Why is Security Important?

https://iuk.one/1033-1002

Clemens H. **Cap**
ORCID: 0000-0003-3958-6136

Department of Computer Science
University of **Rostock**
Rostock,Germany
clemens.cap@uni-rostock.de

Version 2

Overview

1. Integrity of Infrastructure
2. Protecting Personal Data
3. Binding Law
4. Social Stability
5. Technical Stability

1. Integrity of Infrastructure

The integrity of our technical and social infrastructure depends on cybersecurity solutions.

Integrity

Problem

If everything is networked
then everything can be attacked over the network.

Task for the Researcher

How can we connect most devices to the network
without opening them up to the resulting risks?

3 Examples of Attacks on Entire Nations

2007 Attack on Estonia:

- **Type:** Distributed denial of service attacks.
- **Victims:** Parliament, banks, public institutions, newspapers.
- **Effect:** Country disconnected from the Internet for 4 days.

2010 Stuxnet Attack on Iran:

- **Type:** Computer virus infection of PC connected to an industrial controller.
- **Victims:** Uranium centrifuges; changing speeds produced mechanical wear-out.
- **Effect:** Damage to Iranian nuclear engineering program.

2015 Power Grid Attack on Ukraine:

- **Type:** Complex, coordinated cyber-attack consisting of many elements.
- **Victims:** Industrial and powergrid nodes.
  SCADA = **S**upervisory **C**ontrol **a**nd **D**ata **A**cquisition
- **Effect:** 230.000 people without electricity for 1/2 day.

Further Possible Templates of Attacks

Remote Vehicles: Autonomous, networked cars, airplanes or drones as weapons.

Virtual Theft: Thief breaks into a bank from his "homeoffice".

Denial of Service: Power grid, transportation services, payment gateways of an entire country are disabled for 2 days.

Overuse: Lowering and raising the window blinds every 2 seconds for an entire night.

Military: Turning off weapon capabilities by software during a conflict.
Example: Israel and Syria
Example: US and Austrian Fighter Jets
Example: US and German Euro-Hawk Drones

2. Protecting Personal Data

Protecting personal data is an essential task in cybersecurity. Advanced crypto methods can be used for **enhancing** privacy.

Problem

Protecting privacy is a complex problem:

- **Mind set:** An understanding the need for privacy.
- **Legal:** GDPR / DSGVO / laws and regulations.
- **Organizational:** Eg: Clean desk, know your client policies etc.
- **Technical:** Eg: Encryption, privacy by design, access control etc.

Hypothesis: Technological solutions alone often do not help.

Research Questions for You: Privacy

Why is privacy necessary to ensure the dignity of human life?
Give examples!

Where do you see **practical problems** with current data protection **legislation**?
Give examples!

Organizational measures for protecting personal data?
Give examples!

Question to be Answered by Research

Which possibilities do Privacy Enhancing Technologies (PET) offer?

What is a reasonable mix between cryptographic efforts, costs and (in)convenience?

3 Examples of Technologies:

- Zero Knowledge Proofs
- Secret Sharing
- Multiparty Computation

Example 1: Zero Knowledge Proofs

The Problem:

- **Peggy** wants to prove to Victor that she knows the solution to a problem.
- **Victor** wants to verify if Peggy knows the solution to a problem.

Criteria: Victor is

- **Convinced:** Believes that Peggy knows the solution.
- **Non-transferable:** Unable to claim knowledge of the solution towards others.
- **Zero-knowledge:** Learns nothing (zero) about that solution.

Practical use:

- The problem: Represents the user id of Peggy.
- The solution: Represents the password known only to Peggy.

Situation: Is that possible? Yes!

Example 2: Secret Sharing

The Problem:

- A password guards the access to a safe.
- Alice trusts her colleagues Bob, Carol, David and Erin.
- Alice learns, that one person is a traitor (but not who).
- Can Alice restrict the access in such a manner that **only two** of her colleagues **together** can access it?

Situation: Is that possible? Yes!
Alice can even impose more complex restrictions.

Example 3: Multiparty Computation: Naive Approach

Background:

- Alice, Bob, Carol and Dave each have a (private) number.
- They want to calculate the sum.

Question: Can they find an algorithm such that

- **Public output:** At the end, everybody knows the sum.
- **Anonymous input:** Nobody knows the number of any other participant.

Heads Up!

