5.

Softwareproblemer med håndtering af hukommelse

Sikker software, hvorfor?

- Usikker software
- GDPR
  - Etik
  - Ansvarlighed
- ‘Prevention is cheaper than the cure’
- NotPetya omkostninger på $1.2B

Phase	Relative cost to correct
Definition	$1
High-level Design	$2
Low-level Design	$5
Code	$10
Unit test	$15
Integration test	$22
System test	$50
Post-delivery	$100

Hvordan bliver software usikkert?

- Design fejl
  - Privelegier
  - Insecure defaults
  - Defence in depth
- Implementations fejl
  - Input validering
  - Fejlhåndtering
- Maintainence
  - Unpatched software
  - Legacy systemer
- Højkvalitetssoftware = Bedre sikkerhed

C

- C er brugt mange steder
- Agerer forskelligt for forskellige systemer
- Unspecified behaviour
  - ‘a = f(b) + g(b)’
- strcpy() vs strlcpy()
  - Inkluderer længden af strengen

Buffer overflows

- Overskrivelse af boundries
- Formål
  - Læsning af memory
  - Execution

Integer over/underflow

- Min/max på integer
- Unsigner vs signed