Introduction to IT Security

Univ.-Prof. Dr. **René Mayrhofer**
Institute of Networks and Security

https://twitter.com/rene_mobile

WS 2022/23

What is IT security?

A system is considered secure when the cost of successfully attacking it is higher than the potential gain.

Remember that there is no perfect security.

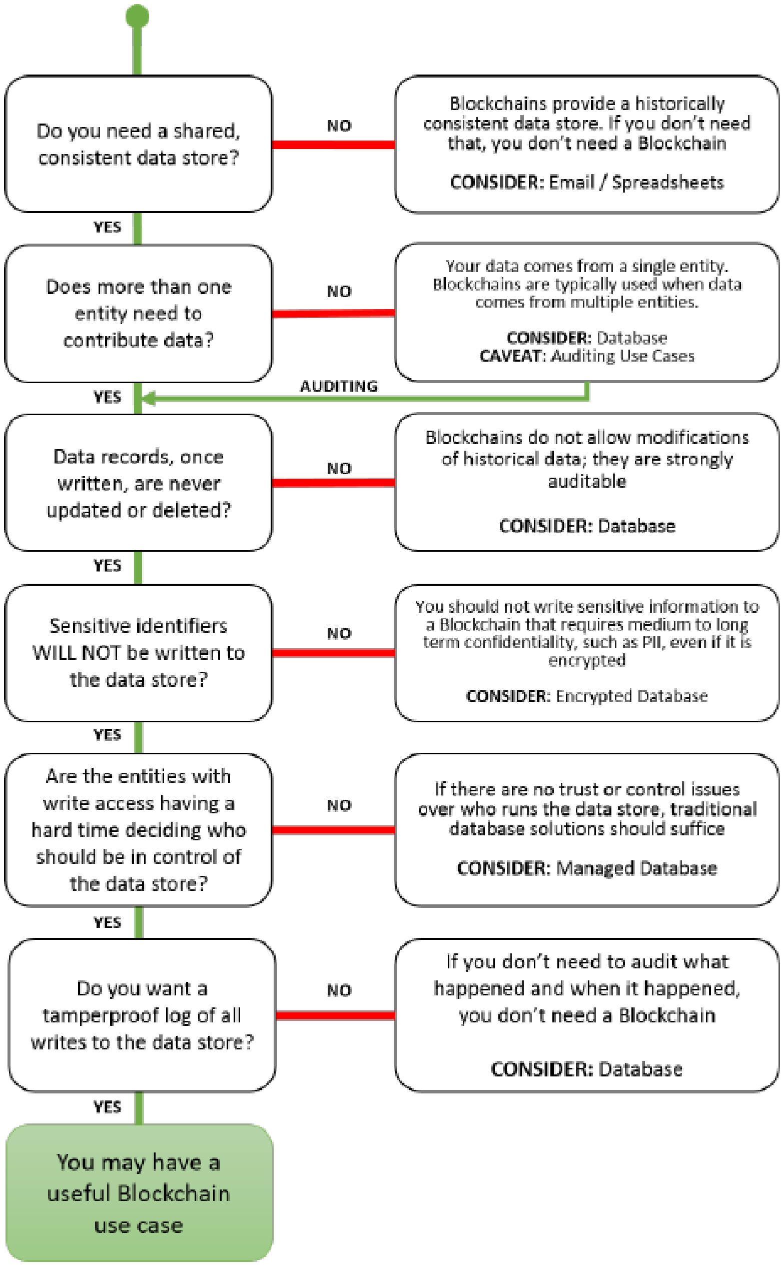
There is no silver bullet

- Blockchain will not solve all security problems
- AI will not solve all security problems
- Quantum computers will not solve (or cause) all security problems
- New-buzzword-of-the-year will not solve all security problems

- (and neither will Zero Knowledge Proofs, a new programming language, a new processor design, tristate logic, etc.)

Interesting security issues often arise at the interface between different layers

See lesson 4/5



Do you need a shared, consistent data store?

NO

Blockchains provide a historically consistent data store. If you don't need that, you don't need a Blockchain

CONSIDER: Email / Spreadsheets

YES

Does more than one entity need to contribute data?

NO

Your data comes from a single entity. Blockchains are typically used when data comes from multiple entities.

CONSIDER: Database
CAVEAT: Auditing Use Cases

AUDITING

YES

Data records, once written, are never updated or deleted?

NO

Blockchains do not allow modifications of historical data; they are strongly auditable

CONSIDER: Database

YES

Sensitive identifiers WILL NOT be written to the data store?

