

# Testi del Syllabus

Resp. Did.	<b>VELTRI LUCA</b>	<b>Matricola: 006125</b>
Docente	<b>VELTRI LUCA, 6 CFU</b>	
Anno offerta:	<b>2016/2017</b>	
Insegnamento:	<b>1005260 - NETWORK SECURITY + LABORATORY (UNIT 1)</b>	
Corso di studio:	<b>5052 - COMMUNICATION ENGINEERING - INGEGNERIA DELLE TELECOMUNICAZIONI</b>	
Anno regolamento:	<b>2016</b>	
CFU:	<b>6</b>	
Settore:	<b>ING-INF/03</b>	
Tipo Attività:	<b>B - Caratterizzante</b>	
Anno corso:	<b>1</b>	
Periodo:	<b>Secondo Semestre</b>	
Sede:	<b>PARMA</b>	



## Testi in italiano

<b>Lingua insegnamento</b>	Inglese
<b>Contenuti</b>	<p>1) Basi di crittografia e meccanismi di autenticazione</p> <ul style="list-style-type: none"><li>- Basi della crittografia simmetrica (classica) ed esempi di algoritmi (DES, 3DES, AES)</li><li>- Basi della crittografia asimmetrica ed esempi di algoritmi (RSA, Diffie-Hellman, DSA); vantaggi e svantaggi</li><li>- Funzioni Hash e MAC (MD5, SHA, HMAC)</li><li>- Algoritmi di autenticazione basati su crittografia simmetrica o asimmetrica</li><li>- Scambio di chiavi tramite Key Distribution Center (KDC)</li><li>- Firma digitale, certificati digitali, autorità di certificazione, standard X.509/PKI (Public Key Infrastructure) e PGP (Pretty Good Privacy)</li></ul> <p>2) Protocolli per la sicurezza</p> <ul style="list-style-type: none"><li>- Protocolli di autenticazione e scambio di chiavi (Kerberos, AAA, RADIUS)</li><li>- Protocolli di comunicazione sicura a livello IP (IPSec/AH/ESP) e reti private virtuali (VPN)</li><li>- Protocolli di comunicazione sicura a livello di trasporto (SSL/TLS) e applicativo (SSH)</li></ul> <p>3) Vulnerabilità e protezione delle reti</p> <ul style="list-style-type: none"><li>- Vulnerabilità dei protocolli TCP/IP, tipologie di attacchi e possibili contromisure (sniffing, network e port scanning, spoofing, flooding, buffer overflow, etc.)</li><li>- Firewall (packet filtering, ALG, NAT, DMZ) ed esempi di configurazioni rete</li><li>- Protocolli per attraversamento di FW e NAT (STUN e TURN)</li><li>- Intrusion Detection System (IDS)</li><li>- Reti di anonimizzazione</li></ul>
<b>Testi di riferimento</b>	<p>[1] L. Veltri, "Network Security", Lucidi del corso [2] W. Stallings, "Cryptography and Network Security: Principles and Practice", Libro</p>

<b>Obiettivi formativi</b>	<p>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 conoscenza di base della crittografia applicata, e approfondire i seguenti argomenti:</p> <ul style="list-style-type: none"> <li>- principali algoritmi e protocolli di autenticazione;</li> <li>- principali protocolli per comunicazioni sicure;</li> <li>- possibili vulnerabilità in rete e principali meccanismi di protezione.</li> </ul> <p>Le capacità di applicare le conoscenze e comprensione elencate risultano essere in particolare:</p> <ul style="list-style-type: none"> <li>- analizzare schemi di autenticazione e di protezione dei dati basati su crittografia simmetrica e/o asimmetrica;</li> <li>- progettare meccanismi di autenticazione e di scambio di dati sicuri;</li> <li>- configurare e utilizzare protocolli e algoritmi standard per la sicurezza (ad esempio protocolli IPSec e TLS; algoritmi di crittografia AES, DES, 3DES, RSA; firma digitale e certificati digitali X.509 e PGP; etc.);</li> <li>- utilizzo di strumenti per il monitoraggio di una rete e scansione delle possibili vulnerabilità;</li> <li>- configurazione di sistemi di protezione dei nodi di una rete (firewall).</li> </ul>
<b>Prerequisiti</b>	<p>Conoscenze di base sulle architetture di comunicazione e i protocolli TCP/IP.</p>
<b>Metodi didattici</b>	<p>Lezioni in aula (36h), esercitazioni in aula (6h) svolte dal docente con gli studenti, e attività di laboratorio.</p>
<b>Modalità di verifica dell'apprendimento</b>	<p>Esami</p> <p>L'esame può essere superato in due modalità diverse:</p> <ol style="list-style-type: none"> <li>1) suddiviso in due prove di verifica in itinere scritte, rispettivamente a metà e a fine del corso integrate con un progetto svolto durante il corso; tali prove, se superate, completano l'esame; oppure</li> <li>2) sostenuto tramite prova scritta e orale durante i regolari appelli di esame.</li> </ol> <p>La prova scritta è composta da quesiti e esercizi da risolvere. Durante il corso verranno mostrati e risolti esempi di esercizi di esame.</p>
<b>Programma esteso</b>	<p>Vedi descrizione in inglese</p>



