384SM COMPUTER NETWORK

Aims

Knowledge and understanding:
Knowledge of the basic functioning principles of the Internet at the application level and internetwork level.
Knowledge of the basic functioning principles of DNS, email, web.
Knowledge of the basic functioning principles of networks and internetworks.
Knowledge of the basic principles of cryptography applied to computer networks.

Applying knowledge and understanding:
Ability to describe message exchanges occurring in selected scenarios in detail, including the fundamental pieces of information within each message as well as the way they are obtained and used.

Making judgements:
Ability to determine autnomously the main architectural components necessary for the working of an Internet application.

Communication skills:
The student shall acquire the ability to describe systems and algorithms by using correct terminology, both technically and logically. The student shall also acquire the ability to describe and point out the logical reasoning followed for solving a problem, separating sharply input data from hypotheses, deductions, necessary components, redundant components and so on.

Prerequisites

Designed to be self-contained
No need for specific preliminary computer-related knowledge (except for some familiarity with e-mail and web browsing).
Suitable also for courses different from Computer Engineering.

Contents

Network Applications, Application Layer, TCP properties.
DNS: usage, implementation, protocol, example.
E-mail: usage, implementation (SMTP, POP). MIME.
WWW. Introduction to HTML. HTTP (request, response, connection management).
Caching. Transmitting data to the server. Dynamic content. Sessions.
Authentication. HTTP Proxy.
Network. Ethernet. Switched Ethernet. Wireless Ethernet. Internetwork. IP. IP addresses and IP header. Connecting a new host. MTU and fragmentation. ICMP. ARP. Static routing. Connecting a new network.
IP address management.
Security problems. Private key cryptography and public key cryptography. Key distribution.
What you believe digital signatures guarantee. What they actually guarantee. Digital signature implementation. Certificates and applications. SSL and HTTPS.

Teaching Format

Lectures based on slides prepared by the teacher on each single topic.
Exercises selected by the teacher, solved by students autonomously for collective discussion.

Archive of common errors maintained along the years and available on the web.

Assessment

Written exam based on exercises followed by oral exam. Exercises are based on varying scenarios and require analysing the generated traffic, providing the configuration necessary to meet the exercise requirements, discuss security guarantees and possible limitations.

---------- o ----------

Obiettivi

Conoscenza e capacità di comprensione:
Conoscenza dei principi base del funzionamento di Internet ai livelli di astrazione applicativo ed internetwork.
Conoscenza dei concetti fondamentali del funzionamento di DNS, email, web.
Conoscenza dei concetti fondamentali del funzionamento di network e internetwork.
Conoscenza dei concetti fondamentali della crittografia applicata alle reti di calcolatori.

Capacità di applicare conoscenza e comprensione:
Capacità di descrivere in dettaglio gli scambi di messaggi che si verificano in situazioni specifiche, indicando le informazioni fondamentali in ogni messaggio, il modo in cui sono ottenute, il modo in cui sono utilizzate.

Autonomia di giudizio:
Capacità di determinare in maniera autonoma i principali componenti architetturali necessari per il funzionamento di un applicativo Internet.

Abilità comunicative:
Lo studente deve acquisire la capacità di descrivere sistemi ed algoritmi utilizzando la terminologia corretta, sia da un punto di vista tecnico sia da un punto di vista logico. Deve inoltre acquisire la capacità di descrivere ed evidenziare il processo logico seguito per risolvere un problema, separando chiaramente dati del problema, ipotesi, deduzioni, componenti necessarie, componenti ridondanti o non necessarie e così via.

Metodi didattici

Lezioni frontali su slide preparate dal docente su ogni argomento trattato nel corso.
Esercizi selezionati dal docente, svolti in maniera autonoma dagli studenti e discussi collettivamente in classe.
Archivio di errori comuni aggiornato nel corso degli anni e consultabile via web.

Verifica dell'apprendimento

Esame scritto basato su esercizi seguito da esame orale.