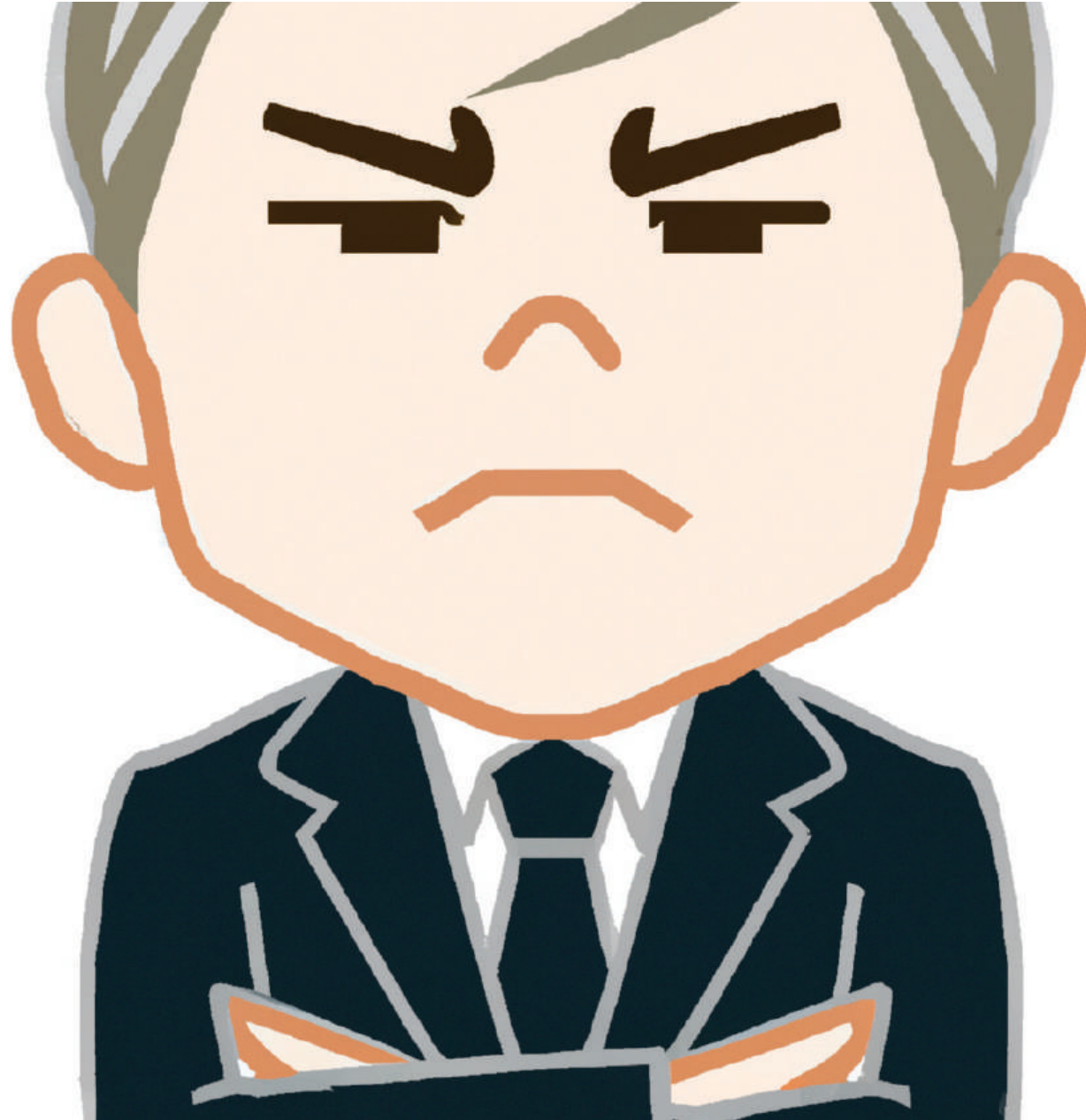


TDT4237: Lecture 1

Security principles



Outline

- Why security matters?
- Some examples of threats or attacks
 - Web defacement
 - Infiltration, control hijacking
 - Phishing
 - Data theft or loss
 - Denial of service
 - Ransomware
- Basic security goals
- Security guidelines

Why security matter?

