Trustworthy computing, hva har det med tillit å gjøre?

Tom Lysemose

Oslo, 20 September, 2006

Innhold

- Definisjon av tillit
- Aspekter ved tillit
- Trustworthy Computing – Trust in Cyberspace
- Trustworthy Computing – Microsoft

Hva er tillit?

- En tillitsrelasjon består av:
  - En der *har* tillit (tillitsgiver)
  - En der *får* tillit (tillitsmottaker)
- Definisjon av tillit:
  - Tillit er den *subjektive sannsynlighet* med hvilken en agent (tillitsgiveren), forventer at en annen entitet (tillitsmottakeren) utfører en gitt handling, som agentens velferd avhenger av.
- Definisjon av tillitsverdighet:
  - Tillitsverdighet er den *objektive sannsynlighet* for at en entitet (tillitsmottakeren) utfører en gitt handling, som velferden til en bestemt agent (tillitsgiveren) avhenger av.

Sentrale aspekter ved tillit

- Tillit er ikke det samme som ’tro’
- Tillit har alltid et element av risiko eller mulighet
- Avhengighetsrelasjoner, hvor utfallet bestemmes av ren tilfeldighet, er ikke tillit
- Tillitsrelasjoner har ofte et normativt element
- Kjennskap til motpartens målsetninger er ofte viktig i tillitsrelasjoner

Representasjon av tillit

- Kvalitativ:
  - F.eks. høj, medium, lav...
- Kvantitativ:
  - F.eks. 80%...
- Raffinering av mål for tillitsnivå:
  - Ved innførelse av mål konfidens

Committee on Information Systems Trustworthiness

Trust in Cyberspace

Trust in Cyberspace (I)

- Et tillitsverdig nettverkstilkoplet informasjonssystem (NIS) er kjennetegnet ved:
  - At det gjør hva det forventes (og ikke noe annet) på tross av sammenbrud i omgivelsene, feil av bruker/operatør eller angrep fra ondsinnete personer.
- Design og implementasjonsfeil bør unngås, elimineres eller kanskje tolereres.

Trust in Cyberspace (II)

- Essensielle egenskaper (overlappende kategorier):
  - Korrekthet (Correctness)
  - Funksjonskorrekthet (korrekthet over tid) (Reliability)
  - Sikkerhet (Security)
  - Personvern (Privacy)
  - Trygghet (Safety)
  - Robusthet (Survivability)
- Tillitsverdighet er multidimensjonal og oppnås ikke ved bare å oppfylle noen av kravene.

Observasjoner og anbefalinger

- Tillitsverdighet er et bredere begrep en det tradisjonel sikkerhets begrep. Det involverer:
  - Lindring av risiko istedenfor fjernelse av risiko
  - Hemme angrep istedenfor fullstendig sikring mot angrep
  - Omplassere sårbarheter istedenfor at eliminere dem
- Et systems reaksjon på angrep kunne være kontrollert og elegant reduksjon av funksjonalitet.
- Ved å bruke monitorering og deteksjons-funksjonalitet, kan man oppnå tillitsverdige systemer der består av ikke-tillitsverdige komponenter.

Trust in Cyberspace – tillitsverdighet?

- Har et abstrakt og sammensatt begrep om tillitsverdighet. Dette gir en subjektiv vinkling av tillitsverdighet.
- Er rettet mot å sikre tillitsverdighet. Kommunikasjon av tillitsverdigheten for å sikre korrekt tillitsvurderinger har liten fokus.
- De normative elementer får ikke mye oppmerksomhet.

Microsoft
Trustworthy Computing

Trustworthy Computing – Microsoft (I)

- Anekdoter antyder at det bl.a. angrepet fra Code Red ormen (buffer overflow), som var årsak til initiativet...

- Hovedaspekter:
  - Sikkerhet (security)
  - Privatlivets fred (privacy)
  - Pålitelighet (reliability)
  - Forretnings helhet (Business Integrity)

Trustworthy Computing – Microsoft (II)

- Sikkerhet:
  - Evne til å beskytte mot angrep. Viktigste aspekter er konfidentialitet, integritet og tilgjengelighet.
- Privatlivets fred/personvern:
  - Sikre kontroll over individets personlige informasjon, også i komplekse situasjoner
- Pålitelighet:
  - Om systemet fortsetter å fungere i sub-optimale situasjoner
- Forretnings helhet:
  - Ansvarlig og responderende
  - Åpenhet

MS Trustworthy Computing – tillitsverdighet?

- Ja, hvis det lykkes....
- Men det er ikke let å skifte kurs med et stort komplekst system...
- Bakover kompatibilitet kan motvirke tillitsverdigheten
- Feil i tredjeparts komponenter kan skade tillitsverdigheten