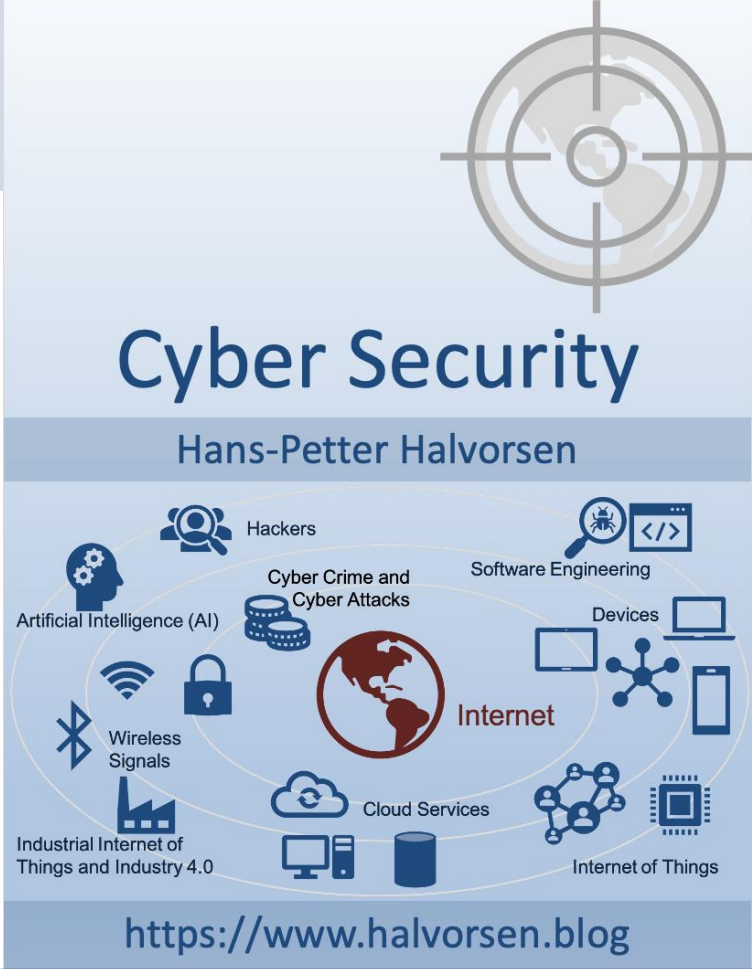
https://www.halvorsen.blog

Introduction to Cyber Security

Hans-Petter Halvorsen

Cyber Security

- Cyber Security Textbook
- Videos
- Code Examples
- Other Resources



https://halvorsen.blog/documents/technology/cyber_security

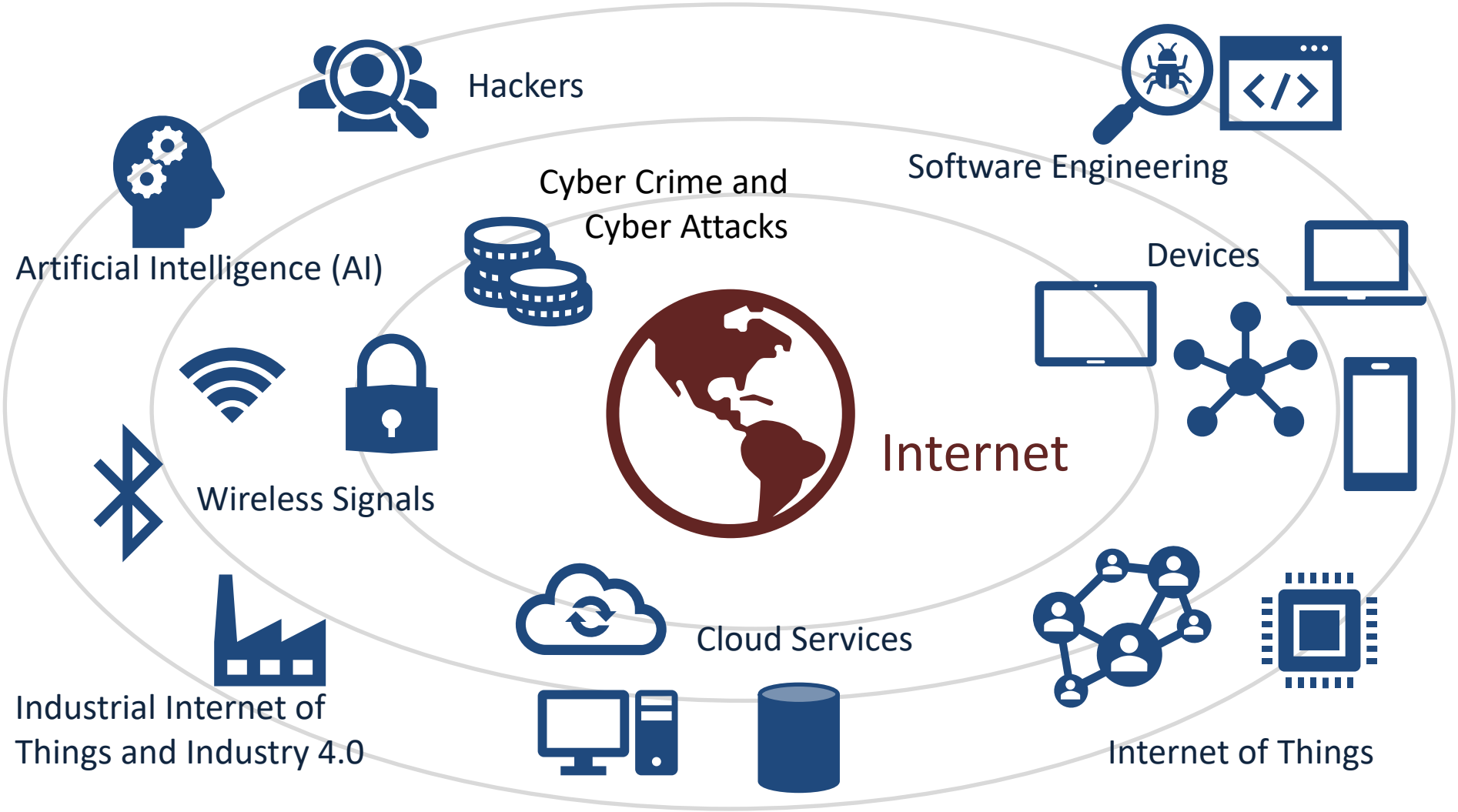
Contents

https://www.halvorsen.blog

Part 1

Internet and the Digital Age

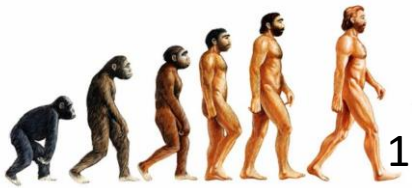
Hans-Petter Halvorsen


Hackers
Software Engineering
Artificial Intelligence (AI)
Cyber Crime and
Cyber Attacks
Devices
Wireless Signals
Internet
Cloud Services
Industrial Internet of
Things and Industry 4.0
Internet of Things

The Internet

- Since Internet connected all devices together a new era of our life was a fact.
- Internet is great for many things, but it is also a great place for criminals.
- We have all become a target for criminal acts in our homes and in our daily life
- With the good, comes the bad.

The Digital Age



1930

The first Computer
The Turing machine, 1936

Internet, 1968-91

The Microprocessor, 1971

1976: Apple I

1984: Macintosh

PC, 1981 (IBM)

Smartphone, 2007

World Wide Web, 1989-93

Internet of Things (IoT), Machine Learning and Industry 4.0

2016

Your Digital Life

- Internet, Cyber crime
- Facebook – Social Network founded by Mark Zuckerberg, 2.2 billion monthly active users
- You probably use hundreds of different Internet services
  - Facebook, Twitter, E-mail, Online Stores, Online Bank, etc.
- Are your personal data safe within these companies?
  - Is the data well protected (from hackers)?
  - Is the data sold to other companies (advertising purposes)?
  - Can you get an overview of the information stored on you?
  - Is it possible to delete it?

“Facebook/Cambridge Analytica”

The “Facebook/Cambridge Analytica” Issue:

- Facebook shared your personal data with Cambridge Analytica
- Cambridge used the data in the US election
- About 87 million people affected by the scandal

https://www.halvorsen.blog

Part 2

What is Cyber Security?

