Dipartimento di Matematica

ROMA TRE UNIVERSITÀ DEGLI STUDI

Presentazione di IN05: Tecniche di sicurezza dei dati e delle reti

Roberto Di Pietro

dipietro@mat.uniroma3.it

Obiettivi

Fornire le basi per poter trattare la sicurezza dei dati delle reti con strumenti metodologici e tecnici adeguati.

Overview del corso

Il corso parte con l'introduzione dei concetti di base che attengono il networking (LAN), ed introduce successivamente i fondamenti dell'architettura di Internet.

Segue una parte più tecnica (prediligendo il punto di vista applicativo) relativa agli algoritmi crittografici a chiave segreta e chiave asimmetrica.

.....

Overview

Si introducono poi quelli che sono i principi relativi alla progettazione di algoritmi per la crittografia, ed infine si trattano le tecniche per l'autenticazione.

Il corso termina affrontando poi tecniche per la sicurezza delle reti: firewall ed IDS (sistemi per il rilevamento delle intrusioni).

In Dettaglio:

- Fondamenti di networking.
- Fondamenti su architettura di Internet.
- Crittografia classica

In Dettaglio:

- Crittografia a chiave simmetrica:
  - Cifrari a blocchi e cifrari a flusso;
  - Algoritmi rappresentativi: Feistel, DES, 3-DES, AES;
  - Modalità implementative dei cifrari.

In Dettaglio:

- Funzioni Hash e Message Digest.
- Crittografia a chiave Asimmetrica:
  - richiami su Diffie-Hellman ed RSA;
  - Firme digitali standard;
  - firme digitali camaleontiche.
- Principii di progettazione per la sicurezza.

In Dettaglio:

- Tecniche di Autenticazione.
- Tecnologie per la Sicurezza:
  - Firewalls;
  - Intrusion Detection Systems (IDS).

Materiale di riferimento

- Risorse on-line
  - Handbook of **Applied Cryptography** (A.J. Menezes et al.)
- LIBRI
  - **Network Security Essentials (W. Stalling)**
  - **Data and Computer Communications "**
  - **Applied cryptography: Protocols… (B. Schneier)**

Materiale di riferimento

- .....Tutto ciò che ritenete criticamente utile;
- Sempre disponibile a confrontare le risorse da voi individuate

Esame

- Scritto, a domande aperte.
- Orale (facoltativo, o a chiamata).

- Progetti:
  - Alla persona, ma cmq. non + di 2 progetti da max 2 persone ciascuno.
- Ricevimento: su appuntamento