- A record 81,5% of organizations suffered from a successful cyberattack last year.
- The vast majority (85,8%) of organizations are experiencing an IT security skills shortfall.

2024 Cyberthreat Defense Report | (ISC)² (isc2.org)
<https://www.isc2.org/landing/Cyberthreat-Defense-Report>



NTNU



The Global Risks Report 2024 19th Edition

INSIGHT REPORT

In partnership with Marsh McLennan and Zurich Insurance Group

Risk categories

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

2 years

- | | |
|------------------|-----------------------------------|
| 1 st | Misinformation and disinformation |
| 2 nd | Extreme weather events |
| 3 rd | Societal polarization |
| 4 th | Cyber insecurity |
| 5 th | Interstate armed conflict |
| 6 th | Lack of economic opportunity |
| 7 th | Inflation |
| 8 th | Involuntary migration |
| 9 th | Economic downturn |
| 10 th | Pollution |



Source

World Economic Forum Global Risks
Perception Survey 2023-2024.

Some examples of threats and attacks



NTNU

Web defacement

- Replace legitimate pages with illegitimate ones

Defaced by Hmei7

Disclaimer:

You have been Hacked !!!, not because of your stupidity
That's because we love you, and we want to warn you
That your web still has large of vulnerability

Dear admin,
This was not a joke or dream, this is fucking reality

at last,
Tidak ada seorangpun, hewan atau banci yang disakiti dalam hacking ini ;)

Thanks:

God,cr4wl3r,black_raptor,Skulmatic,vYcod,Sudden_death,misterfribo,sacred_relic,
c4ur,Bobyhikaru,r13y5h4,r3m1ck,KaMtIEz,3n_byt3,Bl4ck_3n61n3,r4tu_leb4h,
v3n0m,ulga,K4l0ng666,and you!

Read more: <http://news.softpedia.com/news/IBM-Developer-Community-Website-Defaced-177457.shtml#ixzz4F7wmPpr6>

Web defacement (cont')



The Federal Depository Library
Program (fdlp.gov)

Following the U.S. drone strike in
Iraq in 2020

Image Source: [Dailymail.co.uk](https://www.dailymail.co.uk)

Infiltration, control hijacking

- Android: DroidDream Malware (2011)
- Infected 58 apps on Android market
- 260,000 downloads in 4 days
- Send premium-rate SMS message at night





