



Welcome to

# 1. Overview of Computer Security

KEA Kompetence Computer Systems Security 2019

Henrik Lund Kramshøj [hlk@zencurity.com](mailto:hlk@zencurity.com) @kramse  

Slides are available as PDF, [kramse@Github](mailto:kramse@Github)

1-overview-computer-security.tex in the repo security-courses

# Plan for today



## Subjects

- Confidentiality, Integrity and Availability
- Cost-Benefit Analysis
- Risk Analysis
- Human Issues
- Access Control Matrix

## Exercises

- Risk Analysis

# Reading Summary



Bishop chapter 1: An Overview of Computer Security

Bishop chapter 2: Access Control Matrix

Quote, page xxix,

the second edition continues to focus on the principles underlying the field of computer and information security. Many newer examples show how these principles are applied, or not applied, today; but the principles themselves are as important today as they were in 2002, and earlier.

# Goals: Increase Security Awareness



Fact of life: Software has errors, hardware fails

Sometimes software can be made to fail in interesting ways

Humans can be social engineered

We are being attacked by criminals - including paranoid governments

# Paranoia defined



## par·a·noi·a

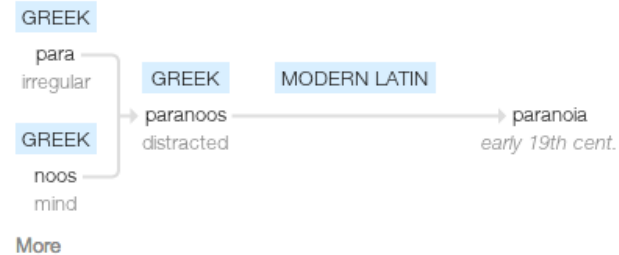
/ˌpærəˈnoɪə/ ⓘ

*noun*

noun: **paranoia**

1. a mental condition characterized by delusions of persecution, unwarranted jealousy, or exaggerated self-importance, typically elaborated into an organized system. It may be an aspect of chronic personality disorder, of drug abuse, or of a serious condition such as schizophrenia in which the person loses touch with reality.  
*synonyms:* [persecution complex](#), [delusions](#), [obsession](#), [psychosis](#) [More](#)
- suspicion and mistrust of people or their actions without evidence or justification.  
"the global paranoia about hackers and viruses"

### Origin



Source: google paranoia definition

# Face reality



From the definition:

suspicion and mistrust of people or their actions **without evidence or justification. the global paranoia about hackers and viruses**

It is not paranoia when:

- Criminals sell your credit card information and identity theft
- Trade infected computers like a commodity
- Governments write laws that allows them to introduce back-doors - and use these
- Governments do blanket surveillance of their population, implement censorship, threaten citizens and journalist

You are not paranoid when there are people actively attacking you!

I recommend we have appropriate paranoia (DK: passende paranoia)

