Homework 4, 2020

Name: _____

Student ID: _____

Notes:

1. Be **brief** and **concise** in your answers.
2. If you wish to be considered for partial credit, show all your work.
3. You are expected to uphold the highest degree of academic honesty.

PROBLEM	MAX SCORE	YOUR SCORE
1	24	
2	40	
3	12	
4	12	
5	12	
TOTAL	100	

YOU ARE EXPECTED TO WORK ON IT INDEPENDENTLY !!

Problem 1 (24 points): Multiple choices (3 points each). Select all correct answers from the given five choices (there *may* be multiple correct answers).

1. Which of the following statements about design principles/rules of cellular networks are correct?

   - Your answer ____ (A) Control-plan signaling is always offered highest serving priority; (B) Voice services are always offered higher serving priorities than Internet-access data services (e.g., accessing CNN website); (C) Use two-plane operations: control-plane and data-plane; (D) Move from circuit-switched (CS) to packet-switched (PS) design.

2. Which of the following statements about packet-switched (PS) and circuit-switched (CS) signaling/services are incorrect?

   - Your answer ____ (A) CS services does not assign dedicated resources to their users; (B) PS service users need to share resources with other users; (C) CS services are also supported in 4G mobile networks; (D) CS voice services can provide users with guaranteed performance (assume that the users are stationary).

3. Which of the following statements about data service charging are incorrect?

   - Your answer ____ (A) the data usage is only accounted at the gateways (i.e., GGSN(3G) and P-GW(4G)) in core network; (B) 4G users do not need to pay for their downlink packets that have been received by P-GW (a gateway in the core network) but discarded by the P-GW later (assume that there exists no vulnerabilities in operators' charging policies); (C) According to charging policies, users may not need to pay for their data usage; (D) Stealth-spam-attack aims to take advantage of operators (e.g., AT&T) rather than attack against mobile users.

4. In cellular network, a plane (e.g., control-plane, data-plane) is a suite of particular protocols (e.g., RRC, NAS) and hosts (e.g., P-GW, MME). Which protocol(s) is/are in both 4G LTE control-plane and data-plane?

   - Your answer ____ (A) RRC; (B) RLC; (C) NAS; (D) PDCP.

5. What are three main procedures in 4G LTE security?

   - Your answer ____ (A) Authentication (B) NAS security setup (C) AS security setup (D) PDP context activation procedure.

6. Nowadays, what are three main voice solutions defined by 3GPP for mobile users?

   - Your answer ____ (A) CSFB (Circuit-switched Fallback); (B) VoLTE (Voice over LTE); (C) Skype; and (D) VoWiFi (Voice over WiFi).

7. Which of the following statements about CSFB voice services are correct?

   - Your answer ____ (A) CSFB will switch a user from 4G LTE networks to 2G/3G networks for voice services; (B) CSFB users can reject the network-initiated CSFB 4G→3G inter-system switch requests ; (C) after a CSFB call ends, the CSFB user will be always immediately switched back to 4G networks; and (D) Dialing a CSFB call will inevitably cause a short-time data service suspension (e.g., a few seconds).

8. Which of the following statements about long-range wireless IoT technologies are incorrect?

- Your answer ____ (A) SigFox and LoRA only support the data rate lower than 100 Kbps; (B) SigFox and LoRA can support critical IoT devices/services which require low latencies and high data rates; (C) Cellular IoT can support both massive and critical IoT devices; and (D) The battery life of cellular IoT devices can also last for a few days as smartphone do.

Problem 2 (40 points; 5 points each): Answer the following questions. Be brief and concise.

1. In CSFB, there are two inter-system switch options, namely handover and cell reselection. Assume that your operator adopts the cell reselection option. Please explain why after you end a CSFB call, you will not be immediately switched back to 4G LTE network when you have some ongoing data services.

2. Please briefly introduce three security vulnerabilities of operational CSFB services.

3. In CSFB, please explain why Ping-Pong attack will reduce the TCP throughput of the victims to 0.08Mbps in a short time?

4. Please explain how to launch a silent call towards a CSFB user via VoLTE?

5. In VoLTE, please explain how operators provide users with "Carrier-grade" VoLTE voice quality?

6. In CS-based SMS, the mobile phone needs to send an SMS to SMSC through SM-TP (Short Message Transfer Protocol). Please briefly explain why SM-TP can prevent users from spoofing other people's phone numbers as the SMS sender phone number.

7. On Android, the Android OS will monitor two SMS activities: (1) sending SMSs to short phone numbers (e.g., 32665) and (2) sending a large number of SMS messages and provide users with warning dialogs. Please briefly explain why IMS-based SMS attack can suppress the warning dialogs.

8. Please briefly explain how 4G LTE operators know the type (e.g., smartphones, smartwatches) of a connected device and what the security vulnerability is.

Problem 3: Circuit-switched Fallback (CSFB) Voice Services (12 points) In the CSFB paper, the authors show that by dialing a silent call to a CSFB user, the user will suffer from a variety of attacks (e.g., TCP throughput downgrade) and will be unaware of these silent calls. Please answer the following questions.

1. (5 points) On smartphones, there are many spam block applications, e.g., Call Blocker, Call Blacklists. Please briefly explain why these applications cannot prevent CSFB users from suffering CSFB-based attacks based on a great number of inter-system switch (e.g., 4G→3G, 3G→4G) by blocking malicious callers? Assume that adversaries do not change their calling phone numbers.

2. (7 points) Please design a security mechanism that helps CSFB users to defend against various CSFB attacks without affecting the functional correctness of CSFB services, which means that users can still use voice services via CSFB without any issues? Assume that adversaries do not change their calling phone numbers.

Problem 4: Mobile Data Service Charging (12 points) In 4G LTE networks, after a user's packets arrive at P-GW, the data usage will be increased. Assume that the user has to pay for the data usage accounted at P-GW. Please answer the following questions.

1. (5 points) The current TCP/IP implementation of most mobile phones will discard unwanted packets (those packets that no applications expect to receive). However, discarding those unwanted packets cannot stop the data usage accounting conducted at P-GW. The user thus needs to pay for these unwanted packets. Assume that the unwanted packets are sent by an adversary outside of cellular network (e.g., a host on the Internet). Please design a security mechanism that helps the user to prevent malicious spamming attack induced by unwanted packets.

2. (7 points) Assume that you are an adversary who aims to launch an overbilling attack against a mobile user and is capable of transmitting packets to the mobile user bypassing the operator's NAT and firewall servers. Please design an attack which silently increases the mobile user's data usage (i.e., no unwanted packets will be received by the mobile user's phone). Hint: P-GW is also a router which supports all Internet packet routing functions (e.g., checking the checksum and TTL fields of IP packets).

Problem 5: 4G LTE Network Security (12 points). The mobile networks adopt symmetric cryptography. A secret key K is stored in a user's SIM card and the operator's authentication center (AuC). Please answer the following questions.

1. (3 points) Which entity produces K_{ASME} at the user side? SIM card or Phone? Hint: Please refer to the slide Key Hierarchy in 4G LTE Security in Lecture 7.

2. (3 points) Which entity performs cellular signaling/data encryption and integrity functions at the user side? SIM card or Phone? Please briefly explain why the entity is selected? Hint: Please refer to the slide Key Hierarchy in 4G LTE Security in Lecture 7.

3. (6 points) In 4G LTE network, the data-plane traffic transmitted between phones and base stations will not be provided with the integrity protection. Please briefly discuss its advantages and disadvantages.