Introduktion till informationssäkerhet

Daniel Bosk

Avdelningen för informations- och kommunikationssytem (IKS),
Mittuniversitetet, Sundsvall.

intro.tex 1586 2014-01-27 14:21:59Z danbos

Mittuniversitetet
MID SWEDEN UNIVERSITY

Översikt

1. Formalia
   - Schema
   - Lärplattform
   - Examination
2. Vad är informationssäkerhet?
   - Översikt
   - Definitioner
   - Kursens innehåll

Litteratur

Föreläsningen ger en introduktion till kursen och informationssäkerhetsområdet. Den täcker ytligt kapitel 1 ”What is security engineering?” i [And08].

Översikt

Schema

- Schemat ska finnas tillgängligt sedan i början av veckan.

Lärplattform

- Kursen ges med Moodle.
- Allt material är publicerat.

Examination

Kursen examineras med

- en laboration,
- två PM,
- två seminarier, samt
- ett projekt.

Examination

- PM1 LIS
- PM2 Verksamhets- och riskanalys
- S3 Verksamshets- och riskanalys
- L4 Lösenordsknäckning och APT
- S5 Lösenordspolicyer och andra säkerhetsaspekter
- Projekt

Översikt

Vad är infosäk?

- Interdisciplinärt område: bl.a. kryptografi, psykologi, ekonomi.
- Mål: saker ska fungera som det är tänkt!

Vad är infosäk?

Policy	Vad som är tänkt att åstadkommas.
Mekanismer	Hur vi åstadkommer detta: ex. kryptografi, åtkomstkontroll.
Tillförlitlighet	Hur mycket vi kan lita på respektive mekanism.
Incitament	Hur vi får stöd för säkerheten hos människor.

Alla dessa interagerar!

Definitioner

System	Allt från komponent, smartcard, kryptomekanism till helt system med användare.
Subjekt	En fysisk person, ex. Adam.
Person	En juridisk person.
Principal	En del som deltar i ett säkerhetssystem. Kan vara subjekt, person, roll, del av utrustning (smartcard) eller sammansättning av andra principals.
Grupp	En uppsättning principals.
Roll	En uppsättning funktioner som antas av olika personer: jourhavande läkare, kursansvarig.

Definitioner

Tillit (*trust*) Ett system man har tillit för kan bryta min säkerhetspolicy vid fel.

Pålitlighet (*trustworthy*) En pålitlig komponent kommer inte att falera.

Definitioner

Sekretess Teknisk term för effekten av en mekanism som begränsar antalet principals som kan komma åt information.

Konfidentialitet Skyldighet att skydda någon annans sekretessbelagda information.

Privacy Möjligheten (och rätten?) att skydda sin personliga information.

Definitioner

Riktighet (*integrity*)	Att något är oförändrat, i sitt ursprungliga skick.
Autenticitet	Integritet tillsammans med färskhet.

Definitioner

Säkerhetstillbud Inträffar när ett system bryter säkerhetspolicyn.

Sårbarhet Kan tillsammans med ett *hot* ge upphov till ett säkerhetsmisslyckande.

Säkerhetsmål Mer detaljerad specifikation av hur säkerhetspolicyn ska implementeras.

Skyddsprofil Likt säkerhetsmål, men ska vara systemoberoende för att kunna jämföras.

Kursens innehåll

- Studiehandledning
- Lydelser:
  - PM1
  - PM2
  - S3
  - L4
  - S5
  - Projekt

Referenser I

[And08] Ross J. Anderson. *Security engineering : a guide to building dependable distributed systems*. Wiley, Indianapolis, IN, 2 utgåvan, 2008.