UNIVERSITÀ DI PISA

COMMUNICATION SYSTEMS AND CYBERSECURITY

MICHELE PAGANO

Anno accademico	2021/22
CdS	INGEGNERIA DELLE TELECOMUNICAZIONI
Codice	1014I
CFU	12

Moduli	Settore/i	Tipo	Ore	Docente/i
COMMUNICATION SYSTEMS	ING-INF/03	LEZIONI	60	GIACOMO BACCI MARCO LUISE
CYBERSECURITY	ING-INF/03	LEZIONI	60	MICHELE PAGANO

Obiettivi di apprendimento

Conoscenze
Al termine dell'esame, nel modulo CyberSecurity lo studente avrà acquisito una conoscenza dettagliata dei fondamenti matematici della crittografia e dei principali algoritmi che sono utilizzati per fornire i vari servizi di sicurezza (autenticazione, confidenzialità e integrità dei dati, firma digitale). Inoltre lo studente acquisirà alcune conoscenze più applicative, con particolare riferimento a IPsec, IDS e firewall.
Nel modulo Communication Systems, lo studente avrà acquisito una conoscenza dettagliata dei fondamenti dei sistemi di comunicazione a largo spettro, comprendendo sia i sistemi di comunicazione mobile (con enfasi sugli standard 3G, 4G e 5G), sia quelli cablati (con enfasi sulle reti di accesso e trasporto in fibra ottica).

Modalità di verifica delle conoscenze
Durante l'esame finale lo studente deve essere in grado di dimostrare il livello di conoscenza e di comprensione del materiale del corso, spiegando il funzionamento di alcuni dei protocolli e algoritmi studiati durante il corso.
Metodo di verifica: Esame finale (orale)

Capacità
Al termine del corso, lo studente sarà in grado di comprendere:

- il funzionamento dei principali meccanismi per la sicurezza di rete e il livello di sicurezza di applicazioni, protocolli e sistemi di rete;
- i concetti fondamentali alla base dei principali sistemi di comunicazione e le caratteristiche principali degli standard wireless e cablati.

Modalità di verifica delle capacità
Durante le lezioni la discussione con gli studenti in relazione al funzionamento degli algoritmi e dei protocolli presentati permetterà di verificare il loro livello di comprensione. Inoltre, la parte finale del corso relativa all'applicazione degli algoritmi studiati permetterà di valutare il livello di comprensione dei concetti di base.

Comportamenti
Lo studente sarà in grado di comprendere l'uso delle principali primitive di sicurezza in sistemi reali. Più in dettaglio, nel modulo CyberSecurity acquisterà familiarità con i seguenti concetti:

- algoritmi di cifratura
- chiavi pubbliche e segrete
- codici MAC e funzioni hash
- firma digitali
- protocolli per lo scambio delle chiavi

Nel modulo Communication Systems, lo studente acquisterà familiarità con i seguenti concetti:

- tecniche di multiplexing e multiple access

- concetti fondamentali alla base di una rete cellulare
- dettagli degli standard 3G e 4G, e cenni alle tecnologie 5G
- reti di trasporto e di accesso basate su fibra ottica
- sistemi di broadcasting satellitari e terrestri

Modalità di verifica dei comportamenti
Le discussioni durante le lezioni e l'esame finale permetteranno di verificare il livello di comprensione da parte degli studenti.

Prerequisiti (conoscenze iniziali)

- Conoscenze di base dello stack protocollare TCP/IP
- Conoscende di base di comunicazioni digitali

Indicazioni metodologiche
Modalità di svolgimento delle lezioni: lezioni frontali, con ausilio di slide (modulo CyberSecurity: in Italiano; modulo Communication Systems: in Inglese)
Modalità di apprendimento:

- partecipazione alle lezioni
- studio individuale

Presenza alle lezioni: Consigliata
Metodi di insegnamento:

- Lezioni frontali con il supporto di slide
- Discussione con gli studenti

Forme aggiuntive di interazione con gli studenti:

- ore di ricevimento per spiegazioni aggiuntive e approfondimenti
- e-mail nel caso di semplici dubbi da parte dello studente
- sito moodle per comunicazioni relative a eventuali cambi nell'orario delle lezioni

Programma (contenuti dell'insegnamento)
Module: CyberSecurity

- Panoramica sulla terminologia
- Basi matematiche
  - Aritmetica modulare e polinomiale
  - Generazione di numeri casuali
  - Numeri primi e relativi teoremi
  - Logaritmo discreto
- Cifratori simmetrici
  - Tecniche classiche di cifratura
  - DES e varianti
  - AES
  - RC
  - Confidenzialità dei dati e distribuzione delle chiavi di sessione
- Crittografia a chiave pubblica
  - RSA
  - Gestione delle chiavi pubbliche e segrete
- Autenticazione e integrità
  - codici MAC e funzioni hash
  - HMAC
  - Firma digitale
- Sicurezza in sistemi di rete
  - Panoramica sulla sicurezza in ambito Web (SSL/TLS e SET) e a livello IP (IPSec)
  - Problematiche di sicurezza in reti wireless IEEE 802.11
- Sicurezza di sistema
  - intruder e sistemi di rivelazione degli attacchi (IDS)
  - firewall: principi generali, architettura e configurazione

Modulo: Commucation Systems:

- Tecniche di multiplexing e accesso multiplo:
  - Frequency division multiplexing (FDM)
  - Time division multiplexing (TDM)

- Code division multiplexing (CDM)
- Frequency division multiple access (FDMA)
- Time division multiple access (TDMA)
- Code division multiple access (CDMA)
- Packet-based multiple access
- Confronto tra le varie tecniche in termini di efficienza spettrale

- Concetti base dei sistemi di comunicazione wireless (da dettagliare)
- Principali standard di sistemi cellulari (da dettagliare)
- Tecnologie basate su fibra ottica (da dettagliare)
- Tecnologie di broadcasting terrestre e satellitare (da dettagliare)

Bibliografia e materiale didattico

- Appunti delle lezioni, resi disponibili prima delle lezioni stesse (modulo CyberSecurity: in Italiano; modulo Communication Systems: in Inglese)
- Bibliografia (in inglese):
  - William Stallings, "Cryptography and Network Security: Principles and Practice", Prentice Hall
  - Wade Trappe and Lawrence C. Washington, "Introduction to Cryptography with Coding Theory", Prentice Hall
  - T.S. Rappaport, *Wireless Communications: Principles and Practice,* 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 2002.
  - J.G. Proakis and M. Salehi, *Digital Communications,* 5th ed. New York, NY: McGraw-Hill, 2007.
  - A.F. Molisch, *Wireless Communications*. West Sussex, UK: J. Wiley & Sons, 2005.
  - M. Luise, *Lezioni di comunicazioni digitali*. Pisa, Italy, Oct. 2021. [Online] http://www.iet.unipi.it/m.luise/LCD_Luise_draft.pdf (in Italiano)

Indicazioni per non frequentanti

La presenza alle lezioni è solo consigliata; gli studenti non frequentanti possono studiare il materiale del corso in maniera indipendente ed eventualmente contattare il docente per chiarimenti. Eventuali studenti stranieri (il corso è in italiano) possono fare riferimento ai riferimenti bibliografici indicati precedentemente.

Modalità d'esame

L'esame consiste in una discussione su alcuni degli argomenti trattati durante il corso (vedi Programma), per verificare il livello di comprensione dello studente e la sua capacità di padroneggiare i principali concetti discussi durante il corso.

Ultimo aggiornamento 10/03/2022 09:50