# Overlapping Security Incidents



New data breaches nearly every week, these from danish news site version2.dk

Problem, we need to receive data from others

Data from others may contain malware

Have a job posting, yes

- then HR will be expecting CVs sent as .doc files

**Flere detaljer i gigantisk hotel-hack: 5,25 mio. ukrypterede pasnumre taget**

Jakob Møllerhøj | Sikkerhed | 07. jan 2019

3

**7,6 millioner spillerkonti lækket fra populært onlinespil**

Niels Møller Kjemtrup | Sikkerhed | 07. jan 2019

2

**Største læk i tysk historie: Politikeres og kunstneres data smidt på nettet**

Morten Egedal | Sikkerhed | 04. jan 2019

2

**Gentleman-aftale mellem politiske partier skal danne mur mod datalæk, hacking og fake news**

Louise Holst Andersen | Sikkerhed | 04. jan 2019

12

**Boligfond beklager læk af følsomme persondata: En menneskelig fejl**

Sikkerhed | 28. dec 2018

6



or the other way

## Attackers used a LinkedIn job ad and Skype call to breach bank's defences

### The attack

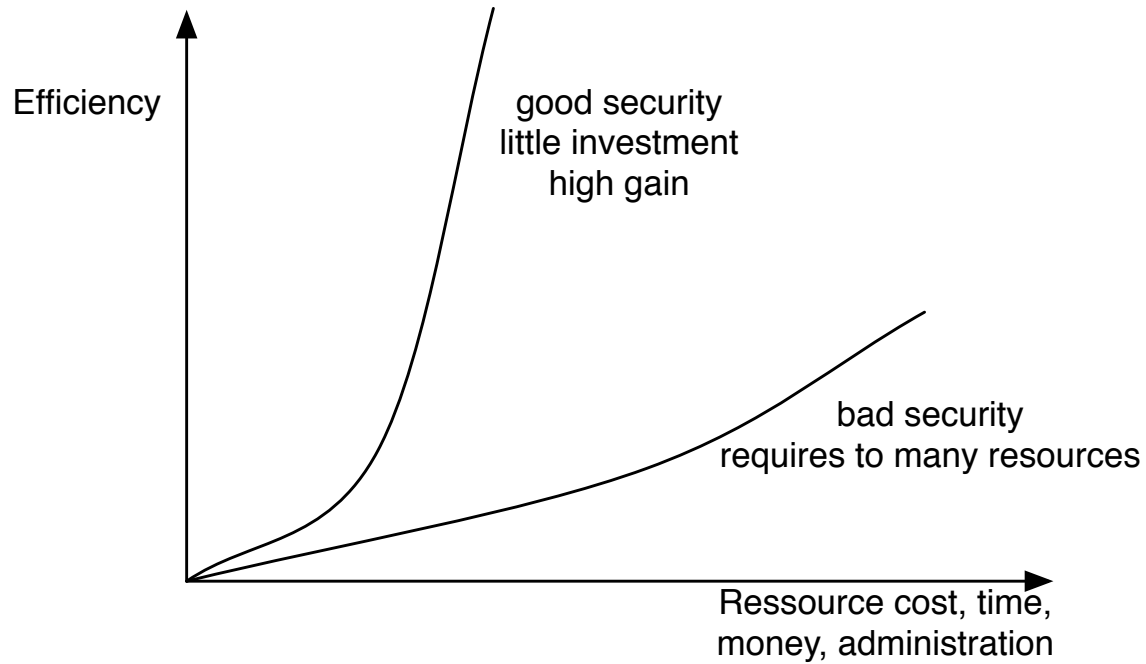
One of these is the Chilean news site's claim that the attack started with a LinkedIn advert offering a developer role to which a Redbanc employee replied.

The attackers set up a Skype call to conduct an interview during which the individual was tricked into downloading a file called ApplicationPDF.exe, sent via a weblink, which subsequently infected the employee's computer.

<https://nakedsecurity.sophos.com/2019/01/21/attackers-used-a-linkedin-job-ad-and-skype-call-to-breach-banks-defences/>



# Good security



You always have limited resources for protection - use them as best as possible

# Recommendations



## **Keep updated!**

- read web sites, books, articles, mailing lists, Twitter, ...

## **Always have a chapter on security evaluation**

- any process must have security, like RFC Request for Comments have

## **Incident Response**

- you WILL have security incidents, be prepared

## **Write down security policy**

- including software and e-mail policies

# Advice



Use technology

Learn the technology - read the freaking manual

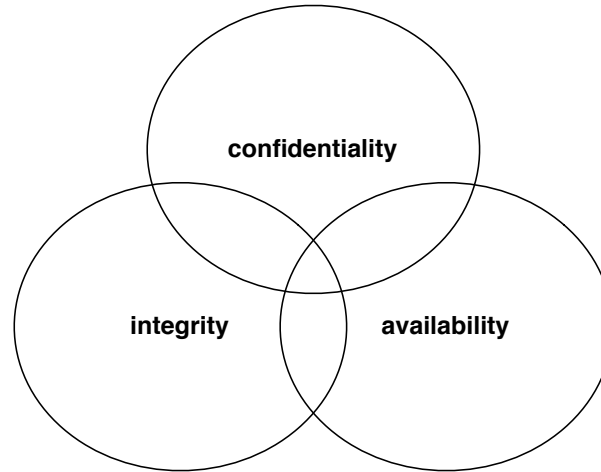
Think about the data you have, upload, facebook license?! WTF!

