Persondatabeskyttelse -

Hvorfor er det så svært umuligt?

Poul-Henning Kamp

phk@FreeBSD.org

phk@Varnish.org

@bsdphk

Komplexitet

1 million forskellige stumper:

USS Ronald Reagan

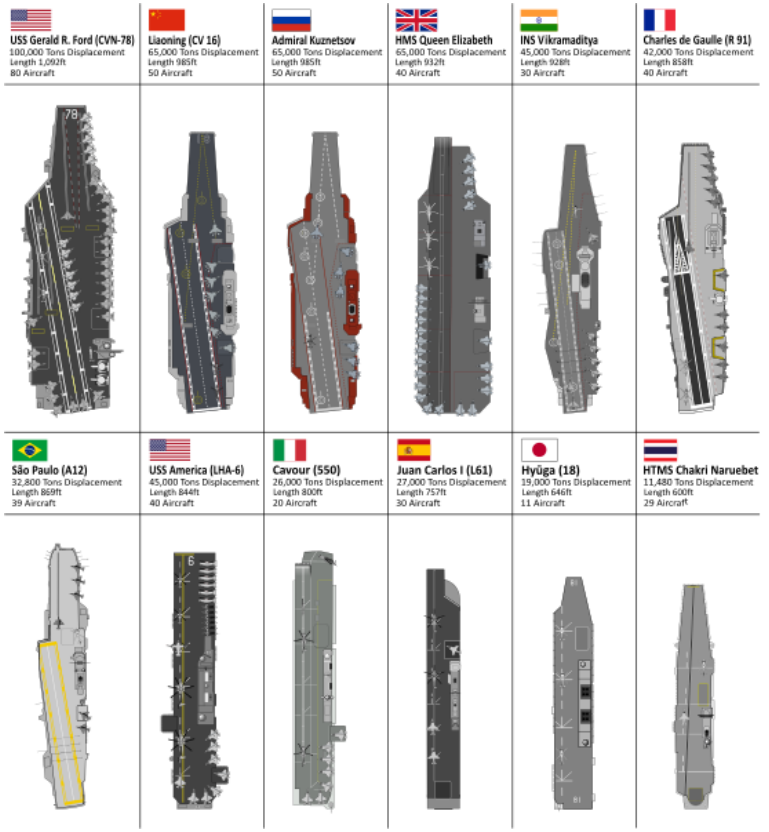
100.000 tons
300m lang
2 atomreaktorer
4 turbiner
8 forsk. radar
3.200 besætning
2.500 flybesætn.
90 fly

Komplexitet

12 mio linier kode

Billigste smartphone på markedet

12 mio stumper



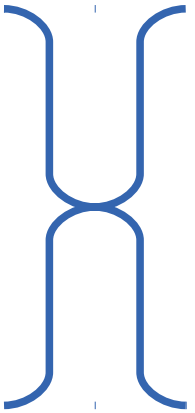
12 hangarskibe

Komplexitet og fejlrate

Program/ Projekt	Millioner kodelinier	fejl per kodelinier	Antal Fejl
Varnish	0,09	1.000	90
Apollo 11	0,15	400.000	<= 1
Space Shuttle	0,4	400.000	~ 1
OpenSSL	0,6	1.000	600
FreeBSD Kernel	1,8	1.000	1.800
F22 fighter	2	2.000.000	>= 1
F35 fighter	8 (est.)	2.000.000	> 4
Java	10	2.000	5.000
Android	12	1.000	12.000
Windows7	45	2.000	22.500
OS/X	86	2.000	43.000

”Trusted Computing Platform”

En computer
+
Et styresystem
+
En applikation



Uden fejl & tåbeligheder

Uden huller & spyware

Uden virus & malware

Stol 100% på sælgeren eller Gør Det Selv

Der findes ingen andre løsninger.

”Reflections on trusting trust”
-- Ken W. Thompson, ACM Turing award speech

”Trusted Computing Platform”

Der er en god grund til at alle superstater
har et Gør Det Selv Operativsystem Projekter:

   USA, Kina, Rusland, Indien ...