NO

You should not write sensitive information to a Blockchain that requires medium to long term confidentiality, such as PII, even if it is encrypted

CONSIDER: Encrypted Database

YES

Are the entities with write access having a hard time deciding who should be in control of the data store?

NO

If there are no trust or control issues over who runs the data store, traditional database solutions should suffice

CONSIDER: Managed Database

YES

Do you want a tamperproof log of all writes to the data store?

NO

If you don't need to audit what happened and when it happened, you don't need a Blockchain

CONSIDER: Database

YES

You may have a useful Blockchain use case

Figure 6 - DHS Science & Technology Directorate Flowchart

Why IT security?

Increasingly large dependency on IT systems for daily life

- 2004-05-04: **Sasser** worm hits UK coast guard, taking down all 19 coastguard control centers (also hit a few banking networks, temporarily disabling bank branches and ATMs)
- 2010-06: **Stuxnet** targets Siemens **SCADA** systems, physically ruining (reported estimate) 1/5 of Iran’s nuclear centrifuges (very advanced, targetted attack including digital signature of device drivers with stolen private keys)
- Austrian power grid and gas distribution networks also rely on SCADA…
- 2008-2010: Study by “Büro für Technologiefolgen-Abschätzung beim Deutschen Bundestag” (TAB): **only a few days of power outage are life-threatening**
- 2011-09-03: **DigiNotar** CA was found to have been exploited to create 531 signed certificates for well-known domains (e.g. Google, Yahoo, Mozilla, WordPress, Tor, etc.)
- 2012-06: **Operation High Roller** uses advanced attacks on mobile banking clients to attempt fraudulent transactions of up to 60 Mio. €
- 1998 – today: NSA **Tailored Access Operations (TAO)** offers huge library of exploits/attacks (including 0day) for currently used hard- and software (e.g. used against Tor users to attack their Firefox browsers)
- 2017: **WannaCry** taking down systems, e.g. UK NHS, Deutsche Bahn, FedEx, etc.

Why IT security?

Increasingly large dependency on IT systems for daily life

- 2019-03: **Scytl e-voting** system shown to have insecure cryptographic proofs (used by Swiss Post and **New South Wales** for elections)
- 2019-05: City of Baltimore infected by ransomware, **permanently loses access to some data**
- 2019-07: 25 Million Android phones infected with malware “**Agent Smith**” from third party app stores
- some years before to 2019-08: **Apple iPhones subject to waterhole attack** with multiple chains of exploits (https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html)
- 2020-01: **Teamviewer** (at least v7-v14) discovered to have stored passwords AES encrypted with global, static key: https://whynotsecurity.com/blog/teamviewer/
- 2020-01: **“Shitrix” bug in Citrix VPN gateway** used to install backdoors (https://threatpost.com/unpatched-citrix-flaw-exploits/151748/) and directly caused e.g. death of one person due to ransomware attack on Uniklinik Düsseldorf in 2020-09 (https://fm4.orf.at/stories/3007276/)
- 2020-12: Attack on **SolarWinds**, used by large organizations with high privileges, leads to more discussion of “supply chain attacks” (external dependencies): https://text.npr.org/985439655

Why IT security?

Increasingly large dependency on IT systems for daily life

- 2021-01: (yet another) **Microsoft Exchange** breach leading to installed backdoors and ransomware “including servers belonging to around 30,000 organizations in the United States, 7,000 servers in the United Kingdom, as well as the European Banking Authority, the Norwegian Parliament, and Chile's Commission for the Financial Market (CMFt)” (https://en.wikipedia.org/wiki/2021_Microsoft_Exchange_Server_data_breach)
- 2021-02 to -09: NSO group **Pegasus spyware** used zero-day zero-click iMessage malware **FORCEDENTRY** used to attack Saudi activists
- 2021-05: US “**Colonial Pipeline**” attacked with targeted ransomware (https://www.theregister.com/2021/05/10/colonial_pipeline_ransomware/) shutting down billing (which led to shutting down the pipeline itself) → triggered new discussion on security regulation that attacks on hospitals did not... (https://www.securityweek.com/hack-prompts-new-security-regulations-us-pipelines)
- 2021-09-15: Web hoster **Epik** (also used by far-right extremist groups, which was the likely reason for the attack) had most of the data, including accounts (passwords hashed with MD5 in logs…) leaked by Anonymous (https://ddosecrets.com), impacting uninvolved bystanders

Aspects of IT security

IT security is not restricted to a single component

- **Computer security**
  - □ OS security (including e.g. compartmentalization)
  - □ Application security (including e.g. web apps)
  - □ Secure code
- **Network security** (communications)
- **Organizational security** (processes, workflows)
  - □ important part: **Storage security** (backups, memory sticks/DVDs)
- **Never forget: end users** are part of the system
  - □ If they don’t understand how to correctly use it, it will probably be insecure.
  - □ If it’s too complicated, they will find a way around.