Hans-Petter Halvorsen

Cyber Security

- Cyber Security is the practice of protecting systems, networks, and programs from Digital Attacks
- Cyber Security is the strategy for protecting data systems from attacks where the purpose is to
  - Stealing money, personal information, system resources (e.g., crypto jacking, botnets), and a whole lots of other bad things

Data Security and Privacy

- Data Security: Protect digital data (e.g., data in a database) from destructive forces and from the unwanted actions of unauthorized users (e.g., hackers, etc.)
- Data Privacy: Issues regarding your personal data stored

https://www.halvorsen.blog

Part 3

Cyber Attacks

Hans-Petter Halvorsen

Hacking and Cyber Attacks

- What are Cyber Attacks?
  - Accessing, changing, or destroying sensitive information, extorting money from users, or interrupting normal business processes
- What is Hacker? Who is hacking?
  - Private persons, professional organizations and even countries.
- What is the goal with hacking?
  - The main goal is to make money or get information from other countries.

Cyber Security Threats

Different types of Cyber Security Threats:

- Spam
- Malware
- Ransomware
- Phishing
- Social Engineering
- Etc.

Spam

- Spam is digital junk mail that is sent to your e-mail system/address
- Spam is endless flood of emails and other messages that you never asked for.
- It started with e-mail, but we also have SMS, Social networking spam, etc.
- Spam is not necessarily dangerous, but very annoying

Malware

- Malware is a type of software designed to gain unauthorized access or to cause damage to a computer.
- Malware is short for “malicious software” (Norwegian: “skadelig programvare”).
- Examples of common malware includes viruses, worms, Trojan viruses, spyware, adware, and ransomware.

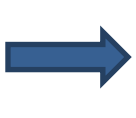
Ransomware

- Ransomware is a type of malicious software
- It is designed to extort money by blocking access to files or the computer system until the ransom is paid
- Examples: Email phishing and malvertising (malicious advertising)
- After it is distributed, the ransomware encrypts selected files and notifies the victim of the required payment
- Paying the ransom does not guarantee that the files will be recovered, or the system restored.
- The most "famous" Ransomware is the WannaCry Ransomware.

Ransomware

The Attacker sends email with malicious code

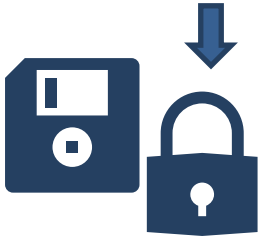
Attacker



Email phishing

User

The user triggers malicious code by open attachments or clicking on links in the email



Files are encrypted

The Attacked User sends Money/Bitcoins to the Attacker (and hope he will get a Key that can Decrypt the Data and make it readable again)

WannaCry

- The most “famous” Ransomware is the WannaCry Ransomware.
- The WannaCry ransomware attack was a worldwide cyberattack using a Cryptoworm
- Attacking Microsoft Windows PCs
- It was encrypting data and demanding ransom payments in the Bitcoin cryptocurrency

Phishing

- Phishing is the practice of sending fraudulent emails that resemble emails from reputable sources.
- The aim is to steal sensitive data like credit card numbers and login information, or to install malware on the victim's machine.
- Phishing is the most common type of cyber-attack.
- You can help protect yourself through education (teach them not to click on links, etc. from untrusted sources) or a technology solution that filters malicious emails.
- Spam vs Phishing: Spam is annoying but is normally not intended to hurt you. They want to sell you something

Social Engineering

- Social engineering is a tactic that adversaries use to trick you into revealing sensitive information.
- They can solicit a monetary payment or gain access to your confidential data.
- Social engineering can be combined with any of the threats listed above to make you more likely to click on links, download malware, or trust a malicious source.

SQL Injection

- A Structured Query Language (SQL) injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not.
- An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.