NTNU

FireEye: Russian Research Lab Aided the Development of TRITON Industrial Malware

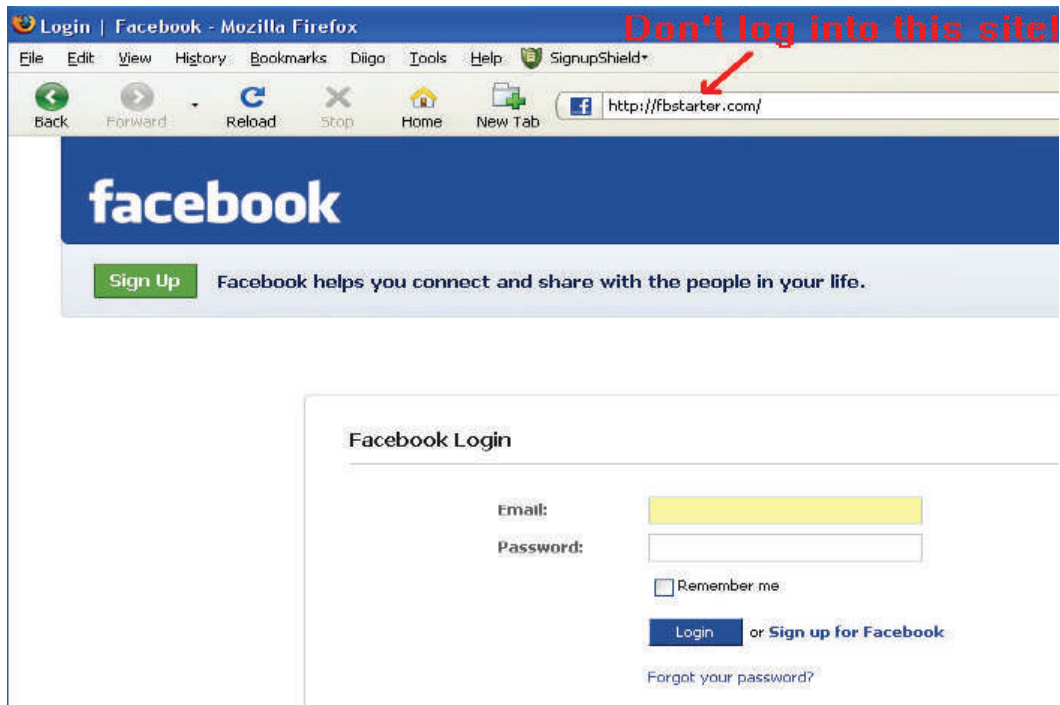
Oct 24, 2018 Swati Khandelwal



Cybersecurity firm FireEye claims to have discovered evidence that proves the involvement of a Russian-owned research institute in the development of the [TRITON malware](#) that caused some industrial systems to unexpectedly shut down last year, including a petrochemical plant in Saudi Arabia.

Phishing

- Spoofed site that looks real



Read more: New Phishing Attack Spreading On Facebook. This Time From Fbstarter (2009).
<https://techcrunch.com/2009/04/30/new-phishing-attack-spreading-on-facebook-this-time-from-fbstarter/>

Phishing (cont')

- Lure user through, e.g., phishing emails or SMS



Data theft / Data loss

May 2016:

Another Day, Another Hack: 117 Million LinkedIn Emails And Passwords

January 2023:

Twitter hacked, 200 million user email addresses leaked, researcher says

<https://www.vice.com/en/article/78kk4z/another-day-another-hack-117-million-linkedin-emails-and-password>

<https://www.reuters.com/technology/twitter-hacked-200-million-user-email-addresses-leaked-researcher-says-2023-01-05/>

Hacker claims breach of US location tracking company Gravy Analytics

GRAFIKK: HENRIK LIED / NRK

By Raphael Satter and A.J.

January 9, 2025 12:45 AM GMT

Companies



Gravy Analytic



Redsense Med

ASHBURN, Virginia, Jan 8 (Reuters) — A hacker claiming to be a former employee of location tracking firm Gravy Analytics said on Monday that the company had been breached.

It is not clear exactly how and when the breach occurred, but screenshots uploaded on a public forum carried a claim that the company had been hacked.



Denial of service (DoS)

- Flood server with packets
- Cause server to drop legitimate packets
- Make service unavailable



CNET > Security > HSBC hit by broad denial-of-service attack

HSBC hit by broad denial-of-service attack

The multinational bank confirms attack, saying it "did not affect any customer data, but did prevent customers using HSBC online services."

Oct. 2012

June 2022:



ЛЕГИОН - КИБЕР СПЕЦНАЗ РФ

☀️ Доброе утро Норвегия! ! Всем отрядам к бою ! ⚡️ L7...

Казалось бы, причем тут Норвегия?

"Норвежские власти отклонили заявку России на пропуск грузов для российских поселков на Шпицбергене через единственный пропускной пункт на российско-норвежской границе Стурскуг, сообщили в МИД страны.

«Конкретная заявка на получение разрешения на перевозку была отклонена 15 июня 2022 года», – сообщило телеканалу NRK министерство, передает РИА «Новости».

В апреле глава МИД Норвегии Анникен Хюитфельдт заявила о решении закрыть для проезда грузовиков из России пункт пропуска Стурскуг на границе. Также было решено ввести запрет для захода судов из России в порты, кроме рыболовных" 👁 2.2К изменено 09:44

Ransomware

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue

DNV-angriperne krever løsepenger: Holder program for skipsstyring som gissel


DNV har fått løsepengekrav etter et datainnbrudd på lørdag. Det rammet servere med programvare for rederiers flåtestyring.



