



Welcome to

12. Security Design

KEA Kompetence OB2 Software Security 2019

Henrik Lund Kramshøj hk@zencurity.com @kramse  

Slides are available as PDF, [kramse@Github](https://github.com/kramse)
12-security-design.tex in the repo [security-courses](https://github.com/kramse/security-courses)

Plan for today



Subjects

- How to reach the goal of secure design
- Security Principles for software
- Principle of least privilege, fail-safe defaults, separation of privilege etc.
- Files, objects, users, groups and roles
- Security by Design
- Privacy by Design
- Benchmarking standards
- CIS controls Center for Internet Security

Exercises

- How should software be designed today

Reading Summary



We will use these as a reference

Security by Design Principles

https://www.owasp.org/index.php/Security_by_Design_Principles

Selected as OWASP has existed for many years, expect site to survive

Likewise we will use the Wikipedia article about *Privacy by Design* https://en.wikipedia.org/wiki/Privacy_by_design

Other resources used today



- This in danish summarizing the implications of General Data Protection Regulation (GDPR)
<https://www.dubex.dk/aktuelt/nyheder/det-skal-du-vide-om-privacy-by-design-ny-vejledning>
- This one which recommends doing Privacy Impact Assessment (PIA)
<https://itb.dk/persondataforordningen/privacy-by-design-default/>
- ENISA, EU security office, <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design> and <https://www.enisa.europa.eu/publications/big-data-protection>

A lot of this is because of GDPR

Goals:



How to reach the goal of secure design



Security Principles for software



Principle of least privilege, fail-safe defaults, separation of privilege etc.



Files, objects, users, groups and roles



Security by Design



Privacy by Design



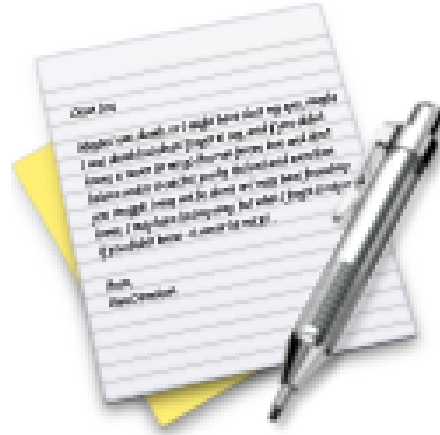
Benchmarking standards



CIS controls Center for Internet Security



Exercise

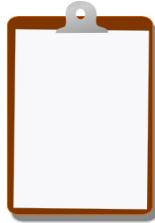


Now lets do the exercise

??

which is number ?? 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