(IT) Security is hard to achieve

- Holistic system view is necessary to bridge all these aspects
- However, organizations are often not (yet) good at that
  - from pure IT point of view, only technical aspects can be controlled
  - legal, organizational, and human aspects need broad commitment by the whole organization (or country, society, …)
  - security costs something, but doesn't immediately offer visible gains
  - often left "for future improvement" under (constant) time pressure
  - you can't do it alone, but need strong collaboration with stakeholders from other domains – central administration departments and end-users need to be on board for introducing any measure

→ Sometimes, the most important step is to ask whether building a product or new feature is worth the additional security risk.
Not all things that can be built, should be built.

Course information

- Weekly physical lectures (unless posted otherwise)
- Written exam at the end of term (potentially Moodle with physical attendance, or online-only depending on situation)
- Slides will be available in **Moodle**
  - □ look through the slides yourself, **not all of them will be discussed in detail** → ask questions for anything unclear
  - □ in addition to slides, we may discuss recent computer security events during the lecture
  - □ can also hold **as a flipped classroom** – let's discuss this right now
- This course is focused on technical aspects, there are separate lectures for organizational/administrative aspects
- **Definitions** are indicated by color and describe well-defined and well-known terms, algorithms, protocols, or methods in computer security. **You will need to remember all such definitions.**

Tentative schedule

01 – Introduction, key concepts, and terminology

02 – Threats and security processes
(more detail in special lecture “Information Security Management”)

03-05 – Cryptography basics + usage of applied cryptography
(more detail in special lecture “Cryptography” by Josef Scharinger)

06 – User authentication and key management
(more detail in special lecture “Biometrische Identifikation” by Josef Scharinger)

07-08 – Secure channels / communication security
(see TLS details in special lecture “Cryptography”)

09 – Network security
(more detail in lectures “Network Security”)

10 – Operating system security
(some more detail in lectures “Betriebssysteme” and “Systems Security”,
additional lectures “Special Topics: Android Security” and “Special Topics: Advanced Operating Systems”)

11 – Code security
(more detail in special lecture “Secure Code”)

