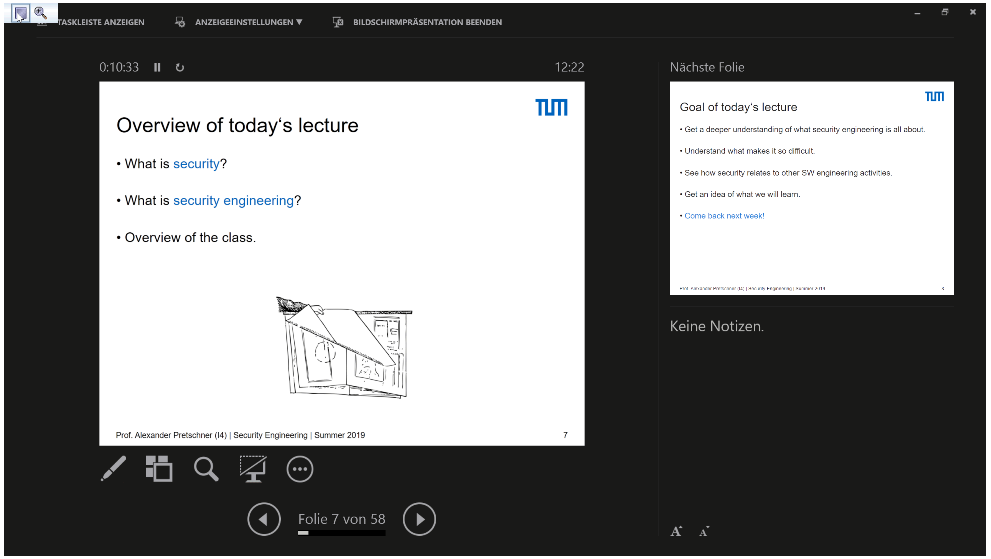
Script generated by TTT

Title: Pretschner: SecEngSS19 (29.04.2019)

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

Duration: 43:33 min

Pages: 6



Overview of today's lecture

- What is security?
- What is security engineering?
- Overview of the class.

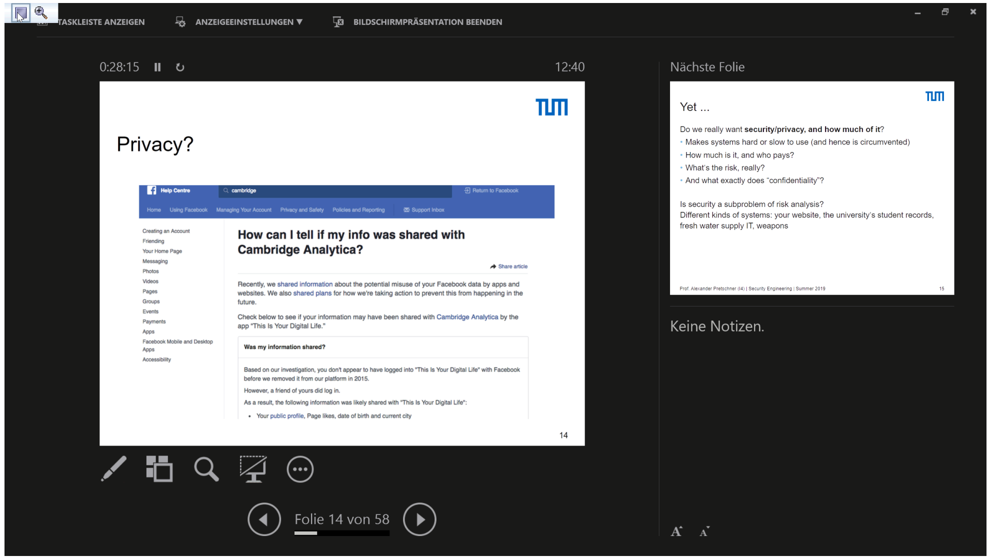
Prof. Alexander Pretschner (I4) | Security Engineering | Summer 2019 7

Goal of today's lecture

- Get a deeper understanding of what security engineering is all about.
- Understand what makes it so difficult.
- See how security relates to other SW engineering activities.
- Get an idea of what we will learn.
- Come back next week!

Prof. Alexander Pretschner (I4) | Security Engineering | Summer 2019 8

Keine Notizen.



Privacy?

How can I tell if my info was shared with Cambridge Analytica?

Recently, we shared information about the potential misuse of your Facebook data by apps and websites. We also shared plans for how we're taking action to prevent this from happening in the future.

Check below to see if your information may have been shared with Cambridge Analytica by the app "This Is Your Digital Life."

Was my information shared?

