T-110.5111 Computer Networks II - Advanced Features

Exam 07.12.2015
No auxiliary material (books, notes, computers, etc.) allowed
Each question is worth 2 points
Justify your answers but try to keep them brief and to the point.
Duration 3h
Teacher: Matti Siekkinen

1. What is the network architecture of the Internet?

2. What are the North Bound and South Bound APIs in Software Defined Networking (SDN)?

3. How does the multiple access control scheme of Wi-Fi differ from those used in cellular networks (3G and/or LTE)? Just outline the main difference(s).

4. Give two examples of how currently used Internet applications try to improve the quality of experience that they provide to the user.

5. You want to download a large file from a distant server over the Internet using your laptop that is connected to a Wi-Fi network. You can manually configure your operating system to use one of the following transport protocols: TCP NewReno, TCP Vegas, CUBIC TCP. Which one do you choose and why?

6. Explain the fundamentals of the congestion control in the Internet, i.e., where it is done and how (no protocol details, just the main principles).

7. Describe two major functional (i.e., not performance) differences between Bluetooth and Wi-Fi.

8. You are developing a mobile app that you wish to distribute on one of the market places. The app usage involves a certain amount of wireless communication that cannot be avoided. Describe (at least) one thing that you can do to reduce the wireless communication induced energy consumption of the smartphones of the users who have installed and use your app. Explain also why and when (if not always) that technique reduces the energy consumption.

9. What is the objective of CoDel? Outline also the way it tries to achieve it.

10. Which main factors determine the most suitable type of datacenter network architecture for a specific datacenter?

T-110.5241 Network security
Examination 2015-12-17
Lecturer: Tuomas Aura
No electronic equipment or reference material is allowed in the examination.

Answer only 5 of the 6 problems. If you answer them all, problems 1–5 will be marked.

1. Name resolution

Explain ARP (very briefly), ARP spoofing, and its consequences. Also, discuss the potential defenses against ARP spoofing, including their limitations.

Note: There are many possible defenses. Answering that part will require your own thinking.

2. Cellular networks

Explain the reasons for the following:

(a) When you arrive by airplane to a new country and turn on your mobile phone, it can take a few minutes before the phone is connected to a cellular network and you can make calls. If you later turn the phone off and then back on, or go temporarily out of the network coverage area, it reconnects without delay.
(b) Fake base stations can exist even though 3G and 4G phones and networks support mutual authentication between the mobile device and the access network.

Note: The answer to this part can be relatively short. In part (a), you only need to consider reasons related to the GSM/UMTS/LTE security architecture and protocols. In part (b), there can be more than one reason.

3. Wireless security

Explain the protocol that takes place when university students connect to the Eduroam network on Aalto campus.

Note: Show the approximate protocol phases, messages and participants, explain their purpose, and explain approximately how the session keys are derived.

4. Denial of Service

Client puzzles (or cryptographic proof of work) can be used to prevent unwanted email. In fact, this was the purpose for which client puzzles were first invented. Their application to denial-of-service prevention in key-exchange protocols like HIP was suggested only later.

Explain how the internet mail-delivery protocol SMTP could be extended with client puzzles to discourage spam. Include the details of the cryptographic protocol.

Please turn the paper over for problems 5–6.

5. Authentication protocols

Consider the following two-message key-establishment protocol:

1. A → B: A, B, N_A
2. B → A: N_A, $E_A(R)$, $Sign_B(h(\text{"confirm"}, N_A, R))$

A's and B's certificates, issued by a trusted CA, are available to everyone at an online directory.
h, E_A, $Sign_B$ = cryptographic hash function, encryption with A's public key, B's signature.
N_A, R = fresh random numbers generated by A and B, respectively.
Session key SK = h("key", N_A, R).

Analyze the security of this protocol.

6. Sybil attack

Sybil attacks are a common problem in peer-to-peer and reputation systems. Explain what is a *Sybil attack* and give examples of Sybil attacks against at least four different types of systems and services.

Hint: You can consider, for example, the Tor anonymity network, politicians on Twitter, hotel reviews on TripAdvisor, the eBay online auction site, vehicular communication e.g. for congestion detection and avoidance, BitTorrent, or paper-based political elections.