Testi del Syllabus

Docente	**VELTRI LUCA**	Matricola:	**006125**

Anno offerta:	**2013/2014**
Insegnamento:	**1005252 - NETWORK SECURITY + LABORATORY**
Corso di studio:	**5052 - COMMUNICATION ENGINEERING - INGEGNERIA DELLE TELECOMUNICAZIONI**
Anno regolamento:	**2013**
CFU:	
Tipo attività:	**-**
Partizione studenti:	**-**
Anno corso:	**1**
Periodo:	**Secondo Semestre**
Sede:	**SEDE DIDATTICA DI PARMA**

Testi in italiano

Tipo testo	*Testo*
Lingua insegnamento	Inglese
Contenuti	Basi di crittografia e principali algoritmi crittografici; Meccanismi di autenticazione e firma digitale; Protocolli per comunicazioni sicure; Principali minacce e vulnerabilità dei sistemi in rete e possibili contromisure; Sistemi per la protezione delle reti; Attività di laboratorio su crittografia, vulnerabilità in rete e protezione delle reti.
Testi di riferimento	[1] L. Veltri, "Network Security", lucidi del corso, http://www.tlc.unipr.it/veltri [2] W. Stallings, "Cryptography and Network Security: Principles and Practice" 5th Edition, Prentice Hall
Obiettivi formativi	L'obiettivo del corso è fornire allo studente le conoscenze principali meccanismi e protocolli utilizzati nell'ambito della sicurezza nelle reti; in particolare si vuole fornire una conoscenze di base della crittografia applicata, e approfondire i seguenti argomenti: - principali algoritmi e protocolli di autenticazione; - principali protcolli per comunicazioni sicure; - possibili vunerabilità in rete e principali meccanismi di protezione. Le capacità di applicare le conoscenze e comprensione elencate risultano essere in particolare: - analizzare schemi di autenticazione e di protezione dei dati basati su crittografia simmetrica e/o asimmetrica; - progettare meccanismi di autenticazione e di scambio di dati sicuri; - configurare e utilizzare protocolli e algoritmi standard per la sicurezza (ad esempio protcolli IPSec e TLS; algoritmi di crittografia AES, DES, 3DES, RSA; firma digitale e certificati digitali X.509 e PGP; etc.); - utilizzo di strumenti per il monitoraggio di una rete e scansione delle possibili vulnerabilità; - configurazione di sistemi di protezione dei nodi di una rete (firewall).
Prerequisiti	Conoscenze di base sulle architetture di comunicazione e i protocolli TCP/IP.
Metodi didattici	Lezioni in aula (36h), esercitazioni in aula (6h) svolte dal docente con gli studenti, attività di laboratorio (21h).
Modalità di verifica dell'apprendimento	I risultati di apprendimento da parte dello studente sono verificati attraverso un esame scritto. Questo esame può essere superato in due modalità diverse: 1) suddiviso in due prove di verifica in itinere scritte, rispettivamente a metà e a fine del corso; tali prove, se superate, completano l'esame; oppure 2) sostenuto tramite prova scritta durante i regolari appelli di esame. In entrambi i casi la prova scritta è composta da quesiti a risposta chiusa, quesiti a risposta aperta, e esercizi da risolvere. Durante il corso verranno mostrati e risolti esempi di esercizi di esame.

Tipo testo	*Testo*
Programma esteso	1) Basi di crittografia e meccanismi di autenticazione - Basi della crittografia simmetrica (classica) ed esempi di algoritmi (DES, 3DES, AES) - Basi della crittografia asimmetrica ed esempi di algoritmi (RSA, Diffie-Hellman, DSA); vantaggi e svantaggi - Funzioni Hash e MAC (MD5, SHA, HMAC) - Algoritmi di autenticazione basati su crittografia simmetrica o asimmetrica - Scambio di chiavi tramite Key Distribution Center (KDC) - Firma digitale, certificati digitali, autorità di certificazione, standard X.509/PKI (Public Key Infrastructure) e PGP (Pretty Good Privacy) 2) Protocolli per la sicurezza - Protocolli di autenticazione e scambio di chiavi (Kerberos, AAA, RADIUS) - Protocolli di comunicazione sicura a livello IP (IPSec/AH/ESP) e reti private virtuali (VPN) - Protocolli di comunicazione sicura a livello di trasporto (SSL/TLS) e applicativo (SSH) 3) Vulnerabilità e protezione delle reti - Vulnerabilità dei protocolli TCP/IP, tipologie di attacchi e possibili contromisure (sniffing, network e port scanning, spoofing, flooding, buffer overflow, etc.) - Firewall (packet filtering, ALG, NAT, DMZ) ed esempi di configurazioni rete - Protocolli per attraversamento di FW e NAT (STUN e TURN) - Intrusion Detection System (IDS) - Reti di anonimizzazione 4) Attività di laboratorio - Certificati digitali X.509, CA, applicazioni (e.g. HTTPS), PGP - IPSec, TLS - Protocol analyzer, Network scanning, Vulnerability test - Firewall (Linux netfilter)