- For two persons, a sum is problematic. Why?
- For n persons, a product is problematic as well. Why?

Thus: Need redefinition of the problem.

Example 3: Multiparty Computation: Elaborate Approach

Background:

- There are n parties.
- f is a function of n variables denoted $v_1, \ldots, v_n$.
- The value v_j is known only to party number j.

Problem: Find an algorithm with the following 2 properties:

- **Public output:** At the end, every party knows $r = f(v_1, \ldots, v_n)$.
- **Info-minimal input:** Every party j knows only what it can deduce from r and v_j.

Situation: Is that possible? Yes!
It is a recent research area of its own, but, *essentially* yes.

Private Credit Scoring

Situation:

- Banker Alice wants to know if client Bob is able to pay back a loan.
- Bob wants that loan.
- Carol is a mobile operator and knows the payment morale of Bob

Question: How can Alice learn whether Bob should get the loan?

Solutions (1)

Solution 1: Data to the Program

- Carol sends Bob's payment data to Alice.
- **Problem:** Privacy Alice receives detailed payment data on Bob.
- **Real life:** Schufa, Fintech access to bank API.

Solution 2: Program to the Data

- Alice sends her evaluation program to Carol who feeds it with Bob's data.
- **Problem:** IP Protection Carols learns the tricks of Alice.
- **Real life:** Not done. Has Alice loses her business case.

Solution 3: Trusted Third Party

- Trent receives data (on Bob) from Carol and algorithm from Alice.
- **Problem:** Costs & trust issues: Trent must be paid and trusted.
- **Real life:** Rarely done due to these 2 problems.

Solutions (2)

Solution 4: Multiparty Computation

- Alice and Carol execute a multiparty protocol.
- Alice knows the answer to her question.
- Carol does not learn about the trade secrets of Alice.
- Alice does not learn Bob's data in detail.

Problem: No further disadvantages, but..

Real life:

- Protocols not well known.
- Research results rather recent.
- No wide implementations of technology in applications.
- Hopefully this will improve...

3. Binding Law

Technology may provide the required basis for applying law, but the situation can be ethically problematic.

Homework: Non-Repudiation

Repeat the basics: What was the protection goal of non-repudiation?

Technical Support for Legal Situations

Situation: Technology proves facts and the law governs the consequences.

Problems:

- Technology provides more or less than what the law is interested in.
- Technology provides more than deemed reasonable by society.

Technology provides more:

- Technology enables things which we do not want: Ultimate fate: Surveillance state

Technology provides less:

- Would it be possible in principle? Often: Yes. So let's implement it!
- How can we limit abuse of infrastructure once it exists?

Question

How can legally binding situations be implemented according to an ethically accepted social consensus?

Example: Criminal Prosecution

"**Datenschutz als Täterschutz**"

- Tracking down a criminal is made impossible by data protection.
- Where ends the data protection rights of suspects?

Core Doctrines of Law

- Commensurability of measures ("Verhältnismäßigkeit der Mittel")
- Presumption of innocence ("Unschuldsvermutung; kein Generalverdacht")
- Prosecutor must demonstrate guilt ("Schuldbeweis, Beweislast-Umkehr")
- No duty of self incrimination ("Keine Verpflichtung, sich selbst zu belasten")

In the US: "Doktrin der Früchte des vergifteten Baumes" (fruits of the poisoned tree)
Proofs obtained by illegal means must not be used in court.

Disclaimer: I am no lawyer and I am not giving legal advice.

Example: Devices as Witness

Scenario:

- My wife, kids and parents do not have to be witnesses against me.
- Reason: Protecting close human relationships.
- But: What about my mobile phone?
- Some phones know more than family knows.
- Do mobile phones need a witness protection?
- Should it be mandatory to render phone PINs and passwords?
- Should there be a backdoor for manufacturer / law enforcement?

Examples of cases:

- Carsharing location data
- Alexa witness of a murder
- Siri as key witness?

4. Social Stability

Social stability is connected with the behavior of people. Where are the limits of security technology regarding behavior?

Example: Elections

Situation: Elections are highly regulated.

- Fairness regulations: Rules for TV debates of candidates.
- Ad regulations: No party ads near election booth.

Problem 1: Technical integrity for determining the results.

- An interesting IT problem on its own.
- Symantec: Video on how to hack a voting machine.
- Security Magazine: Can the voting process be hacked?

