Sicurezza nelle reti di telecomunicazioni

Finalità
Il corso ha come obiettivo quello di analizzare i principali meccanismi e protocolli utilizzati nell'ambito della sicurezza nelle reti di telecomunicazioni. In particolare vengono presentati i concetti base della crittografia, i protocolli di autenticazione e comunicazione sicura, le principali minacce e le possibili soluzioni per realizzare architetture di rete sicure.

Programma
1) Introduzione alla crittografia
Crittografia simmetrica e crittografia asimmetrica (RSA, Diffie-Hellman)
Funzioni Hash e Message Digest
La firma digitale, i certificati digitali, le autorità di certificazione, lo standard X.509/PKI (Public Key Infrastructure) e PGP (Pretty Good Privacy)

2) Protocolli per la sicurezza
Protocolli di autenticazione (CHAP, EAP, RADIUS, Diameter)
Protocolli di comunicazione sicura a livello IP (IPSec), a livello di trasporto e applicativo (TLS, SSH)
Reti private virtuali
Sicurezza in ambiente mobile IEEE 802.11

3) Vulnerabilità dei protocolli TCP/IP e applicativi
Tipologie di attacchi e possibili contromisure (sniffing, network e port scanning, IP spoofing, flooding, buffer overflow, etc)

4) Meccanismi di protezione
Firewalls (packet filtering, application level gateways, proxy, NAT, bastion host, DMZ) ed esempi di rete
Intrusion Detection Systems (IDS)

Attività d'esercitazione
Esercitazioni sugli argomenti trattati e approfondimenti.

Modalità d'esame
Sono necessarie le conoscenze di base sulle architetture di comunicazione e i protocolli TCP/IP.
E' consigliato aver seguito uno dei seguenti corsi: Reti di Telecomunicazioni A, Telematica A, oppure Reti di Calcolatori A.

Testi consigliati
[1] W. Stallings, "Cryptography and Network Security: Principles and Practice" 3th Edition, Prentice Hall
[2] C. Kaufman, R. Perlman, M. Speciner, "Network Security: Private Communication in a Public World" 2nd Edition, Prentice Hall