Man-in-the-middle Attack

- Man-in-the-middle (MitM) attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction.
- Once the attackers interrupt the traffic, they can filter and steal data.
- Can happen when you connects to an unsecure public Wi-Fi network

Denial-of-Service Attack (DoS)

- A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth.
- As a result, the system is unable to fulfill legitimate requests.
- Attackers can also use multiple compromised devices (Botnet) to launch this attack. This is known as a distributed-denial-of-service (DDoS) attack.
- A botnet is a network of devices that has been infected with malicious software

Malware

Hans-Petter Halvorsen

Malware

- Malware is a type of software designed to gain unauthorized access or to cause damage to a computer.
- Malware is short for “malicious software” (Norwegian: “skadelig programvare”).
- Examples of common malware includes viruses, worms, Trojan viruses, spyware, adware, and ransomware.

https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html

Types of malware

- Virus
- Worms
- Trojan virus
- Spyware
- Adware
- Ransomware
- Cryptojacking or Cryptomining malware

https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html

https://www.halvorsen.blog

Part 4

Data Privacy

Hans-Petter Halvorsen

Data Privacy

- You store lots of information about yourself when you use different devices, web sites and services. Can you trust that the data is safe?
- Data Privacy deals with issues regarding your personal data stored on internet, etc.
- GDPR: General Data Protection Regulation. EU directive. Purpose: Protect the privacy and the data stored, i.e., protection of your digital life

https://www.halvorsen.blog

GDPR

Hans-Petter Halvorsen

GDPR

GDPR: General Data Protection Regulation

Purpose:

- Protect the privacy and the data stored, i.e., protection of your digital life
- Better control of your personal data
  - What kind of data is stored?
  - Should be able to delete them

GDPR

- EU regulation
- All countries and companies within EU need to follow the regulation
- Also outside EU if the company save data about EU citizens
- Large fines have been given to those who do not comply with the GDPR regulations

GDPR

About: Data Protection and Privacy

Main contents:

1. You decide what kind of data that should be stored and what the data should be used for
2. Privacy statements: It should be clear what you say yes to
3. It should be possible to later delete the information stored about you

https://www.halvorsen.blog

Part 5

Data Security

Hans-Petter Halvorsen

Data Security

- Data Security: Protect digital data (e.g., data in a database, files on your computer, etc.) from destructive forces and from the unwanted actions of unauthorized users (e.g., hackers, etc.)

How to be Secure?

- How can you avoid cyber attacks in general?
- What can you do as a company or a private person?

Here are some examples:

- Access control
- Passwords
- Firewall
- Antivirus and antimalware software
- VPN
- Wi-Fi Network
- Security Updates
- Backup
- Education
- Etc.

Access Control

- You need to login with a Username and a Password
- An additional layer has also been common: Two-factor authentication

Passwords

- Make sure to use secure passwords
- Don’t use the same password for all your services and software systems
- Make sure to protect your password (don’t give it to others)
- Use Two-factor authentication

Two-factor authentication

- You receive a code on SMS or E-mail that you need to use in addition to Username/Password
- Or more common nowadays: You use an Authenticator App on your smartphone

Firewall

- A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- Firewalls are the first line of defense in network security.
- A firewall can be hardware, software, or both.
- Windows 10 has a built-in firewall
- A web application firewall (WAF) is an application firewall for HTTP applications. A WAF creates a shield between the web application and the Internet, which can avoid many common attacks, such as cross-site scripting (XSS) and SQL injection.

Antivirus/antimalware Software

- The name “Antivirus” software is a little old, because viruses are just one kind of malware in today’s world of cyber threats.
- Though viruses still exist, there are other forms of malware that are more common these days
- All computers should have Antivirus Software today
- Windows 10 has a built-in Antivirus/antimalware Software
- E-mail software also have Antivirus/antimalware/Spam Software

VPN

- A Virtual Private Network encrypts the connection from an endpoint to a network, often over the Internet.

Wi-Fi

- Use only secure Wi-Fi networks, not open Wi-Fi network that don’t need password, etc.
- Standards:
  - Wired Equivalent Privacy (WEP)
  - Wi-Fi Protected Access (WPA/WPA2)

Security Updates

- Today, all software needs to be continuously updated
- Make sure that your OS (PC, Smartphone, etc.) is always up to date

Development of Software

What can the Software Developers do to make secure software?