Think about the data you create - nude pictures taken, where will they show up?

- Turn off features you don't use
- Turn off network connections when not in use
- Update software and applications
- Turn on encryption: IMAPS, POP3S, HTTPS also for data at rest, full disk encryption, tablet encryption
- Lock devices automatically when not used for 10 minutes
- Dont trust fancy logins like fingerprint scanner or face recognition on cheap devices

But which features to disable? Let the security principles guide you

# Confidentiality, Integrity and Availability



We want to protect something

Confidentiality - data kept a secret

Integrity - data is not subjected to unauthorized changes

Availability - data and systems are available when needed

# What is data?



Personal data you dont want to loose:

- Wedding pictures
- Pictures of your children
- Sextapes
- Personal finances

Source: picture of my son less than 24 hours old - precious!

# Security is a process



Remember:

- what is information and security?
- Data kept electronically
- Data kept in physical form
- Don't forget the human element of security

Incident Response and Computer Forensics reaction to incidents

Good security is the result of planning and long-term work

## Security is a process, not a product, Bruce Schneier

Source for quote: [https://www.schneier.com/essays/archives/2000/04/the\\_process\\_of\\_secur.html](https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html)

# Work together



Team up!

We need to share security information freely

We often face the same threats, so we can work on solving these together

# Goals of Security



Prevention - means that an attack will fail

Detection - determine if attack is underway, or has occurred - report it

Recovery - stop attack, assess damage, repair damage



# Policy and Mechanism



**Definition 1-1.** A *security policy* is a statement of what is, and what is not, allowed.

**Definition 1-2.** A *security mechanism* is a method, tool or procedure for enforcing a security policy.

Quote from Matt Bishop, Computer Security section 1.3

# Your data has already have been owned by criminals



The screenshot shows a web browser at the URL <https://haveibeenpwned.com>. The main heading is `';--have i been pwned?`. Below it, a subtext says "Check if you have an account that has been compromised in a data breach". A search bar contains the email `hlk@kramse.org` and a button labeled "pwned?". The result section, which has a dark red background, displays "Oh no — pwned!" and "Pwned on 7 breached sites and found no pastes (subscribe to search sensitive breaches)".

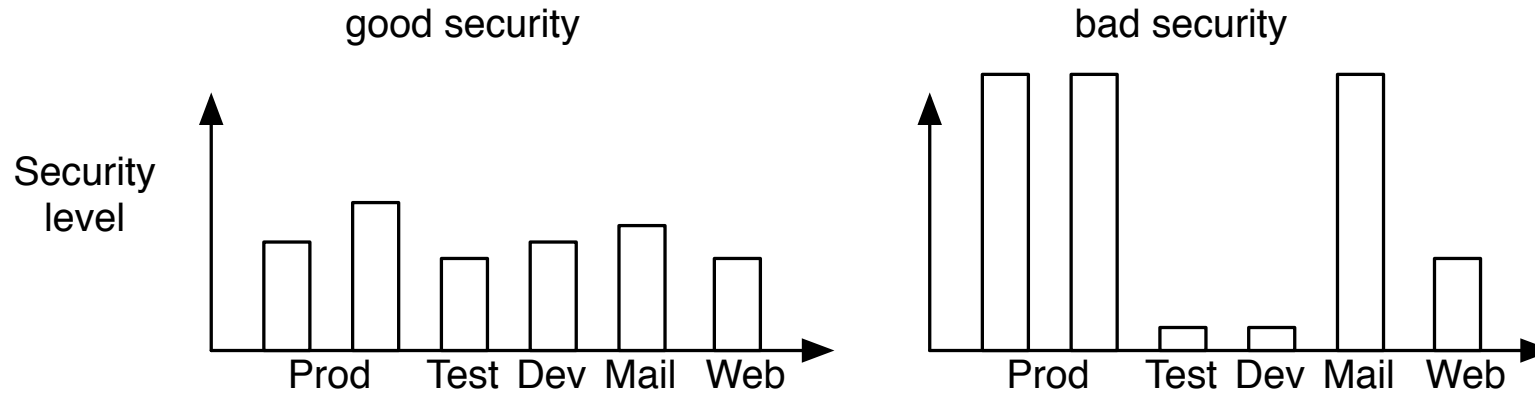
Your data is already being sold, and resold on the Internet