Problem 2: What are the right regulations for **social media**?

- In Germany, political parties have a right to get postal addresses: Regulations
- What about access to social media profiles?
- Should mass-microtargetting via Facebook profiles be permitted?
- Remember the Facebook-Cambridge Analytica Case during Trump/Clinton 2016. Reporting by The New York Times and by The Guardian.

Example: Smart Mob

Situation: Lynch-Mob against an innocent but presumed-guilty person.

- Press report: Rheinische Post
- Press reports: Die Welt
- Wikipedia article

Situation: Apple patent for remotely turning off iPhone cameras

- Press report: Forbes
- Press report: The Guardian
- Press report: ZDNet
- Press report: Heise Newsticker
- Apple Patent

Questions

How can computer science help guarantee the authenticity of data?

To which extent should computer science support this in every situation?

Where are the boundaries between fake news, propaganda and liberty of expression?

Where are the dos and dont's for stabilizing society
from a computer technological perspective?

Is stability of society a higher goal than human dignity ("Menschenwürde")?

5. Technical Stability

Technical stability is the core but – as we see – not the only goal for cybersecurity.

Problems of Networked Systems

Leslie Lamports Famous Definition of a Distributed System

A **distributed system** is one
in which the failure of a computer you didn't even know existed
can **render your own computer unusable**.

- A networked system has systemic side effects.
- The border between safety and security becomes blurred.
- Side effects (safety) may be leveraged into attacks (security).

Example: DNS

DNS: Domain Name System

- Translates hostnames (`mybank.com`) into IP addresses (`128.20.30.55`).
- IP-adress is basis of global routing.
- Erroneous translation ("DNS-resolution") causes data to go to the wrong target.
- Badguy resides at 130.77.77.77.
- Attack causes `mybank.com` to be resolved incorrectly to `130.77.77.77`.
- Badguy gets my banking data.

Example: DNS spoofing (=DNS poisoning)

- DNS-responses often are cached and not authenticated.
- Attacker connects to network and injects DNS-response.
- Clients cache and use non-authenticated response.

Note 1: A seemingly innocent service is of core importance for security.

Note 2: Poisoning attacks try to inject fake data into caches.

Research Questions for You: DNS

Revise your knowledge on DNS and DNS-resolution!

What techniques are known to **prevent DNS spoofing attacks**?

Example: ARP

ARP: Address Resolution Protocol

- Translates (local) IP-address (`130.28.8.4`) to MAC-address (`AC:E8:22:31:46:44`).
- MAC-adress is basis of (local layer 2) addressing.
- Erroneous translation ("ARP-resolution") causes data to go to wrong recipient.
- Again ARP responses are cached by clients.

Example: ARP spoofing (=ARP poisoning)

Note: Similar situation as with DNS.

Research Questions for You: ARP

Revise your knowledge on ARP-resolution!

What techniques are known to **prevent ARP spoofing attacks**?

Example: OCSP

OCSP: Online Certificate Status Protocol

- **Problem:** Is the certificate for Alice correct or has the private key been stolen? Need to know at time of certificate use if Alice has retracted the certificate.
- **Idea:** Special OCSP server operated by CA provides the answer.

Example: Attack the OCSP service.

- Fake OCSP-reply allows fake identities, MITM attacks etc.
- Missing OCSP-reply forces client to abort connection or assume certificate correctness.

Research Question for You: OCSP

Revise your knowledge on certificates!

Would it be a good idea to cache OCSP replies?

What other attacks can be used on OCSP?

How can they be prevented?

Appendix

Contents of Appendix

Terms of Use (1)

Die hier angebotenen Inhalte unterliegen deutschem Urheberrecht. Inhalte Dritter werden unter Nennung der Rechtsgrundlage ihrer Nutzung und der geltenden Lizenzbestimmungen hier angeführt. Auf das Literaturverzeichnis wird verwiesen. Das Zitatrecht in dem für wissenschaftliche Werke üblichen Ausmaß wird beansprucht. Wenn Sie eine Urheberrechtsverletzung erkennen, so bitten wir um Hinweis an den auf der Titelseite genannten Autor und werden entsprechende Inhalte sofort entfernen oder fehlende Rechtsnennungen nachholen. Bei Produkt- und Firmennamen können Markenrechte Dritter bestehen. Verweise und Verlinkungen wurden zum Zeitpunkt des Setzens der Verweise überprüft; sie dienen der Information des Lesers. Der Autor macht sich die Inhalte, auch in der Form, wie sie zum Zeitpunkt des Setzens des Verweises vorlagen, nicht zu eigen und kann diese nicht laufend auf Veränderungen überprüfen.