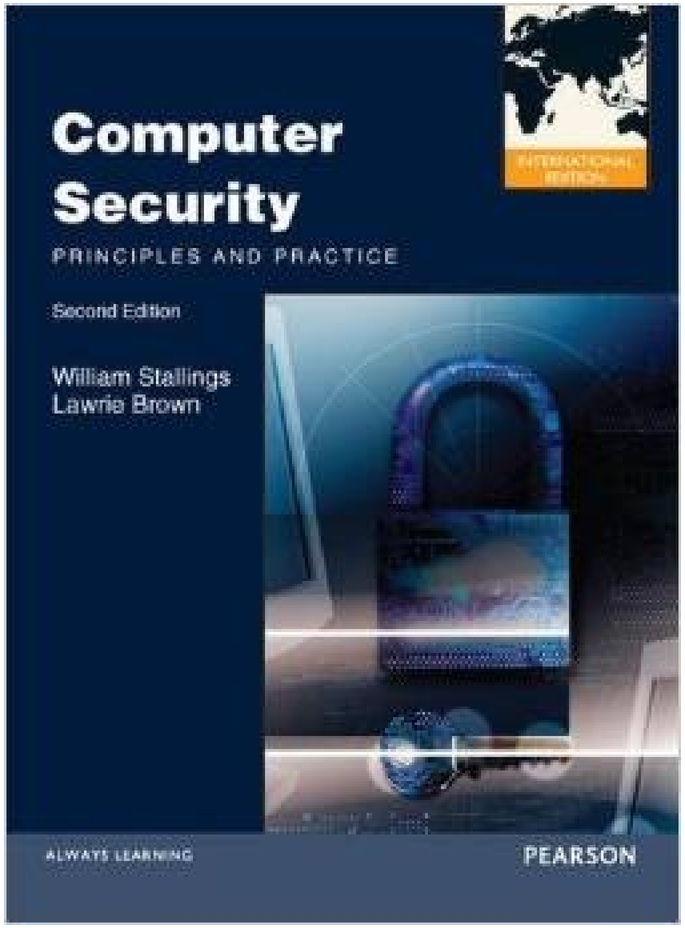
12 – Privacy

13 – Usable security

Primary literature

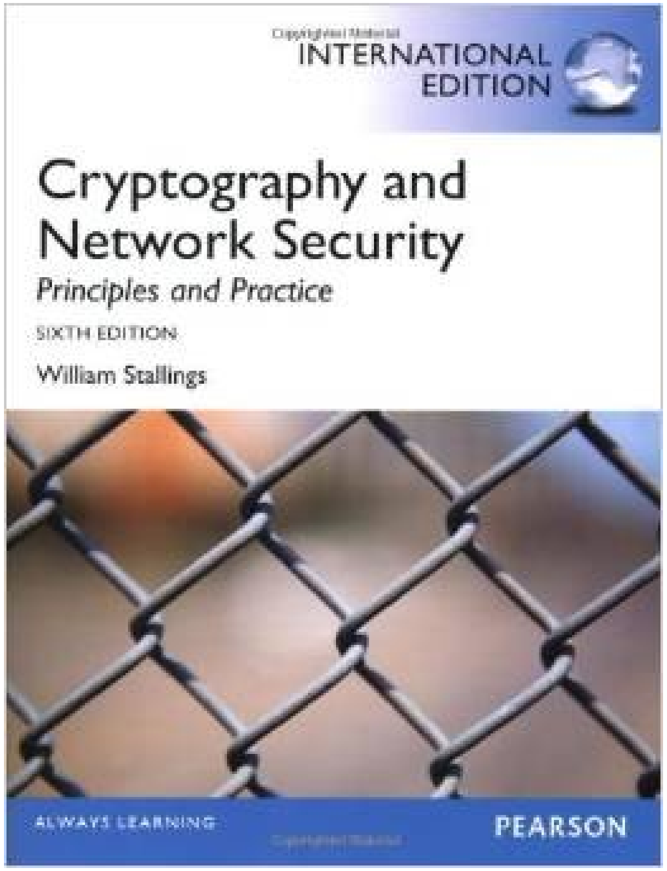
- William Stallings, Lawrie Brown: "Computer Security: Principles and Practices", 2nd edition, Pearson, 2012, ISBN 978-0273764496, ca. 70€
(or any newer additions)

- **Acknowledgments**: Many slides are based on material from this book or have been directly adapted from a slide set by William Stallings and Lawrie Brown available from the Pearson lecturer center.



Additional literature

- William Stallings: "Cryptography and Network Security: Principles and Practice", 6th edition, Prentice Hall/Pearson, 2014, ISBN 978-0273793359, ca. 65€

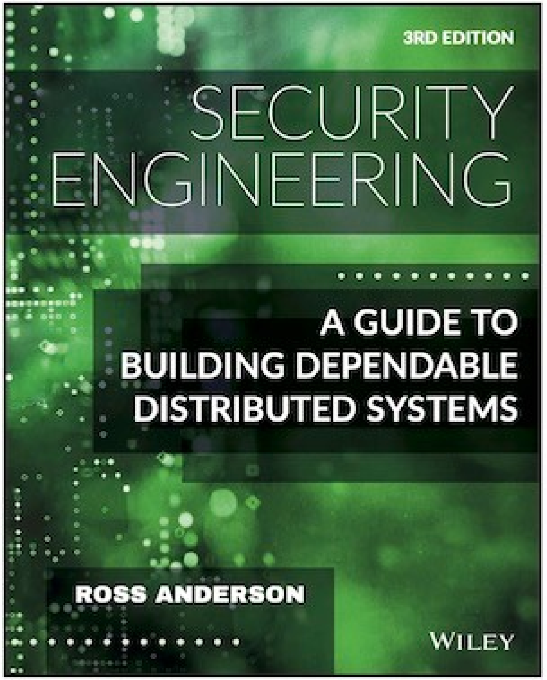


Additional literature

- Ross Anderson:
  ”Security Engineering”

  Third edition was fully available online (e.g., in Oct. 2020) at https://www.cl.cam.ac.uk/~rja14/book.html

