Esame di **Progettazione di servizi web e reti di calcolatori (01NBE)**
Corsi di Laurea in Ing. Gestionale e dell'Organizzazione d'Impresa
Prova scritta di teoria (26/1/2018)

> NOTA
> Le tracce delle soluzioni fornite in questo testo sono da considerarsi solo come un aiuto per comprendere i principali punti da toccare nel risolvere gli esercizi proposti ma non sono né esaustive né presentate in forma adeguata per l'elaborato da consegnarsi in sede d'esame.
> In particolare per molti esercizi le soluzione è volutamente schematica e ci si attende che il candidato spieghi adeguatamente i singoli punti, per dimostrare reale comprensione dell'argomento invece che semplice capacità mnemonica di ricordare i punti elencati nelle slide (o in queste tracce di soluzione).

Esercizio 1 ***(punti: 4)***

Spiegare che cosa sono il *dominio diretto* e quello *inverso* nel DNS, perché sono necessari entrambi e quali problemi si potrebbero avere se un nodo di rete fosse registrato solo in uno dei due domini.

Traccia di una possibile risposta

dominio diretto = traduzione a nome DNS ad indirizzi IP

dominio inverso = traduzione da indirizzo IP a nomi DNS

dominio diretto necessario per permettere agli utenti di usare nomi logici (es. www.polito.it)

dominio inverso necessario per tracciabilità (es. da dati registrati nei log risalire al nome del nodo che ha generato il traffico corrispondente)

se le registrazioni di nomi e indirizzi non corrispondono si potrebbero avere problemi coi server "paranoici" che potrebbero rifiutare la connessione . . .

Esercizio 2 ***(punti: 5)***

Disegnare lo schema di un'architettura web statica con pagine dinamiche, spiegarne il funzionamento ed illustrarne vantaggi e svantaggi.

Traccia di una possibile risposta

(schema di architettura web statica con le pagine che contengono parti dinamiche es. CSS, JS)

il server HTTP gestisce riceve richieste per pagina statiche, le legge da disco e le invia all'UA, che interpreta il contenuto HTML ed esegue localmente la parte dinamica

vantaggi: poco carico sul server, pagine interattive con l'utente, possibilità di caching e indexing

svantaggi: dati statici, carico sul client, funzionalità dipendente dalle capacità del client

Esercizio 3 ***(punti: 5)***

HTTP/1.1 usa per default connessioni persistenti. Spiegare di cosa si tratta e quali sono i vantaggi e svantaggi rispetto alle connessioni standard HTTP/1.0.

Traccia di una possibile risposta

In HTTP/1.1 le connessioni non sono più chiuse automaticamente dopo la risposta del server (come capitava in HTTP/1.0) ma quando il client segnala di voler terminare le comunicazioni (oppure quando la connessione resta inattiva per un tempo superiore al timeout).

Vantaggi: su un stessa connessione è possibile effettuare più richieste e ricevere più risposte, risparmiando in questo modo sul tempo di TCP setup (3-way handshake) e shutdown (4-way teardown) e conservando la window TCP.

Svantaggi: i client possono monopolizzare le risorse del server.

Esercizio 4 *(punti: 5)*

Spiegare il funzionamento dell'architettura *webmail* indicandone vantaggi e svantaggi rispetto ad un'architettura di posta elettronica basata su MUA.

Traccia di una possibile risposta

(disegno dell'architettura webmail)

L'utente usa un browser per accedere via HTTP ad un virtual MUA ospitato sul server del suo provider di webmail. E' quindi compito del provider gestire tutta la configurazione (MSA, MS) e memorizzare la posta per conto dell'utente.

Vantaggi: posta accessibile da qualunque dispositivo, semplicità di gestione.

Svantaggi: conservazione della posta affidata ad un ente terzo, con rischi per la sicurezza e la privacy.

Esercizio 5 *(punti: 5)*

Un server web con scheda di rete a 10 Mbps è collegato ad una rete locale di ateneo che opera a 100 Mbps. Alla medesima rete sono collegati 100 studenti dotati di un laptop con scheda di rete 802.11 da 54 Mbps. Il server web è di tipo iterativo, dotato di due CPU da 2 GHz ciascuna, 64 MB di RAM, disco da 1 TB, 10 ms, 40 MB/s. Sapendo che ogni studente richiede dal server un file da 20 MB (frammentato al 50% e memorizzato con settori da 4 kB), calcolare il tempo minimo entro cui tutti gli studenti avranno ricevuto il file richiesto.

Traccia di una possibile risposta

Trattandosi di un server iterativo, viene utilizzata un'unica CPU che esegue sequenzialmente il trasferimento dei file secondo l'ordine di richiesta.

Il collo di bottiglia nel trasferimento dei dati è dato da:

$$\min(v_{laptop}, v_{LAN}, v_{server}) = \min(54, 100, 10) = 10\,\text{Mbps}$$

Quindi il tempo per trasferire un file è data da:

$$t_R = \frac{20 \cdot 8}{10} = 16\,\text{s}$$

Il tempo per leggere un file da disco è dato dal tempo di accesso moltiplicato il numero di settori non contigui (che dipende dalla frammentazione) più il tempo di trasferimento:

$$\textit{settori} = \frac{20 \cdot 1024\,\text{kB}}{4\,\text{kB}} = 5120 \longrightarrow \textit{frammenti} = 5120 \cdot 50\% = 2560$$

$$t_F = 2560 \cdot 0.01\,\text{s} + \frac{20\,\text{MB}}{40\,\text{MB/s}} = 25.6 + 0.5 = 26.1\,\text{s}$$

In totale il tempo per trasferire un file è:

$$t_1 = 16 + 26.1 = 42.1\,\text{s}$$

ed il tempo per servire tutti gli studenti è:

$$t_{100} = 42.1 \cdot 100 = 4210\,\text{s} = 1\,\text{h}10\,\text{min}10\,\text{s}$$

Esercizio 6 ***(punti: 6)***

Il file A è stato protetto calcolandone il keyed-digest con HMAC-SHA1 e chiave da 128 bit mentre il file B è stato protetto calcolandone la firma digitale RSA-2048 con SHA1.

Spiegare quale tipo di calcoli sono stati fatti nei due casi e di quali proprietà di sicurezza godono i file A e B.

Traccia di una possibile risposta

Per il file A è stato calcolato il digest tramite l'algoritmo SHA1 combinando i dati con una chiave segreta tramite la tecnica HMAC. Questo fornisce al file A le proprietà di integrità (se il file viene modificato è possibile accorgersi della modifica) ed autenticazione (il file può essere stato creato solo da chi consce la chiave segreta).

Per il file B è stato calcolato il digest tramite l'algoritmo SHA1 e poi quest'ultimo è stato cifrato con l'algoritmo RSA con la chiave privata del firmatario. Questo fornisce al file A le proprietà di integrità (se il file viene modificato è possibile accorgersi della modifica), autenticazione (il file può essere stato creato solo da chi consce la chiave privata) e non ripudio (il possessore della chiave privata non può negare di aver firmato il file).