Hochschule Konstanz
Fakultät Informatik

Introduction to IT Security

WIN+AIN

Hanno Langweg

01a Goals and Principles - What Is Security

What is security?

- **Bad events** caused with **malicious intent**
  - Security vs. reliability
- Terminology:
  - **Threat** = bad event that might happen
  - **Attack** = someone intentionally causes the bad thing to happen
  - **Vulnerability** = weakness in an information system that enables an attack
  - **Exploit** = implementation of an attack
  - **Risk** = probability of an attack × damage
- Security is a non-functional property

Erstes Smart Meter Gateway zertifiziert

Meilenstein der Energiewende erreicht

Ort Bonn
Datum 20.12.2018

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat das erste Zertifikat auf Basis des Schutzprofils für das Smart Meter Gateway erteilt, das von der Power Plus Communications AG (PPC) gemeinsam mit der OpenLimit SignCubes AG entwickelt wurde. Das Zertifikat wurde heute im Bundesministerium für Wirtschaft und Energie an das Unternehmen übergeben. Im Zertifizierungsverfahren wurden neben dem Nachweis der Einhaltung der Sicherheitsvorgaben im Smart Meter Gateway auch die Herstellungs- und Entwicklungsprozesse des Herstellers sowie die Auslieferungswege der Geräte betrachtet und durch das BSI abschließend zertifiziert. Mit der Zertifizierung des Smart Meter Gateways ist gleichzeitig auch das erste IT-Sicherheitskennzeichen vergeben worden.

https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Erstes_Smart_Meter_Gateway_zertifiziert_201218.html

Telematikinfrastruktur – das sichere Netz für alle

gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Der Begriff "Telematik" ist eine Kombination der Wörter "Telekommunikation" und "Informatik". Als Telematik wird die **Vernetzung verschiedener IT-Systeme** und die Möglichkeit bezeichnet, Informationen aus unterschiedlichen Quellen miteinander zu verknüpfen.

Grafik: TI als Datenautobahn

Die Telematikinfrastruktur (TI) vernetzt **alle Akteure des Gesundheitswesens** im Bereich der Gesetzlichen Krankenversicherung und gewährleistet den sektoren- und systemübergreifenden sowie **sicheren Austausch von Informationen**. Sie ist ein geschlossenes Netz, zu dem nur registrierte Nutzer (Personen oder Institutionen) mit einem elektronischen Heilberufs- und Praxisausweis Zugang erhalten.

Um allen Datenschutzanforderungen gerecht zu werden und insbesondere die medizinischen Daten von Patienten zu schützen, wird in der Telematikinfrastruktur auf starke **Informationssicherheitsmechanismen** gesetzt. Die sichere, verschlüsselte Kommunikation zwischen bekannten Kommunikationspartnern sowie der Schutz vor dem Zugriff auf sensible Informationen sind daher das Fundament der Telematikinfrastruktur.

https://www.gematik.de/telematikinfrastruktur/

Critical infrastructures

- Entities/organisations that are important for essential services delivered to the public
- Loss or deterioration of service would have a significant impact on public safety

- Sectors: **Energy, IT, Telecommunication, Water, Food, Finance, Health, Transport**

Wenn IT-Einbrecher lebenswichtige Medizingeräte entern

Der Pharmakonzern Johnson & Johnson meldet eine Sicherheitslücke in vernetzten Insulinpumpen. Der Fall ist besonders spektakulär.

05.10.2016, von JONAS JANSEN

müssen. In dem Schreiben, das an Ärzte und etwa 114000 Patienten in Nordamerika rausging, musste J&J einräumen, dass es eine Sicherheitslücke in einer Insulinpumpe gibt und Hacker theoretisch das Gerät fernsteuern könnten. Das kann für Diabetiker lebensgefährlich sein, wenn die Insulinzufuhr manipuliert wird, also etwa mehr Insulin durch die tragbare Pumpe ausgeschüttet wird, die über einen Katheter mit dem Körper verbunden ist.

http://www.faz.net/aktuell/wirtschaft/insulin-wenn-it-einbrecher-lebenswichtige-medizingeraete-entern-14467704.html

Cyber-physical systems (e.g. embedded, control of industrial processes)

- Increased complexity
  - More powerful hardware, more features
  - More developers, suppliers, components
- Non-networked ➔ networked
  - Change of environment invalidates assumptions during development/deployment
  - Increased attack surface
- Integration
  - Data flow: devices ➔ monitoring
  - Data flow: remote control ➔ devices
  - Data flow: end-users ➔ devices ➔ end-users

19.03.2019

Warning:

Cyber Attack Against the Hydro Network.