## Testi in inglese

<b>Lingua insegnamento</b>	<p>English</p>
<b>Contenuti</b>	<ol style="list-style-type: none"> <li>1) Basics of cryptography and authentication mechanisms <ul style="list-style-type: none"> <li>- Basics of symmetric (classic) cryptography and examples of algorithms (DES, 3DES, AES)</li> <li>- Basics of asymmetric cryptography and examples of algorithms (RSA, Diffie-Hellman, DSA); advantages and disadvantages</li> <li>- Hash and MAC functions (MD5, SHA, HMAC)</li> <li>- Authentication algorithms, based on both symmetric and asymmetric cryptography</li> <li>- Key exchange, agreement, and distribution</li> <li>- Digital signature, digital certificates, certification authority, Public Key Infrastructure, standard X.509, PGP (Pretty Good Privacy)</li> </ul> </li> <li>2) Security protocols <ul style="list-style-type: none"> <li>- Protocols for authentication and key exchange (Kerberos, AAA, RADIUS)</li> <li>- Protocols for secure communications at IP layer (IPSec/AH/ESP), and virtual private networks (VPNs)</li> </ul> </li> </ol>

- 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

## Testi di riferimento

[1] L. Veltri, "Network Security", Slides of the course

[2] W. Stallings, "Cryptography and Network Security: Principles and Practice", Book

## 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.

The abilities in applying the above-mentioned knowledge are in particular in the:

- 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

Classroom teaching (36h), and in class exercises (6h) carried out by the teacher with students, and laboratory activities.

## Modalità di verifica dell'apprendimento

Exams

The exam can be succeeded as:

1) divided into two written examinations, at the middle and the end of the course, together with a project carried out during the course, that complete the exam; or

2) written and oral exam, during regular scheduled examinations.

The written exam is composed of questions and exercises.

Examples of exercises are shown and solved during the course.

## Programma esteso

Syllabus (every lecture = 2 hours)

Lecture 1: course organization, objectives, textbooks, exam details; preview of the course; security services; attacks; security tools; symmetric cryptography: introduction; cryptography and cryptanalysis; cipher example (Caesar cipher)

Lecture 2: symmetric cryptography: types of attacks; side channel attack; computational security; example of cryptanalysis; substitution cipher; polyalphabetic substitution cipher; one time pad (OTP) cipher; transposition

Lecture 3: product cipher; steganography; block and stream ciphers; block ciphers: block size; substitution and permutation; Feistel cipher; DES

Lecture 4: double DES; TDEA; IDEA; AES; usages of symmetric cryptography; encryption of long messages; padding; ECB

Lecture 5: encryption of long messages: ECB; examples of attacks to ECB; CBC; examples of attacks to CBC; OFB; CFB; CTR; CBC-MIC, Unix crypto; hash functions; brute force attack

Lecture 6: birthday paradox; MD5; SHA; usages of hash functions

Lecture 7: message authentication; MAC and HMAC functions, number theory: group, ring, field

Lecture 8: number theory: modular arithmetic, relative prime, Euclid's algorithm, multiplicative inverse, extended Euclid's algorithm, Fermat's theorem, Euler's theorem

Lecture 9: extended Euclid's algorithm; examples, Fermat's theorem; Euler's theorem

Lecture 10: Euler's theorem demonstration; RSA; RSA example; RSA public and private keys

Lecture 11: discrete logarithm, DH, MITM attack to DH; digital signature; RSA

Lecture 12: DSA; zero-knowledge identification; Fiat-Shamir

Lecture 13: peer entity authentication; password management; one-time password

Lecture 14: general expression of the totient function; challenge-response authentication schemes

Lecture 15: exercises

Lecture 16: symmetric-cryptography-based key establishment; server-based key establishment

Lecture 17: public-key based key establishment; public key distribution; digital certificates

Lecture 18: digital certificates; cert chain; trust path; certification authority (CA); public key infrastructure (PKI); X.509 certificates; PKCS; certification revocation list (CRL)

Lecture 19: X.509 issues; PGP; AAA; HTTP authentication

Lecture 20: RADIUS; Diameter; Kerberos; security at PH, IP, TLS, and Application levels; IPSec; transport and tunnel modes;

Lecture 21: IPSec security association (SA); AH; ESP; IKE; transport Layer Security (TLS)

Lecture 22: TLS handshake; TLS analysis (wireshark); anonymity; high-latency anonymity systems; low-latency anonymity systems

Lecture 23: onion routing; network vulnerabilities; sniffers; eavesdropping; MITM;

Lecture 24: spoofing; ARP spoofing; TCP spoofing; ICMP attack; distributed DoS (DDoS) attacks; routing attacks; DHCP attacks; DNS poisoning; network scanning; host scanning; port scanning

Lecture 25: firewall: packet filter; PF examples; application level gateway

(ALG); firewall configurations

Lecture 26: packet filter exercises; linux netfilter/iptables; NAT

Lecture 27: intrusion detection system (IDS); exercises