Introduction to Web Application Security

Daniel Bosk

Department of Information and Communication Systems (ICS),
Mid Sweden University, Sundsvall.

intro.tex 1287 2013-09-10 19:44:49Z danbos

Översikt

Litteratur

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

Översikt

Se studiehandledningen. (Uppdaterad!)

Se projektlydelsen. (Uppdaterad!)

Examination

Kursen examineras med

- skriftlig rapport för ett projekt,
- muntlig presentation av samma projekt,
- skriftlig rapport för granskning av annans projekt, och
- muntlig presentation i av granskning i form av opponering.

Schema

- Alla möten (föreläsningar, presentationer, etc.) finns i centrala schemat.
- URL: `https://portal.miun.se/web/student/schedule`.

Lärplattform

- Kursen ges med Lärplattform 2.0.
- Allt material är publicerat.
- Det kommer dock ges fler referenser för föreläsningarna allteftersom de ges.

Lärplattform

Se lärplattformen.

Översikt

- Se [Pro13].
- Föreläsningarna utgår från denna.

- Se [owa05].
- Läses parallellt med föreläsningarna.
- Välstrukturerat dokument, enkelt att läsa.
- Innehållet och eventuella svåra passager diskuteras under handledningstillfällena – läs inför dem!

- Se [owa08].
- Läses parallellt med föreläsningarna.
- Välstrukturerat dokument, enkelt att läsa.
- Innehållet och eventuella svåra passager diskuteras under handledningstillfällena – läs inför dem!

Översikt

Vad är säkerhet?

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

Vad är säkerhet?

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!

Översikt

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.

Pålitlig (*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.

Referenser I

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

[owa05] A guide to building secure web applications and web services, 2005.

[owa08] Owasp testing guide, 2008.

[Pro13] The Open Web Application Security Project. OWASP Top 10 - 2013: The Ten Most Critical Web Application Security Risks, Jun 2013.