DNV har solgt programvaren Ship Management til 70 kunder med en flåte på totalt 1.000 skip.
 Illustrasjon: DNV

Cyber-attack on ShipManager, a DNV software

Published: 16 January 2023
 Author: [Anne Vandbakk](#)
 Contact: [Margrethe Andersen](#)
[Anne Vandbakk](#)

CONTACT US: 

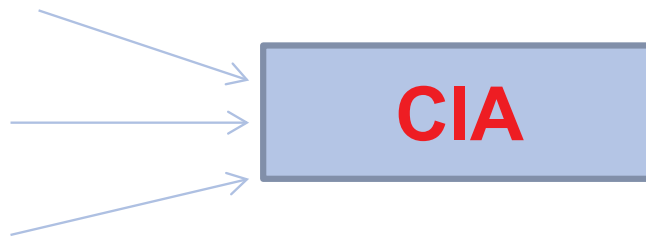
DNV confirms its ShipManager software was victim of a ransomware cyber-attack on the evening of Saturday 7 January. DNV experts have shut down ShipManager's IT servers in response to the incident. All users can still use the onboard, offline functionalities of the ShipManager software.

Discussion (5 minutes)

- What do you think these companies could have done to prevent these attacks?

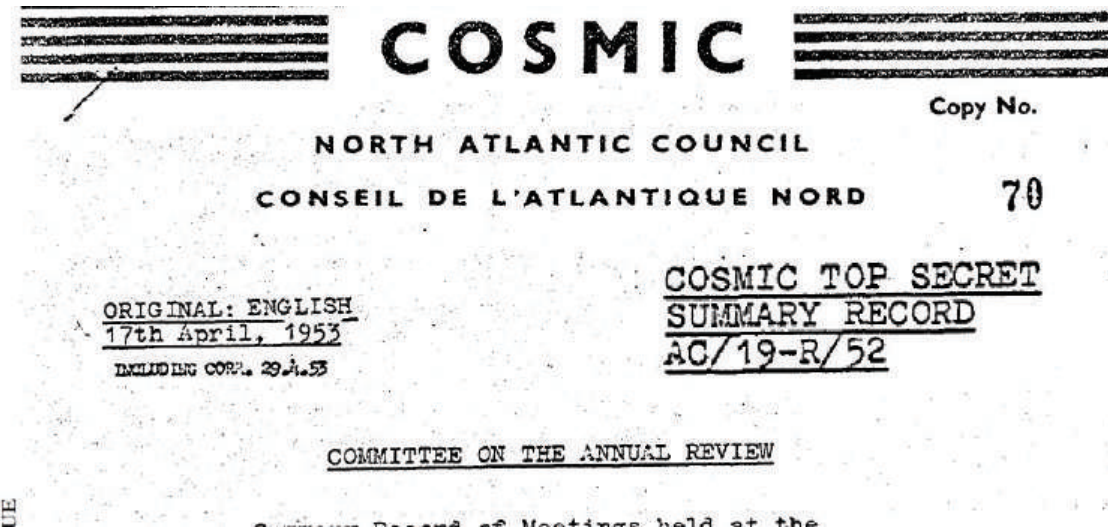
Basic security goals

- **Confidentiality**
- **Integrity**
- **Availability**
- Privacy
- Accountability
- Non-Repudiation



Confidentiality

- Keep something secret
 - Communication
 - Data on storage (at rest)
- Typically accomplished with
 - Cryptography
 - Authentication
 - Authorization
 - Sealed envelopes
 - Etc.