Testi in inglese

Tipo testo	*Testo*
Lingua insegnamento	English
Contenuti	Cryptography basics and algorithms; Authentication mechanisms and digital signature; Protocols for secure communications; Main network threats, vulnerabilities, and countermeasures; Systems for network protections; Laboratory activities on cryptography, network vulnerabilities and network protection.
Testi di riferimento	[1] L. Veltri, "Network Security", slides of the course, http://www.tlc.unipr.it/veltri [2] W. Stallings, "Cryptography and Network Security: Principles and Practice", Prentice Hall
Obiettivi formativi	The course aims to provide the student with the knowledge of the main security mechanisms and protocols used for securing communications and for protecting computer networks; in particular the knowledge and understanding of: - applied cryptography; - main algorithms and protocols for authentication and for securing data exchanges; - main communication security protocols; - possible network vulnerabilities and main network protection mechanisms. Applying knowledge and understanding are: - analysis of authentication and data protection schemes based on symmetric and/or asymmetric cryptography; - design of mechanisms for authentication and secure data exchange; - configuration and use of standard security protocols and algorithms (e.g. IPSec and TLS protocols; AES, DES, 3DES, RSA cryptography algorithms; digital signature and certificates X.509 and PGP; etc.) - use of tools for network monitoring and vulnerabilities scanning; - configuration of systems (e.g. firewalls) for network protection.
Prerequisiti	Familiarity with TCP/IP stack and networking.
Metodi didattici	Class lessons (36h), and in class exercises (6h) carried out by the teacher with students, laboratoy acitvities (21h).
Modalità di verifica dell'apprendimento	The exam can be succeeded as: 1) divided into two written examinations, at the middle and the end of the course, that complete the exam; or 2) written exam, during regular scheduled examinations. In both cases, the exam is written and composed of multiple choice questions, open answer questions, and some exercises. Examples of exercises are shown and solved during the course.
Programma esteso	1) Basics of cryptography and authentication mechanisms - Basics of symmetric (classic) cryptography and examples of algorithms (DES, 3DES, AES) - Basics of asymmetric cryptography and examples of algorithms(RSA, Diffie-Hellman, DSA); advantages and disadvantages

Tipo testo	*Testo*
	- Hash and MAC functions (MD5, SHA, HMAC) - Authentication algorithms, based on both symmetric and asymmetric cryptography - Key exchange, agreement, and distribution - Digital signature, digital certificates, certification authority, Public Key Infrastructure, standard X.509, PGP (Pretty Good Privacy) 2) Security protocols - Protocols for authentication and key exchange (Kerberos, AAA, RADIUS) - Protocols for secure communications at IP layer (IPSec/AH/ESP), and virtual private networks (VPNs) - Protocols for secure communications at transport (SSL/TLS) and application layer 3) Network vulnerabilities and countermeasures - Vulnerabilities of TCP/IP protocols, attacks and countermeasures (sniffing, network and port scanning, spoofing, flooding, buffer overflow, etc.) - Firewall (packet filtering, ALG, NAT, DMZ), examples of network configurations - Protocols for FW and NAT traversal (STUN e TURN) - Intrusion Detection System (IDS) - Anonymity networks 4) Laboratory activity - Creation and use of digital certificates (X.509), CA, applications, PGP - IPSec, TLS - Protocol analyzer, Network scanning, Vulnerability test - Firewall (Linux netfilter)