Based on our investigation, you don't appear to have logged into "This Is Your Digital Life" with Facebook before we removed it from our platform in 2015.

However, a friend of yours did log in.

As a result, the following information was likely shared with "This Is Your Digital Life":

- Your public profile, Page likes, date of birth and current city

14

Yet ...

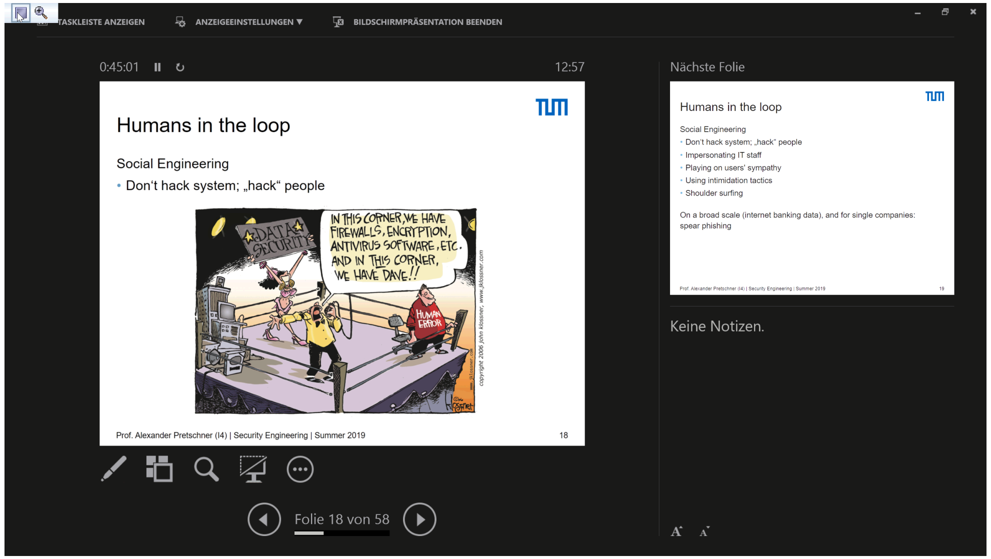
Do we really want **security/privacy, and how much of it**?

- Makes systems hard or slow to use (and hence is circumvented)
- How much is it, and who pays?
- What's the risk, really?
- And what exactly does "confidentiality"?

Is security a subproblem of risk analysis?
Different kinds of systems: your website, the university's student records, fresh water supply IT, weapons

Prof. Alexander Pretschner (I4) | Security Engineering | Summer 2019 15

Keine Notizen.


TASKLEISTE ANZEIGEN
ANZEIGEEINSTELLUNGEN ▾
BILDSCHIRMPRÄSENTATION BEENDEN
0:45:01
12:57
Folie 18 von 58
Nächste Folie
DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
copyright 2006 john klossner, www.jklossner.com

Humans in the loop

Social Engineering

- Don't hack system; „hack" people

Prof. Alexander Pretschner (I4) | Security Engineering | Summer 2019 18

Humans in the loop

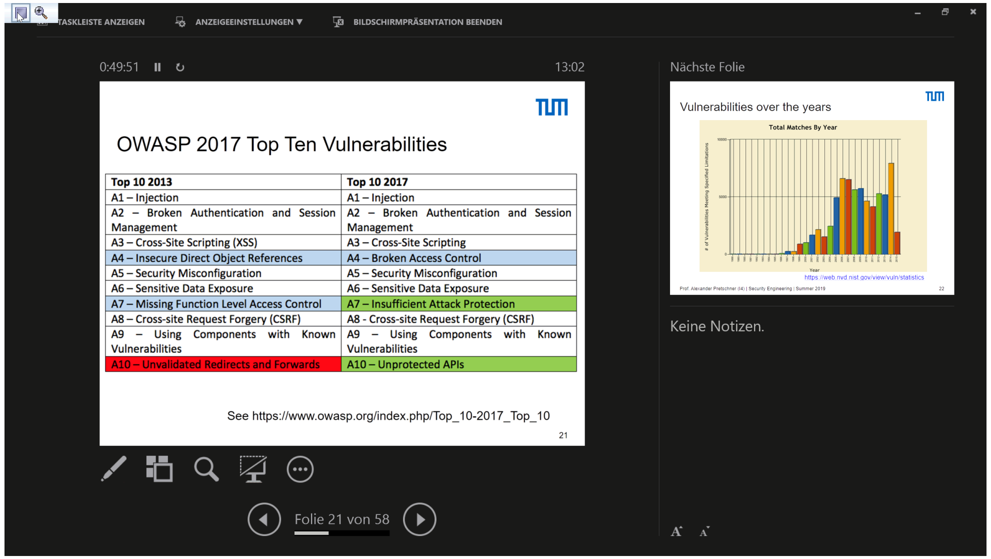
Social Engineering

- Don't hack system; „hack" people
- Impersonating IT staff
- Playing on users' sympathy
- Using intimidation tactics
- Shoulder surfing

On a broad scale (internet banking data), and for single companies: spear phishing

Prof. Alexander Pretschner (I4) | Security Engineering | Summer 2019 19

Keine Notizen.