Integrity

- Data integrity = No corruption
- Control integrity = No control hijacking
- Different from confidentiality
 - Confidentiality: who can **read** the message
 - Integrity: who can **write** the message
- Sometimes accomplished with
 - Message/data hashing

Availability

- System uptime
- System response time
- Free storage



Privacy

- Right to be left alone
- Different from confidentiality
 - Confidentiality: the secret of business information
 - Privacy: the protection of personal information



Accountability

- Logging and audit trails
- Accomplished by
 - Secure timestamping
 - Data integrity in logs and audit trails



Non-Repudiation

- Two parties cannot deny that they have interacted with each other
- A trusted 3rd party can be used
 - E.g., Alice wants to prove to Trent that she did a transaction with Bob
- Generate evidence/receipts (digitally signed statements)

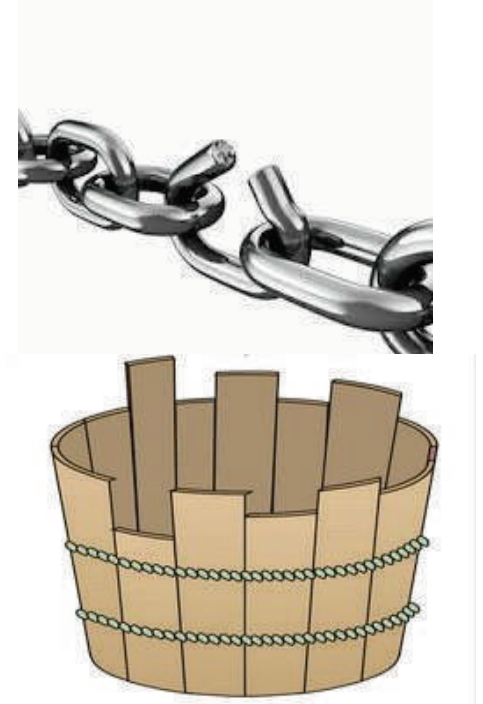


Security guiding principles

1. Secure the weakest link
2. Practice defense in depth
3. Fail securely
4. Compartmentalize
5. Be reluctant to trust
6. Follow the principle of least privilege
7. Keep it simple
8. Promote privacy
9. Remember that hiding secrets is hard
10. Use your community resources

1. Secure the weakest link

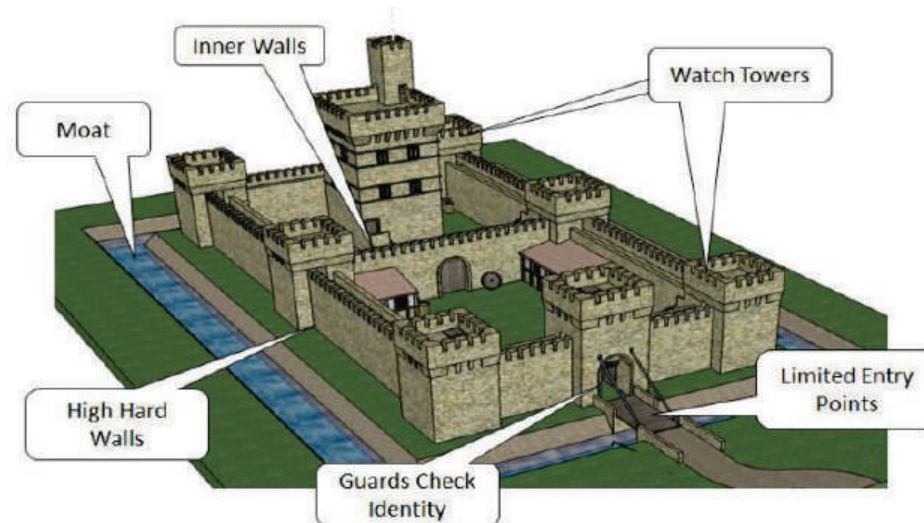
- *Information security is as strong as its weakest link*
- The attacker only needs to find one flaw
- Designers have to try and cover all possible flaws
- Common weak links
 - Weak passwords
 - People: social engineering attacks, internal attacks
 - Poor software



