COMP 61421

Two hours

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Cyber Security

Date: Monday 23rd January 2017

Time: 14:00 - 16:00

Please answer any THREE Questions from the FOUR Questions provided

This is a CLOSED book examination

The use of electronic calculators is NOT permitted

[PTO]

1. Assuming that *Alice* is a client and *Bob* is a server, and both of them have access to any cryptosystems such as a public-key cryptosystem, a symmetric-key cryptosystem, and a cryptographic hash function. Answer the following questions.

   (a) Using the challenge-response authentication approach, design *four* different authentication protocols (or protocol variants) by which *Bob* can verify *Alice's* identity. For each designed protocol, you should clearly explain what is in the Challenge, what is in the Response, and how the Response is verified. You should also make clear any assumptions used in your design. The protocols should protect against impersonation and replay attacks.

   (12 marks)

   (b) Outline any factors and/or design considerations that may impact on the security of the protocols that you have designed in (a).

   (8 marks)

2. E-Payment is a starting up business aimed at supporting electronic payment services through customers' mobile phones. The company has already got a wired network in the building, and is now planning to install an IEEE802.11 hub to support service access through mobile devices by their employees. This wireless LAN facility is to be integrated with the existing wired network. Answer the following questions.

   (a) Identify *three* security threats that could be introduced as the result of this wireless network installation and integration, and outline security services that are necessary to counter each of the threats you identify.

   (6 marks)

   (b) Describe key features of the IEEE802.1x authentication standard, and outline the benefits of having these key features.

   (5 marks)

   (c) Wired Equivalent Privacy (WEP) is the original IEEE802.11 Security proposal, whereas WPA is the intermediate and WPA2 (Wireless Protected Access) is the full implementation of IEEE 802.11i proposal (which is the WLAN Security Standard).

   Use a table to contrast the three security proposals (WEP, WPA and WPA2) in terms of key size, key management method, and security services that they each support. You should also indicate (where appropriate) how the security services are provided in these proposals.

   (9 marks)

[PTO]

3. An enterprise network is connected to the Internet via a packet filtering firewall. The intention is to protect the enterprise network against attacks from the Internet. Answer the following questions.

   (a) Describe what these attacks are and how they are mounted: Port Scanning, IP Spoofing, Smurf, TCP SYN flood, and IP fragmentation attacks.

   (10 marks)

   (b) Would this packet filtering firewall be able to protect against these attacks. Justify your answer.

   (10 marks)

4. A university teaching hospital is going to install a patient health monitoring system for monitoring a patient's health 24 hours per day and 7 days per week. This system consists of a personal health monitor, *M*, a software system, *P*, and another software system, *G*. *P* is supposed to run on a host, or a device, that is connected to a trusted network in the vicinity of the patient's location. *G* is used by the patient's doctor, and operates on a networked computer or a mobile device such as a smartphone. *M* collects the patient's health data and sends the data to *P* via a wireless channel regularly. *P* generates health monitoring reports for the patient based on the data received from *M*. *G* can request the latest health monitoring report from *P* at any time. Answer the following questions.

   (a) Design a secure and efficient protocol that allows (i) system *G* to request the patient's private health monitoring report from system *P*, and (ii) *P* to respond to the request by sending the report to *G*. The design should satisfy the following *five* requirements: (R1) the protocol should protect against unauthorised access to health monitoring reports; (R2) the protocol should protect against unauthorised or accidental changes to health monitoring reports; (R3) the protocol should protect against repudiation of origin and message replay; (R4) the protocol should protect patient's identity privacy; (R5) the protocol should be the most *efficient* in terms of computational and communication costs.

   Note that the design is permitted to use any (symmetric and/or asymmetric) cryptosystems including secure hash functions. You should present your protocol formally, e.g. using the Kerberos protocol format, state any assumptions you have made for the design, and explain clearly how the protocol operates, including any verifications performed by the protocol entities.

   (10 marks)

   (b) Justify how the designed protocol satisfies the five requirements outlined in 4(a).

   (10 marks)

END OF EXAMINATION