Introduktion till informationssäkerhet

Daniel Bosk

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

infosak.tex 1723 2014-04-04 07:45:55Z danbos

Mittuniversitetet
MID SWEDEN UNIVERSITY

Översikt

Litteratur

To introduce you to the area of security, you should first read Chapter 1 in *Security Engineering* [And08] and then read Chapters 1 and 2 in *Computer Security* [Gol11]. These chapters cover the history of the security field and an introduction to what it is all about.
After reading this material you are recommended to do exercises 1.2, 1.3 and 1.7 in [Gol11].

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

Säkerhetsincident 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.

Översikt

Se lärplattformen!

Referenser I

[And08] Ross J. Anderson. *Security Engineering*. Wiley, Indianapolis, IN, 2 utgåvan, 2008.

[Gol11] Dieter Gollmann. *Computer Security*. Wiley, Chichester, West Sussex, U.K., 3 utgåvan, 2011.