Cannikin Law

2. Practice defense in depth

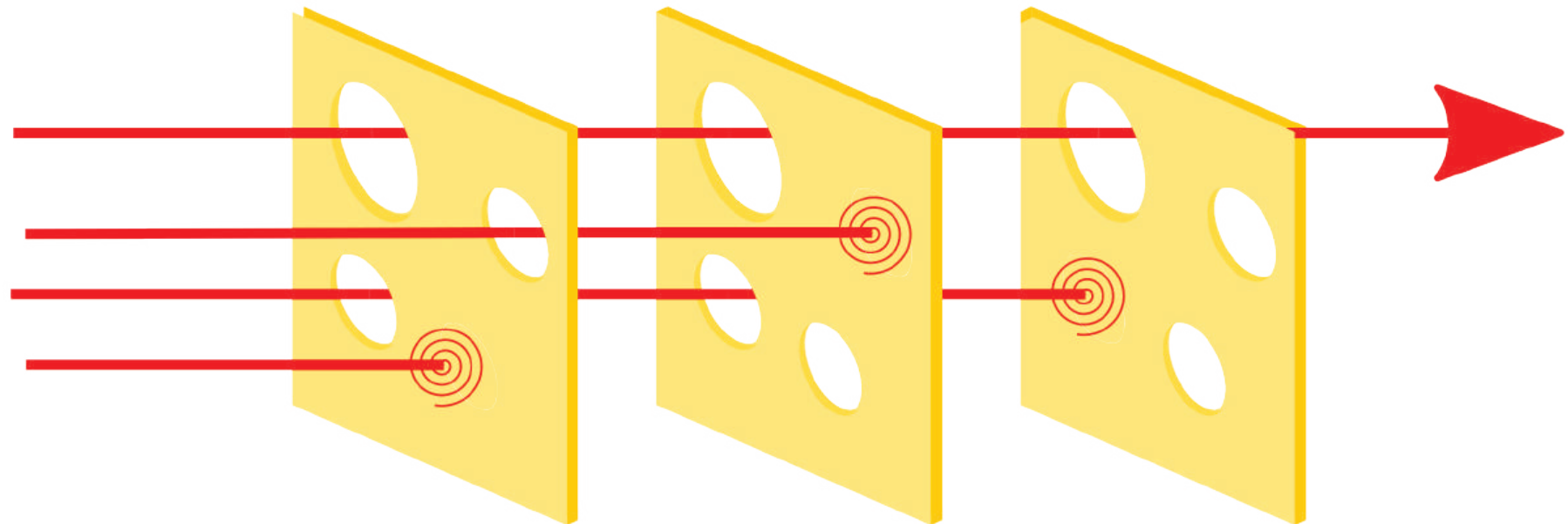
- Layers of defense
- Do not rely on one-shot security
 - E.g., firewall + authentication + authorization + cryptography, etc.





NTNU

Swiss cheese model



https://en.wikipedia.org/wiki/Swiss_cheese_model#/media/File:Swiss_cheese_model_textless.svg

2. Practice defense in depth (cont')

- Prevention
- Detection
- Containment (e.g., emergency response plan)
- Recovery

3. Fail securely

- Expect failure of security features
 - Exception of a security control itself
 - E.g., if a firewall fails, let no traffic in
 - Other exceptions can cause a security feature not to be invoked
 - E.g., when the line to the credit card company is down, no online credit card authentication, still allow transactions?



4. Compartmentalize

- Separate something (e.g., code) into parts
- Don't mix those parts, e.g.:
 - Separate network into different zones
 - Run the sensitive application on separate computers



5. Be reluctant to trust

- Skepticism is always good
 - Don't trust any code library
- Should not trust or assume the validity of user inputs
 - E.g., SQL injection attack

It's far too complicated
to explain, so you'll
have to trust me.



But I don't
trust you.



freshspectrum

6. Follow the principle of least privilege

- Minimum access necessary to get the job done
 - E.g., only system admin can read and modify system files
 - E.g., web server can read, but cannot modify .html file
- Minimum amount of time necessary
 - E.g., after a user is inactive for a while, the system logs out the user automatically