  Some chapters remain available for free download



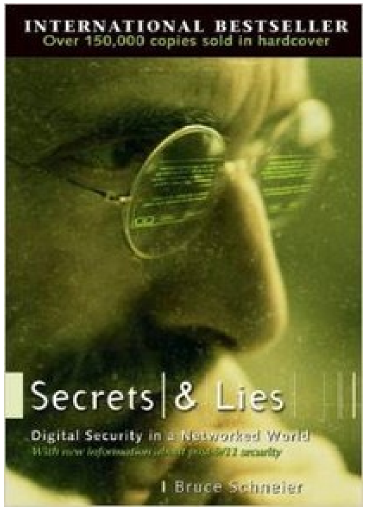
Additional literature

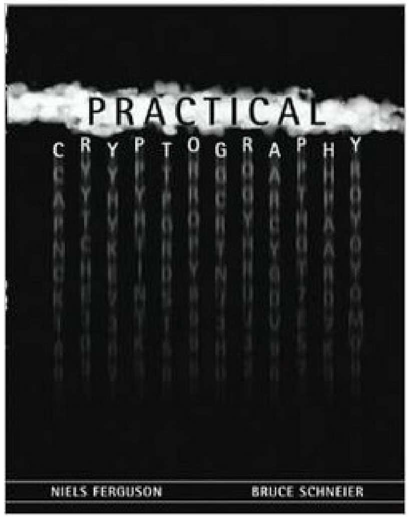
Bruce Schneier: „Applied Cryptography:

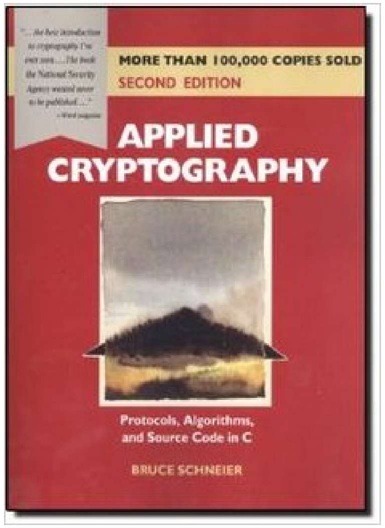
- Protocols, Algorithms and Source Code in C” (2nd edition), 2005

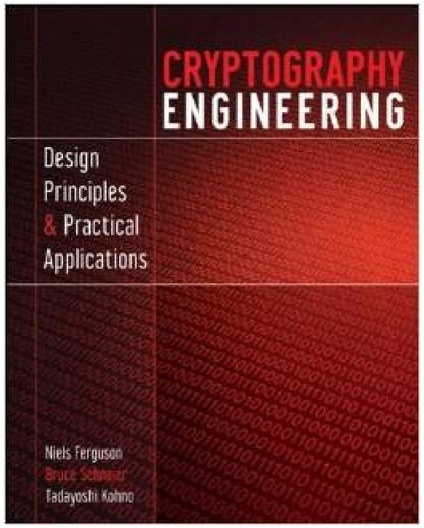
Niels Ferguson and Bruce Schneier:

- „Practical Cryptography”, 2003


INTERNATIONAL BESTSELLER
Over 150,000 copies sold in hardcover
Secrets & Lies
Digital Security in a Networked World
Bruce Schneier




MORE THAN 100,000 COPIES SOLD
SECOND EDITION
APPLIED CRYPTOGRAPHY
Protocols, Algorithms, and Source Code in C
BRUCE SCHNEIER



Additional material

- http://blog.cryptographyengineering.com/
- https://www.ssllabs.com/
- http://www.slideshare.net/digicomp/hacking-challenges
- …

Optional Material for self-study: Challenges in Offensive Security

- **JKU SIGFLAG team**: https://www.sigflag.at/ - highly encouraged to join the team if you enjoy solving puzzles
- http://try2hack.nl/
- http://overthewire.org/wargames/
- http://www.wechall.net/challs/
- http://google-gruyere.appspot.com/part1
- https://www.hacking-lab.com/

Open position – 1 year - 20h/week

- Project “Infraspec”
  - Automatic inspection of critical infrastructure
    - Specifically: by a robot 3D-scanning & comparing to previous scans supply ducts; incl. inspection of differences and detected problems
      - Airport (VIE), energy (Wiener Netze), BMLV, BMI…
- Tasks:
  - Capturing forensic evidence: Web user interface
    - Actions, alerts, display, stream data (video) …
  - Securing the data
    - Security model; encryption, signatures, timestamps
    - Exporting parts (e.g. time- or location-based) with secure logs (signatures, watermarks…)

  Design & Implementation

  - Obfuscation/anonymisation of 3D sensor data
    - Should still be usable, but unrecognizable

  Research

- Project start: 1.12.2022 (position can start later)

Open position – 1 year - 20h/week

- Project “Digidow”
  - Distributed digital identity, many partners (e.g. Ekey, KUK, NXP, 3-Banken-IT, Österreichische Staatsdruckerei)
  - Looking 10 years into the future of digital ID
- Tasks:
  - Biometric authentication
  - Reproducible and transparent system builds
  - Cryptographic privacy and signing protocols
  - Network privacy (e.g. Tor)
  - Android app development for user interaction
  - Localization (e.g. UWB)
- Project start: any time