Two hours

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Computer and Network Security

Date: Thursday 15th January 2015
Time: 09:45 - 11:45

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. Secure Sockets Layer (SSL) is a suite of protocols developed to support private communications over a public network such as the Internet. Answer the following questions.

(a) Explain how, in SSL, client and server mutual authentications are achieved and how traffic protection keys are established. (12 marks)

(b) Use a diagram to outline SSL Record Protocol format, and describe this protocol outbound (i.e. data transfer) and inbound (i.e. data reception) data processing operations. (8 marks)

2. A firewall is a perimeter defence mechanism commonly used to protect a private network against external attacks. Answer the following questions.

(a) With the use of proper diagrams, explain the major differences between the two firewall architectures: the screened bastion host and screened subnet, and indicate their respective merits. (8 marks)

(b) For each of the following attacks, describe how the attack is carried out, and what consequence it has on the underlying network.
   (i) Smurf attack
   (ii) IP Fragmentation attack
   (iii) IP Packet Sniffing attack

   Also for each of the attacks named above, describe a countermeasure, or how to configure firewall rules, to reduce the risk of the attack. (12 marks)
3. A personal health monitor worn by a patient transmits collected health data through wireless communication to a software system $P$ to produce the patient’s health monitoring reports. $P$ is supposed to run on a trusted network host in the vicinity of the patient’s location. Another software system $G$ used by the patient’s GP (or doctor) operates on a networked computer or a mobile device such as a smartphone. $G$ can request the latest health monitoring report from $P$ to allow the GP to check the report and take necessary actions when needed.

(a) Identify two security threats to the communications between the two systems $P$ and $G$ mentioned above, and explain the consequences that could be caused by each of the identified threats.

(b) Clearly a secure communication protocol is needed to allow (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 $G$. Note that the protocol is permitted to use any (symmetric and/or asymmetric) cryptosystems including secure hash functions.

Design such a protocol and present it formally, e.g. using the Kerberos protocol format. State any assumptions you have made for the design, and explain how the designed protocol operates.

(c) Justify how the designed protocol can prevent each of the two security threats identified in 3 (a).

4. A university network uses Kerberos 4 for client authentication.

(a) Explain why Kerberos uses two different types of servers: authentication and ticket-granting servers. Clearly describe their respective functionalities and any benefits for separating them.

(b) Describe step by step, with necessary protocol details, how a client applies its password to eventually obtain a cryptographic key shared between the client and an application server.

(c) Kerberos uses an authenticator for message authentication. Discuss whether such an authenticator is stronger than a RSA-based digital signature in terms of protections against false denial of transmissions.

END OF EXAMINATION

Page 3 of 3