ive User Logout Settings

Logout

Message Content

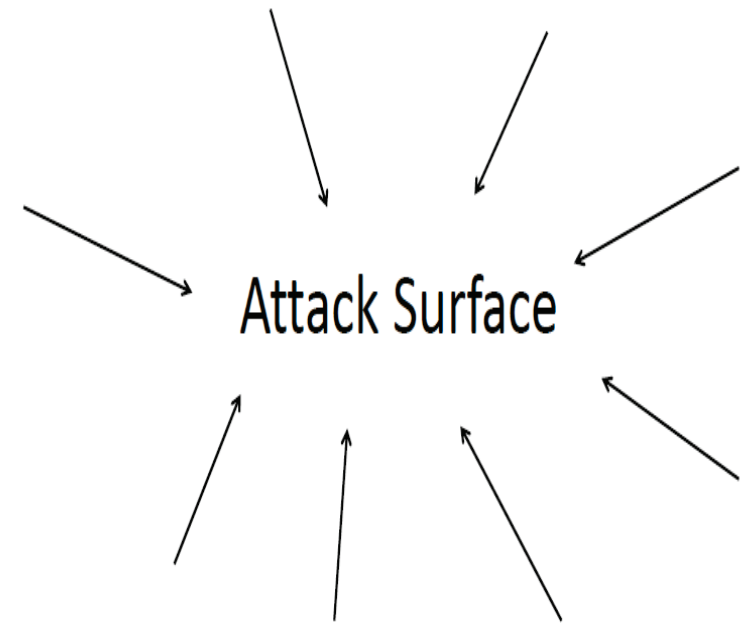
Session Timeout

You are being timed-out out due to inactivity. Please choose to stay signed in or to logoff.
Otherwise, you will be logged off automatically.

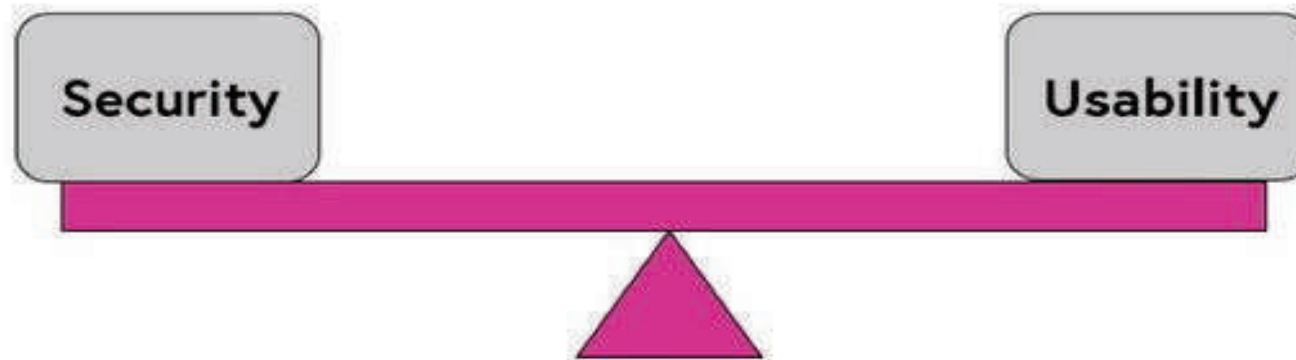
Continue (7)

7. Keep it simple

- Make systems simple
 - Reduce attack surface
 - Less functionality = less security exposure
 - All unnecessary features/functions off
 - Close unnecessary ports



7. Keep it simple (cont')



- Tradeoff: relative security benefit at only slight inconvenience



NTNU

PIN-kode fra SMS

Vi vil nå sende deg en valideringskode på SMS, vennligst bekreft at dette telefonnummeret er korrekt: +474 [redacted]

BEKREFT

Eller legg inn korrekt telefonnummer ved å trykke [her](#)

8. Promote privacy

- Do not to compromise the privacy of the user
- “nice-to-have” VS necessary information



9. Remember that hiding secrets is hard

- “Security by obscurity”
 - Maybe necessary, but not sufficient
- Attackers can probe for weaknesses
- Open vs. Close Source
 - A business decision, not a security one

10. Use your community resources

- Websites and sources of information
- “Known threats” and vulnerabilities
- E.g.,
 - Common vulnerabilities and Exposures
 - <https://cve.mitre.org/>
 - National vulnerability database
 - <https://web.nvd.nist.gov/view/vuln/search>
 - <https://web.nvd.nist.gov/view/vuln/statistics>
 - OWASP Top 10
 - https://www.owasp.org/index.php/OWASP_Top_Ten_Project

Next lecture...