Alle sonstigen, hier nicht angeführten Inhalte unterliegen dem Copyright des Autors, Prof. Dr. Clemens Cap, ©2020. Wenn Sie diese Inhalte nützlich finden, können Sie darauf verlinken oder sie zitieren. Jede weitere Verbreitung, Speicherung, Vervielfältigung oder sonstige Verwertung außerhalb der Grenzen des Urheberrechts bedarf der schriftlichen Zustimmung des Rechteinhabers. Dieses dient der Sicherung der Aktualität der Inhalte und soll dem Autor auch die Einhaltung urheberrechtlicher Einschränkungen wie beispielsweise Par 60a UrhG ermöglichen.

Die Bereitstellung der Inhalte erfolgt hier zur persönlichen Information des Lesers. Eine Haftung für mittelbare oder unmittelbare Schäden wird im maximal rechtlich zulässigen Ausmaß ausgeschlossen, mit Ausnahme von Vorsatz und grober Fahrlässigkeit. Eine Garantie für den Fortbestand dieses Informationsangebots wird nicht gegeben.

Die Anfertigung einer persönlichen Sicherungskopie für die private, nicht gewerbliche und nicht öffentliche Nutzung ist zulässig, sofern sie nicht von einer offensichtlich rechtswidrig hergestellten oder zugänglich gemachten Vorlage stammt.

Use of Logos and Trademark Symbols: The logos and trademark symbols used here are the property of their respective owners. The YouTube logo is used according to brand request 2-9753000030769 granted on November 30, 2020. The GitHub logo is property of GitHub Inc. and is used in accordance to the GitHub logo usage conditions https://github.com/logos to link to a GitHub account. The Tweedback logo is property of Tweedback GmbH and here is used in accordance to a cooperation contract.

Terms of Use (2)

Disclaimer: Die sich immer wieder ändernde Rechtslage für digitale Urheberrechte erzeugt für mich ein nicht unerhebliches Risiko bei der Einbindung von Materialien, deren Status ich nicht oder nur mit unverhältnismäßig hohem Aufwand abklären kann. Ebenso kann ich den Rechteinhabern nicht auf sinnvolle oder einfache Weise ein Honorar zukommen lassen, obwohl ich – und in letzter Konsequenz Sie als Leser – ihre Leistungen nutzen.

Daher binde ich gelegentlich Inhalte nur als Link und nicht durch Framing ein. Lt EuGH Urteil 13.02.2014, C-466/12 ist das unbedenklich, da die benutzten Links ohne Umgehung technischer Sperren auf im Internet frei verfügbare Inhalte verweisen.

Wenn Sie diese Rechtslage stört, dann setzen Sie sich für eine Modernisierung des völlig veralteten Vergütungssystems für urheberrechtliche Leistungen ein. Bis dahin klicken Sie bitte auf die angegebenen Links und denken Sie darüber nach, warum wir keine für das digitale Zeitalter sinnvoll angepaßte Vergütungssysteme digital erbrachter Leistungen haben.

Zu Risiken und Nebenwirkungen fragen Sie Ihren Rechtsanwalt oder Gesetzgeber.

Weitere Hinweise finden Sie im Netz hier und hier oder hier.

Citing This Document

If you use contents from this document or want to cite it,
please do so in the following manner:

Clemens H. Cap: Why is Security Important?. Electronic document. https://iuk.one/1033-1002
14. 4. 2021.

Bibtex Information: https://iuk.one/1033-1002.bib

```
@misc{doc:1033-1002,
   author       = {Clemens H. Cap},
   title        = {Why is Security Important?},
   year         = {2021},
   month        = {4},
   howpublished = {Electronic document},
   url          = {https://iuk.one/1033-1002}
}
```

Typographic Information:
Typeset on April 14, 2021
This is pdfTeX, Version 3.14159265-2.6-1.40.21 (TeX Live 2020) kpathsea version 6.3.2
This is pgf in version 3.1.5b
This is preamble-slides.tex myFormat©C.H.Cap

List of Slides

Legend:
continuation slide
slide without title header
image slide