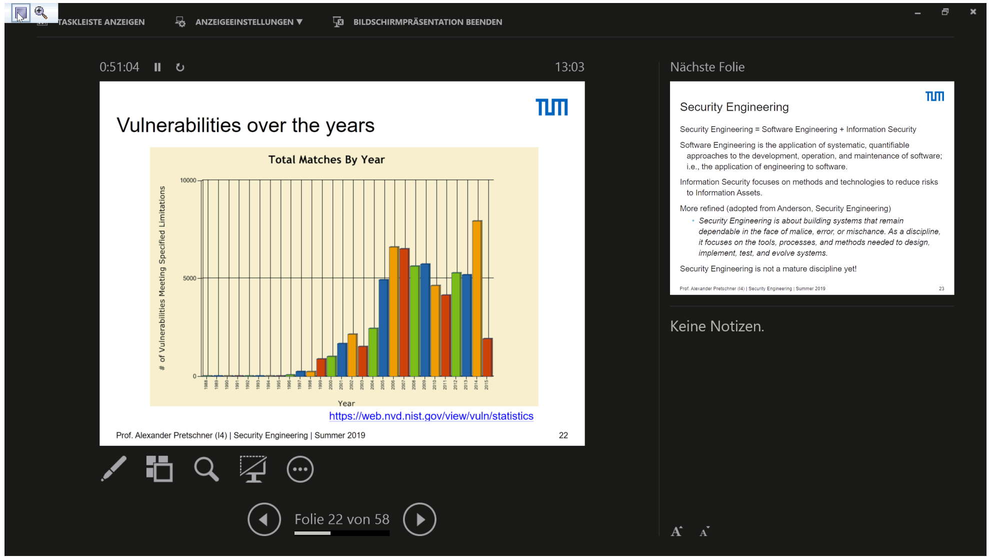
OWASP 2017 Top Ten Vulnerabilities

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

Vulnerabilities over the years

Keine Notizen.



Vulnerabilities over the years

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

Security Engineering

Security Engineering = Software Engineering + Information Security

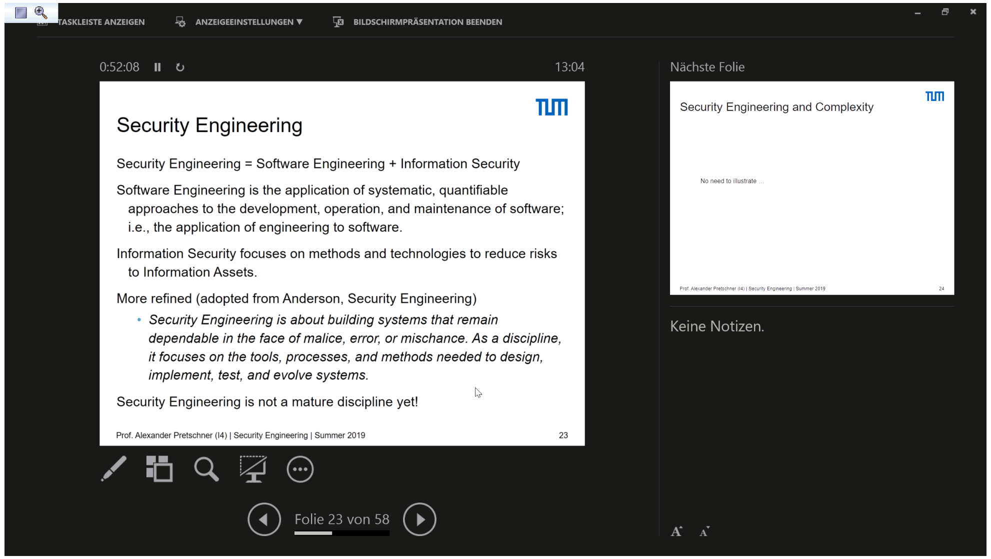
Software Engineering is the application of systematic, quantifiable approaches to the development, operation, and maintenance of software; i.e., the application of engineering to software.

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

More refined (adopted from Anderson, Security Engineering)

Security Engineering is not a mature discipline yet!

Keine Notizen.



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!

Security Engineering and Complexity

No need to illustrate …

Keine Notizen.