Università degli Studi di Verona, Dipartimento di Informatica

Programmazione e Sicurezza delle Reti, A.A. 2016/2017

Appello d'esame del 21 febbraio 2018

- L'esame consiste di due parti; ciascuna parte è composta da un esercizio e alcune domande.
- Lo studente svolga Parte I e Parte II su fogli distinti per permetterne la correzione in parallelo.
- Su ciascun foglio scrivere ***nome***, ***cognome*** e ***numero di matricola*** (non è obbligatorio consegnare la brutta copia)
- I risultati verranno pubblicati sugli avvisi della pagina del corso ***mercoledì 21 febbraio dopo le 21:00***
- La correzione dei temi d'esame può essere visionata durante la registrazione o il ricevimento docenti
- ***Orali*** (facoltativi a meno di una richiesta esplicita dei docenti) e ***registrazioni*** si terranno ***giovedì 22 febbraio alle 17:00 in aula M***

I Parte

Esercizio 1 (8 punti)

Implementare un sistema distribuito di monitoraggio del traffico stradale basato sul principio del *crowdsourcing*. Ciascun utente installa sul proprio smartphone un client che comunica ogni *T* secondi ad un server centrale le proprie coordinate GPS, il proprio ID univoco ed un numero di sequenza progressivo. Il server calcola la velocità di spostamento del client *j* all'istante *i* mediante la formula $v(i,j)=[x(i,j)-x(i-d,j)]/[d*T]$ dove $d>1$ in caso di perdita dei messaggi intermedi nella sequenza. Il server usa il valore di velocità, assieme a quello calcolato tramite altri client su quella stessa strada, per stimare il relativo livello di traffico. Si assume che la funzione per sapere le coordinate GPS si chiami *getGPS()* e che quella che blocca il thread chiamante per *T* secondi si chiami *wait(T)*.
Si chiede di:

1. Scrivere il codice Java relativo alla parte di comunicazione di client e server
2. Scrivere il codice Java che permette all'utente, quando lo desidera e in parallelo all'invio periodico della posizione, di chiedere al server il livello di traffico
3. Motivare la scelta del protocollo di livello trasporto utilizzato nelle due comunicazioni

Domande (2 punti ciascuna)

Si risponda in maniera sintetica e concisa (poche frasi per risposta sono sufficienti) alle seguenti domande:

1. Che cosa si può osservare in Wireshark nella prima fase di scambio di messaggi TCP per l'apertura di una connessione? Perché?
2. Per cosa è servito chiamare il comando IPTABLES durante l'esercitazione?
3. Come è strutturato un cavo UTP per Ethernet?

II Parte

Esercizio 2 (7 punti)

Un hotel è collegato al proprio ISP con un singolo router. L'hotel è composto da 30 camere, ciascuna dotata di porta di rete, la reception e due uffici amministrativi, dotati anch'essi di due porte di rete ciascuno. L'hotel ha dato in esterno la gestione del proprio server web e serve di posta elettronica, per cui non possiede nessun server che debba essere raggiunto dall'esterno. Per connettersi ad Internet, l'hotel ha sottoscritto un abbonamento con in ISP, il quale fornisce un indirizzo IP statico al router presente nell'hotel.

Per lo scenario sopra descritto si mostrino:

1. Lo schema della rete, indicando gli indirizzi assegnati alle interfacce del router, e alla rete dell'hotel (la scelta è arbitraria e funzionale al secondo punto; non serve scrivere nessun comando per gli apparati di rete);
2. Per il router, i comandi necessari per la comunicazione verso l'esterno degli utenti dell'hotel.

Domande (4 punti ciascuna)

Si risponda, elaborando quanto più possibile, alle seguenti domande:

1. Tra i primi sistemi di crittografia a chiave simmetrica vi è la cifratura monoalfabetica: si spieghi come funziona tale schema e si indichi la dimensione dello spazio delle chiavi.
2. Si descriva, anche attraverso esempi, su quali fattori si basa l'autenticazione degli utenti, indicando aspetti positivi e negativi di ciascun fattore.
3. Relativamente al Certificato Digitale, si descriva come viene creato, da chi viene creato, cosa contiene e il suo utilizzo.