engineering is the application of systematic, quantifiable approaches to the development, operation, and maintenance of software; i.e., the application of engineering to software.

Information Security focuses on methods and technologies to reduce risks to Information Assets.

More refined (adopted from Anderson, Security Engineering)

- Security Engineering is about building systems that remain dependable in the face of malice, error, or mischance. As a discipline, it focuses on the tools, processes, and methods needed to design, implement, test, and evolve systems.

Security Engineering is not a mature discipline yet!

Prof. Alexander Pretschner (14) | Security Engineering | Summer 2019

Folie 23 von 58

Nächste Folie

### Security Engineering and Complexity

No need to illustrate ...

Prof. Alexander Pretschner (41) | Security Engineering | Summer 2019

Keine Notizen.