Stop reusing passwords, use a password safe to generate and remember

Check you own email addresses on <https://haveibeenpwned.com/>

Go ahead try the web site - hold up your hand if you are in those dumps

# Balanced security



Better to have the same level of security

If you have bad security in some part - guess where attackers will end up

Hackers are not required to take the hardest path into the network

Realize there is no such thing as 100% security

# Cost-Benefit Analysis



Benefits of computer security must be weighed against value of assets

Often more expensive to add security mechanisms to a system, than designing them in

# Risk management defined



## Information Risk Management

*Life is full of risk.*

Risk is the possibility of damage happening and the ramifications of such damage should it occur. *Information risk management (IRM)* is the *process* of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level. There is no such thing as a 100 percent secure environment. Every environment has vulnerabilities and threats to a certain degree. The skill is in identifying these threats, assessing the probability of them actually occurring and the damage they could cause, and then taking the right steps to reduce the overall level of risk in the environment to what the organization identifies as acceptable.

Source: Shon Harris *CISSP All-in-One Exam Guide*

# Quantitative Risk Assessment



In **quantitative risk assessment** an **annualized loss expectancy (ALE)** may be used to justify the **cost of implementing countermeasures to protect an asset**. This may be calculated by multiplying the single loss expectancy (SLE), which is the loss of value based on a single security incident, with the annualized rate of occurrence (ARO), which is an estimate of how often a threat would be successful in exploiting a vulnerability.

Quote from [https://en.wikipedia.org/wiki/Risk\\_assessment](https://en.wikipedia.org/wiki/Risk_assessment)

# Annualized Loss Expectancy



The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as:

$$ALE = ARO \times SLE$$

Suppose that an asset is valued at \$100,000, and the Exposure Factor (EF) for this asset is 25%. The single loss expectancy (SLE) then, is 25% \* \$100,000, or \$25,000.

The annualized loss expectancy is the product of the annual rate of occurrence (ARO) and the single loss expectancy.

For an annual rate of occurrence of one, the annualized loss expectancy is 1 \* \$25,000, or \$25,000.

For an ARO of three, the equation is:  $ALE = 3 * \$25,000$ . Therefore:  $ALE = \$75,000$

Example from:

[https://en.wikipedia.org/wiki/Annualized\\_loss\\_expectancy](https://en.wikipedia.org/wiki/Annualized_loss_expectancy)

[https://en.wikipedia.org/wiki/Single-loss\\_expectancy](https://en.wikipedia.org/wiki/Single-loss_expectancy)

# Qualitative risk analysis

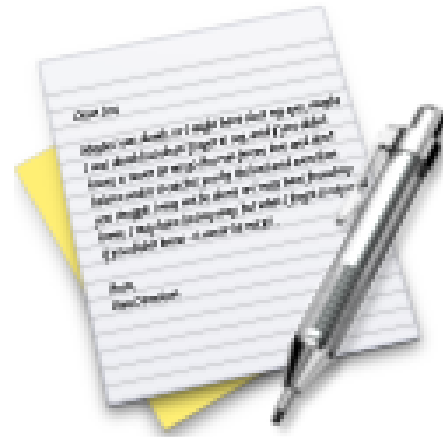


**Qualitative risk analysis** is a technique used to quantify risk associated with a particular hazard. Risk assessment is used for uncertain events that could have **many outcomes and for which there could be significant consequences**. Risk is a function of probability of an event (a particular hazard occurring) and the consequences given the event occurs. Probability refers to the likelihood that a hazard will occur. **In a qualitative assessment, probability and consequence are not numerically estimated, but are evaluated verbally using qualifiers like high likelihood, low likelihood, etc.** Qualitative assessments are good for screening level assessments when comparing/screening multiple alternatives or for when sufficient data is not available to support numerical probability or consequence estimates. Once numbers are inserted into the analysis (either by quantifying the likelihood of a hazard or quantifying the consequences) the analysis transitions to a semi-quantitative or quantitative risk assessment.

