COMx501: Computer Security and Forensics

Achim D. Brucker

a.brucker@sheffield.ac.uk https://www.brucker.ch/

Software Assurance & Security Research

Department of Computer Science, The University of Sheffield, Sheffield, UK

https://logicalhacking.com/

February 8, 2018

COMx501: Computer Security and Forensics

Part 1: Introduction & Motivation

Achim D. Brucker

a.brucker@sheffield.ac.uk https://www.brucker.ch/

Software Assurance & Security Research

Department of Computer Science, The University of Sheffield, Sheffield, UK

https://logicalhacking.com/

February 6, 2018

Outline

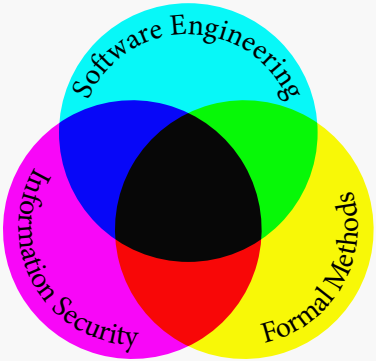
Personal Background

- PhD from ETH Zurich, Switzerland
- Eight years of enterprise secure software development:
  - Member of the central security team, SAP SE (Germany)
    - Working on all software security aspects
    - (Global) Security Testing Strategist
    - Security Research Expert/Architect
  - Work areas:
    - Defining the risk-based Security Testing Strategy of SAP
    - Introducing security testing tools (e.g., SAST, DAST) at SAP
    - Identify white spots and evaluate and improve tools/methods
    - Secure Software Development Life Cycle integration
    - Applied security research
    - …
- Since 12/2015:
  - Senior Lecturer, The University of Sheffield, UK
  - Head of the Software Assurance & Security Research Team
  - Available as consultant & (research) collaborations

https://www.brucker.uk/

- Research interests:
  - security engineering (at daytime)
  - verification and testing (formal methods)
  - software (and hardware) engineering
- Other areas I am interested in:
  - attacking systems (at night)
  - process and economical aspects building (secure) systems
  - social and political aspects of security and surveillance
  - research transfer & commercialisation (yes, still …)
- My agenda:
  Methods, tools, and processes for ensuring the
  - security,
  - safety, reliability, and correctness

  of software (and hardware) systems



SAP SE

- Leader in Business Software
  - Cloud
  - Mobile
  - On premise
- Many different technologies and platforms, e.g.,
  - In-memory database and application server (Hana)
  - Netweaver for ABAP and Java
- More than 25 industries
- 63% of the world's transaction revenue touches an SAP system
- over 68 000 employees worldwide over 25 000 software developers
- Headquarters: Walldorf (Heidelberg), Germany

What do you expect from this module?

- Discuss with your neighbour
  - what motivates you to take a security module?
  - what do you expect to learn in this module?
  - what security experience do you have?

Outline

Example (LinkedIn, May 2016)

- 164 million email addresses and passwords
- from an attack in 2012, offered for sale May 2016
- Compromised data:
  - email addresses
  - passwords

Example (TalkTalk, October 2015)

TalkTalk

- nearly 157,000 customer records leaked
- nearly 16,000 records included bank details
- more than 150,000 customers lost
  (home services market share fall by 4.4 percent
  in terms of new customers)
- Costs for TalkTalk: around £60 million

Example (Ashley Madison, July 2015)

- more than 30 million email addresses and much more

Costs of Data Breaches

> A hack not only costs a company money, but also its **reputation** and the **trust** of its customers. It can take years and millions of dollars to repair the damage that a single computer hack inflicts.
>
> (http://financialedge.investopedia.com/financial-edge/0711/Most-Costly-Computer-Hacks-Of-All-Time.aspx)