Closed source har ingen troværdighed
   = katten i sækken

Open Source er den mindst ringe troværdighed
   ... fordi vi kan kigge i sækken

NB: OSS != FOSS

”Trusted Computing Platform”

Konsum-HW: (iPad, Laptop, Mobil, PC)
   Antag at bagdøre er designet ind
   (eller at der er fejl nok at vælge imellem)

Servere:
   Iflg. NSA afsløringer:
   USA Hardware med indbyggede bagdøre.
   (”Interdiction – Implants”)
   Formodentlig kun ”high-value targets”
   Kun specialister kan detektere det

Mindst elendige bud: Hardware fra Taiwan ?

De 7 trin i teknologiudvikling

1. Det går aldrig godt!
2. Det gør ting ved køernes mælk.
3. Fantastisk!
4. Det næste bliver flyvende biler.
5. Det her slår folk ihjel!
6. Området er helt ude af kontrol!
7. Dette lovforslag bringer ...

Brand:
Bygningsreglement

Trafikuheld:
Færdselslov

Dødsfald:
Elektricitetslov

...

Jura løser ”uløselige” problemer

... ved at gøre det til nogens problem.

Nedstyrtende bygninger -> Anerkendte statikere

Elsikkerhed -> Autoriserede elinstallatører

Overdreven kapitalisme -> Produktansvar

De to undtagelser fra produktansvar:

1. Religion

2. Software

”Uanset hvad der sker, uanset hvad programmet gør, uanset hvad vi har lovet det ville gøre, er vores ansvar begrænset til at sende dig en ny CD med den præcis samme software.”

Vi skal have produktansvar på software, nu!

Persondatasikkerhed

(Og en hel del andre IT problemer)

Kan kun løses ved at gøre det til nogens problem

=> Produktansvar på software

=> Autorisationsordning for driftansvarlige

=> Tilsyn og kontrol med bid og konsekvens

=> IT-havarikommision så vi lærer af fejlene

Folketinget ved hvordan man gør det

§ 6. En tilladelse kan kaldes tilbage, såfremt:

1) væsentlige forudsætninger for tilladelsen viser sig ikke at have været til stede,

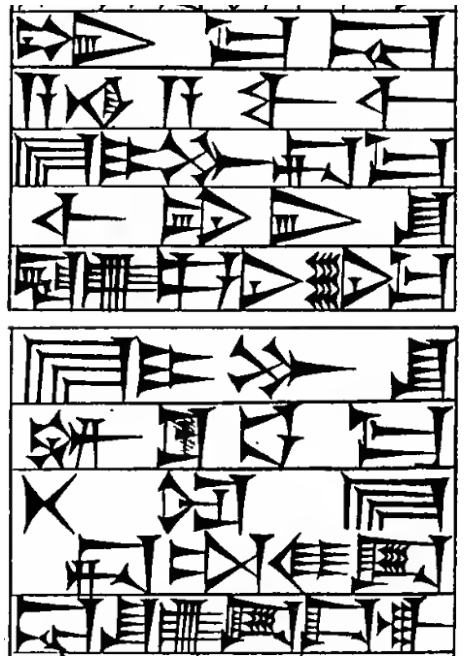
2) der sker tilsidesættelse af stillede vilkår eller

3) hensynet til sikkerheden eller anden tvingende grund i øvrigt kræver standsning eller nedlæggelse af anlægget.

§ 7. Miljøstyrelsen og sundhedsstyrelsen har adgang til at fordre sig meddelt enhver oplysning, der af disse myndigheder skønnes af betydning for sikkerheden. De kan til enhver tid uden retskendelse mod behørig legitimation fordre adgang til at udøve tilsyn på anlægget under bygning og drift eller hos leverandører til anlægget. De kan meddele pålæg, som er fornødne til at sikre overholdelsen af opstillede vilkår og betingelser, eller som i øvrigt skønnes nødvendige af sikkerhedsmæssige grunde, ligesom de i påtrængende tilfælde af sikkerhedsmæssige grunde kan forlange brugen af anlægget standset, indtil der er taget stilling til, om og i bekræftende fald hvornår brugen af anlægget kan genoptages.

Hammurabis lov ca. 1745 bc.

”If a builder build a house for a man and do not make its construction firm, and the house which he has built collapse and cause the death of the owner of the house, that builder shall be put to death.”



šum-ma bânûm
a-na a-wi-lim
bîtam i-bu-uš-ma
ši-bi-ir-šu
la u-dan-ni-in-ma
bîtum i-bu-šu
im-ku-ut-ma
be-el bîtim
^{b}uš-ta-mi-it
bânûm šu-u id-da-ak