Please do not connect any devices to the Hydro network. Do not turn on any devices connected to the Hydro Network.

Please disconnect any device (Phone/Tablet etc.) from the Hydro Network.

Await new update.

-Security

OBS

HYDRO ER UNDER CYBER-ANGREP.

IKKE KOBLE PC TIL NETTVERK INNTIL NY BESKJED

ORS

Huge aluminium plants hit by 'severe' ransomware attack

19 March 2019 Share

Hydro employs more than 35,000 people

One of the world's biggest aluminium producers has switched to manual operations at some smelting plants following a "severe" ransomware attack.

https://www.nrk.no/norge/skreddersydd-dobbeltangrep-mot-hydro-1.14480202
https://www.bbc.com/news/technology-47624207

Proactive vs. reactive security

- **Technical prevention:** design systems to prevent, discourage and mitigate attacks
  - If attack cannot be prevented, increase its cost and control damage
- **Detection and reaction:** detect attacks and take measures to stop them, or to punish the guilty
- In open networks, attacks happen all the time
  - We can detect port scans, spam, phishing etc., yet can do little to stop it or to punish attackers
    → **Technical prevention and mitigation must be the primary defence**
- However, **detection is needed to monitor effectiveness of technical prevention**

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

As the two hackers remotely toyed with the air-conditioning, radio, and windshield wipers, I mentally congratulated myself on my courage under pressure. That's when they cut the transmission.

Immediately my accelerator stopped working. As I frantically pressed the pedal and watched the RPMs climb, the Jeep lost half its speed, then slowed to a crawl. This occurred just as I reached a long overpass, with no shoulder to offer an escape. The experiment had ceased to be fun.

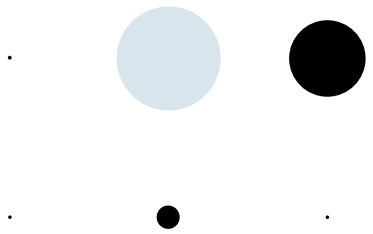
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Security is a continuous process

- **Continuous race** between attackers and defenders
  - Attackers are **creative**
- No security mechanisms will stop all attacks; attackers just move to new methods and targets
  - Some types of attacks can be eliminated but others will take their place
  - Compare with crime statistics: Do locks or prisons reduce crime in the long term?
- Security **mechanisms will fail** and new threats will arise
  - → Monitoring and auditing for new attacks
  - → Contingency planning: how to recover from a breach

Security is not safety

- Intelligent adversaries!
- Adversarial behaviour hard to predict
- Hard to model
- Hard to measure



