Introduktion till nätverkssäkerhet

Daniel Bosk

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

intro.tex 1939 2014-09-01 14:06:04Z danbos

Mittuniversitetet
MID SWEDEN UNIVERSITY

Översikt

1. Formalia
   - Schema
   - Lärplattform
   - Examination
2. Introduktion
   - Vad är nätverkssäkerhet?
   - Definitioner

Litteratur

The lecture introduces the material of the course and the area of network security. It provides an overview of chapter 1 “Introduction” in *Network security essentials : applications and standards* [Sta13] and certain contents from chapter 1 “What is security engineering?” in *Security Engineering* [And08].

Översikt

Schema

Lärplattform

Examination

Översikt

Vad är nätverkssäkerhet?

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

Säkerhetsmisslyckande 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.

Referenser I

Ross J. Anderson. *Security Engineering. A guide to building dependable distributed systems*. 2. utg. Indianapolis, IN: Wiley, 2008. ISBN: 978-0-470-06852-6 (hbk.) URL: http://www.cl.cam.ac.uk/~rja14/book.html.

William Stallings. *Network security essentials : applications and standards*. 5. utg. International Edition. Pearson Education, 2013. ISBN: 978-0-273-79336-6.

Mittuniversitetet
MID SWEDEN UNIVERSITY