Two hours

UNIVERSITY OF MANCHESTER
DEPARTMENT OF COMPUTER SCIENCE

Cyber Security

Date: Monday 13th January 2020

Time: 09:45 - 11:45

Please answer all THREE Questions
Each question is worth 20 marks

This is a CLOSED book examination

The use of electronic calculators is NOT permitted

1. Kerberos is a computer-network based authentication protocol allowing nodes connected via a non-secure network to prove their identities to one another in a secure manner. In a nutshell, Kerberos provides two services, an authentication service and a ticket granting service.

   a) Describe the Kerberos version 4 (Kerberos-v4) protocol. (4 marks)

   b) Use Kerberos-v4 to explain how the authentication service and the ticket granting service are provided. (4 marks)

   c) Identify *three* security threats in relation to node authentication in a networked environment and, for each threat you have identified, explain the countermeasure used in the Kerberos-v4 protocol. (6 marks)

   d) Extend the Kerberos-v4 protocol to allow a client *C* in a realm *A* to access a server in another realm *B*. Justify your extended protocol by explaining what additional functions the extended protocol provides and why. (6 marks)

2. Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role Based Access Control (RBAC) are three main access control approaches. With regard to the DAC approach, there are multiple access control models, e.g. Access Control List (ACL), Capability-based and Procedure-based models. Answer the following questions.

   a) Contrast the *four* access control models, i.e. RBAC, ACL, Capability-based and Procedure-based model, in terms of how access control is facilitated with each model. Also, for each model, identify an access scenario which the model is mostly suited to. (8 marks)

   b) There are *two* security models associated with MAC. Name these *two* security models, and, for each of the security models, explain what security protection it provides and how it is provided. (8 marks)

   c) Use a diagram to illustrate the functional components an access control system typically consists of and, based on the diagram, explain how these components inter-work to accomplish the task of access control. (4 marks)

3. A firewall is commonly used to protect a private network against attacks from the Internet. Answer the following questions.

   a) Outline *three* functions (i.e. protections) a firewall can provide and *three* limitations in the use of a firewall to protect a private network against security attacks in general. (6 marks)

   b) Describe and contrast *three* different firewall architectures. (6 marks)

   c) Describe what a *TCP SYN Flood* attack is, and comment on how a firewall may be used to counter this attack and any limitations. (4 marks)

   d) Explain how to use IP Fragmentation to launch a DoS attack on a host and a countermeasure to thwart this attack. (4 marks)

END OF EXAMINATION