- Make sure software has proper Authentication
  - Keywords: Encryption and Decrypting, Hashing, Salting, 2 Factor Authentication
- Avoid SQL Injection
- …

Encryption and Decryption

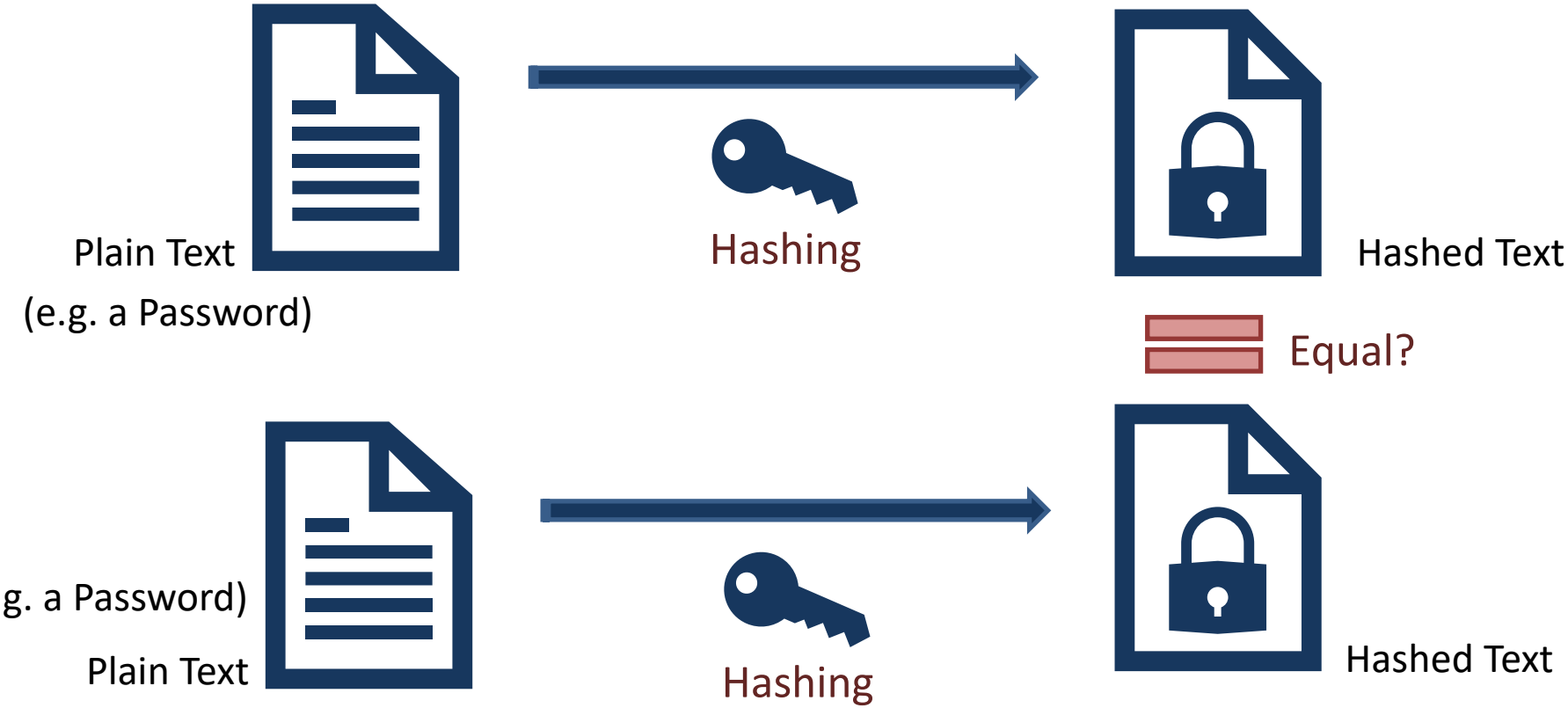
- Encryption is the practice of scrambling information in a way that only someone with a corresponding key can unscramble and read it.
- Encryption is a two-way function.
- When you encrypt something, you're doing so with the intention of decrypting it later.
- To encrypt data, you use an algorithm. Many different encryption algorithms do exist

Encryption and Decryption

Encryption and Hashing

- Hashing is the practice of using an algorithm to map data of any size to a fixed length.
- Encryption is a two-way function
- Hashing is a one-way function.
- While it's technically possible to reverse-hash something, the computing power required makes it unfeasible. Hashing is one-way.
- Encryption is meant to protect data in transit, hashing is meant to verify that a file or piece of data hasn't been altered—that it is authentic. In other words, it serves as a check-sum.
- Every hash value is unique

Hashing


Plain Text
(e.g. a Password)
Hashing
Hashed Text
Equal?
(e.g. a Password)
Plain Text
Hashing
Hashed Text

