Kursus i IT- Sikkerhed

Ivan Damgård,

Daimi, Århus Universitet

Praktiske ting

Kursushjemmeside www.daimi.au.dk/dSik

Her findes noter, links til materiale, opgaver, m.v.

Der bruges et sæt noter, der findes på hjemmesiden, derudover ganske få artikler, der bliver udleveret.

Afleveringsopgaver: 1 hver uge de første 6 uger

Eksamen: er mundtlig, eksamensspørgsmål offentliggjort på forhånd.

Øvelser:

Hold 1: Ti 14-17

Hold 2: To 11-14

Hold 3: Fre 8-11

Starter i næste uge

Hvad er IT sikkerhed?

Ingen generel, præcis definition

men nogenlunde enighed om at det handler om at nå visse generelle sikkerheds-mål:

- Konfidentialitet

- Autenticitet

- Tilgængelighed

Hvad det ikke er: f.eks. driftssikkerhed/korrekthed af programmer

OBS: nogle af de værste sikkerhedsproblemer opstår på grund af bugs i software, naturligvis relevant her – men korrekthed ville være et problem selvom alle opførte sig pænt

Konfidentialitet

Sikre at data kun kan tilgås af dem, der skal have adgang.
Gælder hvad enten data lagres, processeres eller kommunikeres.

Autenticitet

Sikre at data kun kan modificeres af dem der skal have lov.
Gælder naturligvis indholdet (kaldes ofte integritet), men også brugerens overbevisning om indholdet.

Tilgængelighed

Sikre at brugerne kan få deres data når der er brug for det.

Til et virkeligt system er det nødvendigt med mere præcise mål for den sikkerhed vi vil opnå.

Vigtigt at beskrive hvad vi vil have før vi begynder at designe en løsning.

Hertil bruges en

Sikkerhedpolitik

Indeholder en beskrivelse af hvilke mål vi har. Sagt på en anden måde: hvilke tilstande af systemet er sikre, hvilke er usikre.

Indeholder også ofte en overordnet beskrivelse af hvilke strategier vi vil bruge for at nå målene.

Eksempel:

"Vi ønsker at undgå virusangreb på maskinerne i virksomheden. Derfor skal der være installeret viruscannere på alle maskiner, og enhver der er ansvarlig for en maskine skal sikre at scanneren opdateres mindst

Angreb

Ethvert IT system er udsat for angreb, f.eks. Fra

- ærlige, men uheldige brugere

- ondskabsfulde brugere

- eksterne hackere

Vi har derfor brug for en

Angrebsmodel (Trusselsmodel)

-Beskriver hvilke angreb vi ønsker at beskytte os mod – og dermed også hvad vi *ikke* vil bekymre os om.

Afgørende vigtigt at man er bevidst om hvordan angrebsmodellen ser ud: et system kan være OK under én angrebsmodel, men totalt usikkert under en anden.

Sikkerhedsmekanismer

En fællesbetegnelse for alle de midler vi bruger for at sørge for at vores system opfører sådan som sikkerpolitikken foreskriver, under de angreb der er i angrebsmodellen.

Fysiske låse, ID kort, pasords-beskyttelse, virus scannere, kryptografi, etc., etc.

Skellet mellem sikkerhedspolitik og sikkerhedsmekanismer er lidt uklart, men generelt: overordnede strategier er en del af sikkerhedspolitikken, tekniske løsninger er sikkerhedsmekanismer.

Sikkert System =

Sikkerhedspolitik +

Trusselsmodel +

Er det sikkert?

Givet sikkerhedspolitik, angrebsmodel og de sikkerhedsmekanismer vi vil bruge, kan vi så vide at systemet vil opføre sig som sikkerhedspolitikken forlanger?

Desværre kan vi næsten aldrig være sikre!

Bevis for sikkerhed: opstille en matematisk model for systemet, og bevis en sætning der siger at systemet aldrig opfører sig på en uønsket måde. Som regel opstår et af to problemer:

- angrebsmodellen er så generel, at den omfatter (næsten) alle mulige angreb. Det er så meget svært, ofte umuligt at bevise sikkerheden

- angrebsmodellen er begrænset nok til at vi kan vise noget – man hvad så hvis systemet udsættes for noget der ikke var forudset i modellen?

Vi vil imidlertid holde kurset alligevel: at teorien er ukomplet, er

Plan for kursusindhold

Bottom-up:

- Start med teknologi og sikkerhedsmekanismer
- Derefter sikkerhedspolitikker af forskellig art
- Tilsidst en række eksempler på fejl og faldgruber

Kryptologi

- "Sikker kommunikation over usikre kanaler"
- Ikke kun hemmeligholdelse
- Kryptografi er ofte en helt nødvendig del af løsningen
- Men er aldrig hele løsningen

Kryptografiske teknikker kan deles op på to måder:

Hvilken type problem løser vi?

- Konfidentialitet eller autenticitet, de tekniske løsninger er forskellige, vigtigt at bruge den rigtige løsning til det givne problem.

Hvilken grad af sikkerhed opnår vi?

- Ubetinget sikkerhed, eller beregningsmæssig sikkerhed

Opdeling af Kryptografiske Teknikker

		Konfid.	Autent.
Ubetinget sik.			
Beregn. Sik.	Secret-Key alg.		
	Public-Key alg.		