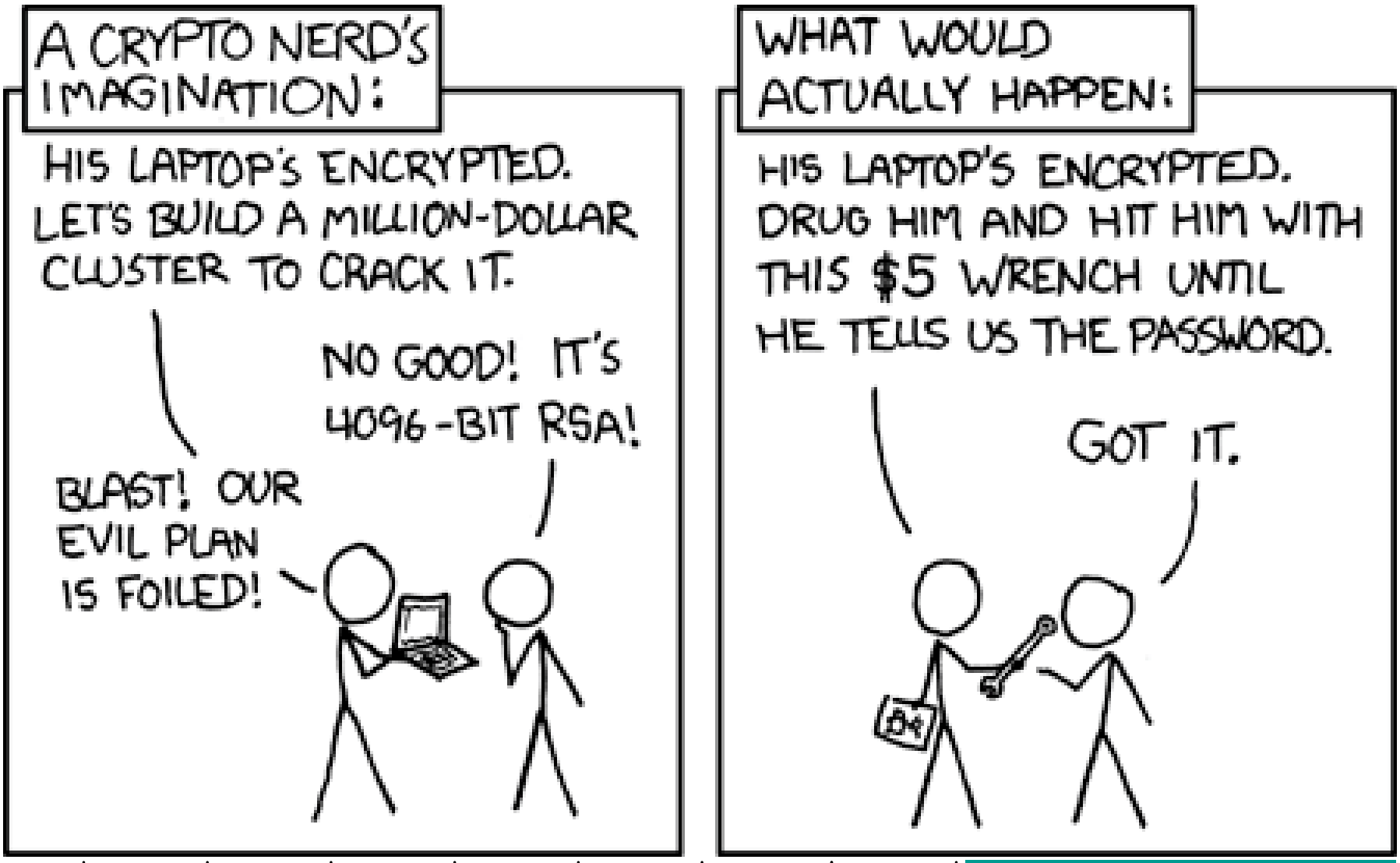
Traditional security goals

- CIA = **c**onfidentiality, **i**ntegrity, **a**vailability
  - **Confidentiality** — protection of secrets
  - **Integrity** — only authorized modification of data and system configuration
  - **Availability** — no denial of service, business continuity
- CIA model good starting point but not all:
  - Privacy — control of personal data and space
  - Accountability/non-repudiation — ability to prove that actions happened
  - Hexad (Parker): CIA + control, authenticity, utility
  - What else?

Cost vs. benefit

- **Rational attackers** compare cost of attack with gains
  - Attackers look for **weakest link**; thus, little is gained by strengthening already strong bits
- **Rational defenders** compare the risk of an attack with the cost of implementing defenses
  - Lampson: “Perfect security is the enemy of good security”
- But human behaviour is not always rational:
  - Attackers follow each other and flock all to same path
  - Defenders buy a peace of mind; **avoid personal liability** by doing what everyone else does

  → Many things are explained better by **group behaviour** than rational choice



https://www.xkcd.com/538/

Security is an inherently economic problem

- There is no absolute security
  - Relative to adversary's abilities and resources
- Nothing useful can be said about the security of a mechanism except in the context of a specific application and environment.
- Never spend more mitigating a risk than tolerating it will cost you.
- *"There are management solutions to technical problems, but no technical solutions to management problems."* (Robert Courtney, IBM)

Huawei could be banned from 5G in Germany

- The German government is considering banning Huawei from providing 5G equipment in the country saying security concerns are of "high relevance."
- The decision to ban Huawei 5G equipment would mark a shift from Germany, which has not been as vocal as other Western countries about security concerns.
- Huawei says 5G security concerns are unfounded.

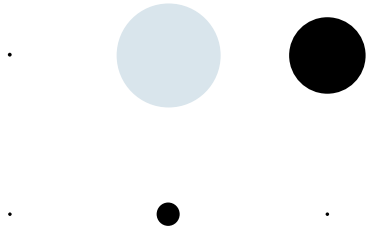
Elizabeth Schulze | Chloe Taylor

Published 4:13 AM ET Fri, 18 Jan 2019 | Updated 10:58 AM ET Fri, 18 Jan 2019

CNBC

How to achieve security

- Ethics
- Laws
- Rules, organisation, management
- Technical controls



Summary

- Goals of IT Security
  - Confidentiality, integrity, availability ("CIA")
  - Privacy, authenticity, accountability, control, utility, ...
- Security relative to adversary
- Security vs. safety