UNIVERSITÀ DI PISA

COMMUNICATION SYSTEMS AND CYBERSECURITY

RUGGERO REGGIANNINI

Anno accademico	2020/21
CdS	INGEGNERIA DELLE TELECOMUNICAZIONI
Codice	1014I
CFU	12

Moduli	Settore/i	Tipo	Ore	Docente/i
COMMUNICATION SYSTEMS	ING-INF/03	LEZIONI	60	RUGGERO REGGIANNINI
CYBERSECURITY	ING-INF/03	LEZIONI	60	MICHELE PAGANO

Obiettivi di apprendimento

Conoscenze
Al termine dell'esame 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.

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)
- Semplice esercizio sulle basi matematiche della crittografia

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.

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, acquisterà famigliarità con i seguenti concetti:

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

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

Indicazioni metodologiche

Modalità di svolgimento delle lezioni: lezioni frontali, con ausilio di slide (in Italiano)
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)

- 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

Bibliografia e materiale didattico

- Appunti delle lezioni, resi disponibili prima delle lezioni stesse (in italiano)
- 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

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 un semplice esercizio sulle basi matematiche della crittografia e della prova orale, che prevede una paio di domande su diverse parti del programma (vedi Programma). La soluzione corretta dell'esercizio e una conoscenza di base dei diversi argomenti è necessaria per superare l'esame; la valutazione finale dipenderà dal livello di comprensione e di approfondimento dimostrato dallo studente durante l'esame.

UNIVERSITÀ DI PISA

Ultimo aggiornamento 28/07/2020 14:30