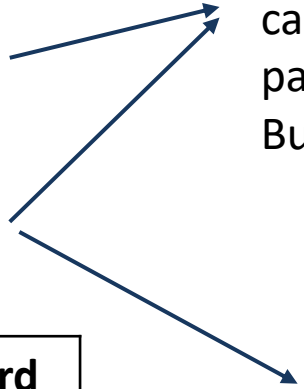
Encryption and Hashing

- Encryption is a two-way function.
- You encrypt information with the intention of decrypting it later.
- Examples when to use encryption:
  - Protecting Files and Information on your Computer
  - Protecting your Cloud data
  - Transmitting Data between 2 Computers
  - Etc.
- The key is that Encryption is reversible. Hashing is not.

Hacking Hashing?

Password Table for System X

UserName	HashedPassword
Mike	4420d1918bbcf7
Bob	73fb51a0c9be7d
Peter	4420d1918bbcf7



If a Hacker gets access to this Database, he can see that Mike and Peter have the same password.
But he does not know the actual password

If the Hacker has access to so-called "**Rainbow table**" (which is essentially a pre-computed database of hashes), he may also be able to find the Password (as seen here)

Password	HashedPassword
tesla	4420d1918bbcf7
friendship	73fb51a0c9be7d
bicycle	7420e1618abcf6

Rainbow table

If you have a complicated password, it is less likely that your password is in such a Rainbow table

Salting

- Salting is a technique typically used for Password Hashing.
- It is a unique value that can be added to the end of the password to create a different hash value.
- The additional value is referred to as a “salt”.
- This is done to make it even more secure.
- Typically, the Hashing Algorithm uses a Random salt.
  - This prevents an attacker from seeing whether users have the same password.

Salting

```
password = "Password123"
salt = "Tesla"

passwordHashed = HashPassword(password, salt);
```

Typically, Salting is built into the Hashing Algorithm and it is changed every time

```
password = "Password123"

ph1 = HashPassword(password);
ph2 = HashPassword(password);
```

ph1 ≠ ph2

This means if 2 different Users use the same Password, the Hashed Password will be different!

Hacking Hashing with Salt?

Assume Mike and Peter use the same Password

UserName	HashedPasswordwithSalt
Mike	4420d1918bbcf7
Bob	73fb51a0c9be7d
Peter	4520d1818cbcf7

If a Hacker gets access to this Database, he cannot see that Mike and Peter have the same password.

Because a random Salt has made these 2 Hashed Passwords different!

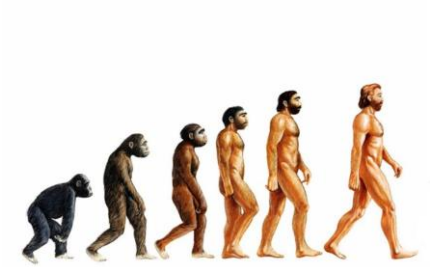
https://www.halvorsen.blog

Part 6

Internet of Things and Cyber Security

Hans-Petter Halvorsen

Industry 4.0



20 mill Years ago

Year Zero

Water, Steam and Mechanical production

Industry 1.0

~1784

Industry 2.0

Electricity and mass production

~1870

Industry 3.0

Electronics, IT and Automation

~1969

Industry 4.0

Internet of Things

Robotics

Today

~2011->

Industry 4.0

- Industry 4.0 is the new buzzword for the combination of industry, automation and the current Internet of Things (IoT) technology.
- Also referred to as IIoT
- Industrial Internet of Things (IIoT)
- A new approach to achieve results that weren't possible 10 years ago thanks to advancements in technology over the past decade.

Internet of Things and Cyber Security

- Security is crucial in IoT/IIoT Applications
- An important standard is IEC62443

IEC62443

- Cyber Security standard for IACS systems
- IACS – Industrial Automation and Control Systems.

References

- Data Security: https://en.wikipedia.org/wiki/Data_security
- GDPR: https://gdpr-info.eu
- GDPR - Wikipedia: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
- What is Cyber Security? https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Hans-Petter Halvorsen

University of South-Eastern Norway

www.usn.no

E-mail: hans.p.halvorsen@usn.no

Web: https://www.halvorsen.blog