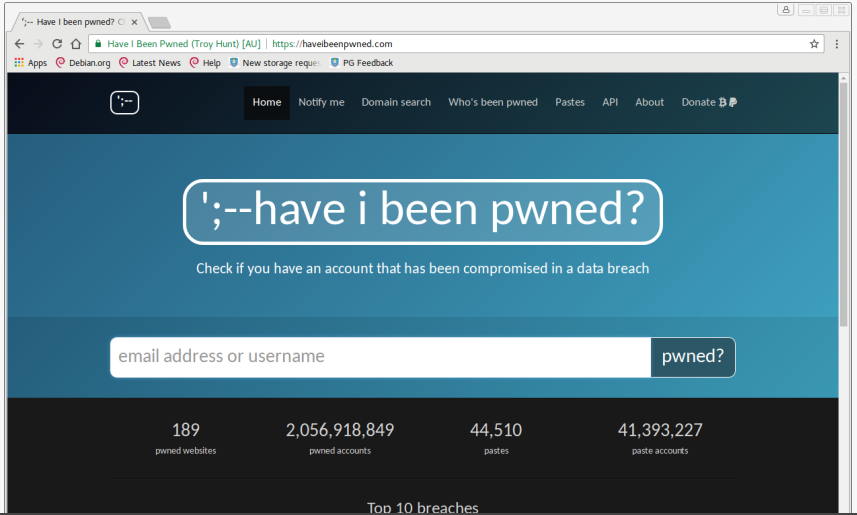
TJX Company, Inc. (2007)	$ 250 million
Sony (2011)	$ 170 million
TalkTalk (2015)	ca. $ 75 million
Heartland Payment Systems (2009)	$ 41 million

Note:

- Publicly known incidents are usually "Business-to-Customer (B2C)"
- Business-to-Business (B2B) incidents are often not publicly known

Have I been Pwned?

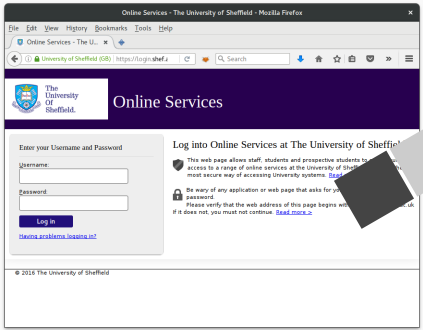
https://haveibeenpwned.com/



What's the Problem?

Authenticate without a password using "SQL Injection"

- Implementation (simplified):




```
SELECT * FROM ‘users‘ WHERE
‘name‘ = ’test’ AND ‘pwd‘ = ’secret’;
```

Root cause: a bug.

Let's use "' OR '1'='1" as password:

```
SELECT * FROM ‘users‘ WHERE
‘name‘ = ’test’ AND ‘pwd‘ = ’’ OR ’1’=’1’‘name‘ = ’test’ AND ‘
```

- No password check!

How Can We Build Secure Systems?

We will answer this in this module (not today ...)

In this lecture you will

- develop a general understanding of information/computer security
- learn various security technologies
- learn the nature of security vulnerabilities
- learn how to develop secure systems (defensive)
- learn how to test the security of systems (offensive)
- learn the challenges managing and discussing security issues

The Lecture Roughly Follows the Secure Software Lifecycle

- Foundations and Security Technologies
  - Access Control
  - Cryptography
  - Security Protocols
- Building Secure Systems
  - Analyzing Security Protocols
  - Application Security & Secure Programming
  - Security Testing
- Secure Operations, Response, and Forensics
  - Secure Operations
  - Security Response
  - Forensics

Thank you for your attention!
Any questions or remarks?

Contact:

Dr. Achim D. Brucker
Department of Computer Science
University of Sheffield
Regent Court
211 Portobello St.
Sheffield S1 4DP, UK

a.brucker@sheffield.ac.uk
@adbrucker
https://de.linkedin.com/in/adbrucker/
https://www.brucker.ch/
https://logicalhacking.com/blog/

Bibliography I

Ross J. Anderson.

Security Engineering: A Guide to Building Dependable Distributed Systems.
John Wiley & Sons, Inc., New York, NY, USA, 1st edition, 2001.
The complete book is available at: http://www.cl.cam.ac.uk/~rja14/book.html.

Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot.

Handbook of Applied Cryptography.
CRC Press, Inc., Boca Raton, FL, USA, 5th edition, 2001.
The complete book is available at: http://cacr.uwaterloo.ca/hac/.

Document Classification and License Information