Quote from [https://en.wikipedia.org/wiki/Qualitative\\_risk\\_analysis](https://en.wikipedia.org/wiki/Qualitative_risk_analysis)



# Exercise



Now lets do the exercise

## Risk Assessment 101

which is number **5** in the exercise PDF.

# Human Issues and Organizational Problems



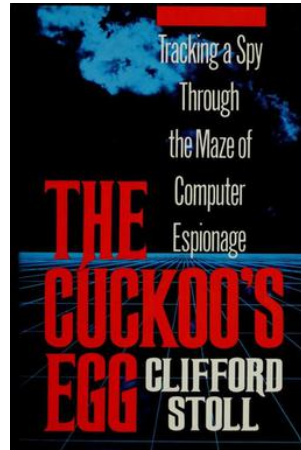
Returning to resources, it takes a lot of resources and people to secure systems:

- Time
- Money
- Skilled resources for designing, implementing, administer, monitor
- Computing resources

Often threats are focussed on outsiders, but insider threat can be common

Dont try to fix people problems with tech

# Cuckoo's Egg 1986 A real spy story



*Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage,*  
Clifford Stoll

*During his time at working for KGB, Hess is estimated to have broken into 400 U.S. military computers*

Source: [https://en.wikipedia.org/wiki/Markus\\_Hess](https://en.wikipedia.org/wiki/Markus_Hess)

# Morris Internet Worm - 30 years ago



Used multiple vulnerabilities:

- Sendmail Debug functionality, we have similar things and Google Hacking
- Buffer overflow in fingerd, we still have those
- Weak passwords/password cracking, list of 432 words and /usr/dict/words, same problem today
- Trust between systems rsh, rexec, think Domain Admin today
- Found new systems using /etc/hosts.equiv, .rhosts, .forward, netstat ...

Also known as the Morris Internet Worm

*The Internet Worm Program: An Analysis*

Purdue Technical Report CSD-TR-823, Eugene H. Spafford

Resulted in creation of the CERT, <http://www.cert.org>

# Internet Worms history repeats itself



Camouflage, tried to hide, malware today hides as well

- Program name set to 'sh', looks like a regular shell
- Used fork() to change process ID (PID)
- Worms in the 2000s spread quickly, like Code Red 2001 to approx 350.000 systems in a week
- SQL Slammer "It spread rapidly, infecting most of its 75,000 victims within ten minutes."

New malware today can use the same strategies

Except a lot of malware tries to stay hidden, less noisy

Using a small password list of 50 words it is possible to create your own botnet with 100.000s

# Access Control Matrix Model



Access Control Matrix model describes rights of subjects over all entities in a matrix

Example The Unix system read, write, execute for files, devices, processes

Everything is a file, sort of

A directory write permission allows one to rename files

Unix superuser root can access all files, processes etc.

# Trusted Computing Base



**Definition 20-6.** A *trusted computing base* (TCB) consists of all protection mechanisms within a computer system – including hardware, firmware, and software – that are responsible for enforcing a security policy

Quote from Matt Bishop, Computer Security

Keeping this small, simple and understandable help keeping systems more secure.

Example the Qubes OS depend on few security-critical components:

<https://www.qubes-os.org/doc/security-critical-code/>

# Exercise



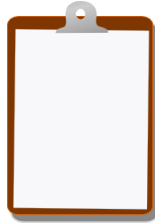
Now lets do the exercise

**Investigate /etc 10 min**

which is number **4** in the exercise PDF.



## For Next Time



Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books

Most days have less than 100 pages, but some days may have more!

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools