COMP 61421

Two hours

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Cyber Security

Date: Friday 19th January 2018

Time: 14:00 - 16:00

Please answer all THREE Questions.

This is a CLOSED book examination

The use of electronic calculators is NOT permitted

[PTO]

1. A company has been given a job of designing an Air Space Control system. The system should be able to tell (within a few seconds) if an aircraft appearing on their radar is authorised. If the aircraft is authorised to use the air space, then the system will not take any further action. Otherwise, the system will issue an instruction for a military action to be taken to bring down the aircraft. After some research, the company has come up with a solution. In this solution, authorised aircrafts and the air traffic controller (AirTrafficController) are each issued with a pre-shared secret key, *K*. At run time, AirTrafficController uses a challenge-response protocol to verify any incoming aircraft. This protocol consists of two messages, a challenge and a response, as shown below:

   I. $A \rightarrow B: n$;
   II. $B \rightarrow A: \mathrm{E}(K, n)$;

   Where message I is the challenge that is sent by *A* (AirTrafficController) to *B* (any incoming aircraft), message II is *B*'s response to the challenge, *n* is a unique random nonce, *K* is the pre-shared secret that is known to all the authorised aircrafts and AirTrafficController, and *E* is an encryption function (or a secure one-way cryptographic function).

   Answer the following questions.

   a) Can this protocol be used to identify any unauthorised aircraft? You should justify your answer. Also explain the purpose for the use of the nonce in this protocol.

   (4 marks)

   b) Analyse the security of this protocol, identifying at least *three* security threats or attacks that may compromise the security of this protocol (i.e. any threats or attacks by which an enemy aircraft, or an unauthorized aircraft, can successfully invade the air space). For any threats or attacks you have identified, describe how they are mounted.

   (10 marks)

   c) For each of the threats or attacks you have identified in b), describe a countermeasure.

   (6 marks)

[Please Turn Over]

2. An access control system should ensure that every access to a system and its resources is controlled and that only authorized accesses are allowed. Answer the following questions.

   a) Use a diagram to illustrate the functional components of an access control system and explain how these components inter-work to accomplish the task of access control. In your explanation, you should make clear the names of the functional components, the sequence of operations undertaken by the access control system when serving an access request, and the functions the access control system provides and how the functions are provided.

   (6 marks)

   b) Least privilege and separation of duties are two of the security principles used for RBAC (Role Based Access Control). Explain what they mean.

   (6 marks)

   c) There are a number of ways (referred to as access control mechanisms or models) that can be used to implement an access control system, for example, Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role-based Access Control (RBAC) models. DAC can further be classified into Access Control List (ACL) and Capability, etc. For each of the access control models, i.e. MAC, RBAC, ACL and Capability, name one application scenario or context, where the model is mostly suitable. You should also provide justifications to your answer.

   (8 marks)

3. Alice is going to purchase a smart phone from one of the on-line vendors, called SmartPhones, using the Web Browser on her desktop. She will make the payment using her MasterCard. To ensure transaction security, SSL (Secure Socket Layer) has been enabled on the vendor's Web Server (hereafter referred to as Server) and Alice's desktop Web Browser (hereafter referred to as Client). Answer the following questions.

   a) Describe how mutual authentication is achieved between the Client and the Server. The description should cover the operations carried out, respectively, by the Client and the Server in achieving the mutual authentication.

   (8 marks)

   b) Describe how the confidentiality and integrity of Alice's MasterCard details are protected. You should also make clear which SSL protocol provides these protections, and how the protocol operates.

   (6 marks)

   c) Explain how the cryptographic keys (i.e. the keys used for protecting the confidentiality and integrity of Alice MasterCard details) are established.

   (6 marks)

END OF EXAMINATION