Two hours

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Computer and Network Security

Date: Friday 17th January 2014
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
1. Authentication, confidentiality, and integrity are three properties of secure communication. A networked system may be subject to threats to these properties by attackers who exploit vulnerabilities in the system. To counter the threats we implement security controls or services.

Suppose that $KU_a$ and $KR_a$ are the public and private keys of a party $A$, respectively, $KU_b$ and $KR_b$ are those of a party $B$, and each of $A$ and $B$ can use any cryptosystems.

(a) If $A$ wants to send a very long message to $B$, suggest an encryption method by which only $B$ can decrypt the message and the encryption/decryption processes are the most efficient.

(b) Repeat question (a), but this time the message should be protected with both confidentiality and message origin authentication services.

(c) Now suppose that the two parties wish to establish a secure session, and they use the following authentication protocol to authenticate each other. Here $ra$ and $rb$ are random numbers picked by $A$ and $B$, respectively; $i \rightarrow j: M$ means that party $i$ sends a message $M$ to party $j$; $x || y$ means the concatenation of $x$ and $y$; $E_K()$ means encryption using $K$.

1. $A \rightarrow B$: $E_{KR_a}(ra || B || A)$
2. $B \rightarrow A$: $ra || E_{KR_b}(rb || A || B)$
3. $A \rightarrow B$: $rb$

Identify a security flaw in this protocol, and suggest a solution to fix the flaw. Clearly state any assumption(s) that you may use.

(d) Prior to communication, parties $A$ and $B$ must have each other’s digital certificates. Explain what a digital certificate is, and what security assurance it provides.
2. A distributed intrusion detection system is deployed over a wide area network. For effective intrusion detection, the network is divided into a number of realms (i.e. domains). Each realm hosts an information server and a group of detection agents, which are software components, used to detect potential intrusions in the realm. The agents cooperate among themselves and with agents in other realms whenever necessary. They access network information hosted on the information server for intrusion analysis. As the network information is important, the agents’ identification and authentication are essential for information protection. For this reason, Kerberos 4 (i.e. version 4) is employed to provide the authentication service in each realm.

(a) Describe the steps that Kerberos 4 takes to establish a session key between a client (i.e. a detection agent) and an application server (i.e. the information server) in the same realm.

(6 marks)

(b) Describe the role of the authenticator used in the Kerberos protocol, and explain why an authenticator is NOT required when a client requests a ticket-granting ticket from an authentication server.

(4 marks)

(c) Suggest three improvements to Kerberos 4.

(6 marks)

(d) Now assume that a detection agent, C, in realm A needs to access information hosted by an information server in realm B. Explain how to extend the Kerberos 4 protocol to allow C in realm A to access the server in realm B.

(4 marks)
3. A small financial firm is currently using ACL (Access Control List), a discretionary access control mechanism, for the protection of its resources (including computer systems and data files). As the firm is small, its resources are located in the same building and managed in the same domain. However, recently this firm is planning a merger with another firm, and if this merger is successful, its IT system will be transformed into a large-scale distributed system where resources will be managed in multiple domains. You have been asked to do a review of its access control strategy and to assess if ACL would still be adequate for the new IT system. Answer the following questions.

(a) Contrast the two access control mechanisms, Capability and Role Based Access Control (RBAC), in terms of their respective working mechanisms (i.e. how access control is governed), strengths and limitations.

(b) Contrast the two access control mechanisms, ACL and Capability, in terms of (i) ease of making an authorisation decision during execution; (ii) ease of adding access for a new subject; (iii) ease of deleting access by a subject; and (iv) ease of creating a new object to which all subjects by default have access to. Justify your answers to the questions.

(c) One of the suggestions for the new IT system is to apply mandatory access control to the system. Outline two main differences of mandatory access control from discretionary access control, and one main advantage of mandatory access control over discretionary access control.

4. Upon a risk analysis on a university’s site network, the following threats and attacks are identified: threats from malicious code (e.g. virus, worms and Trojan horse), port scanning, IP spoofing, and TCP SYN flood attacks. To counter these threats and attacks, an administrator in the university, Bob, has suggested using a firewall to control the access of the site network from the Internet.

(a) Describe what Port Scanning, IP Spoofing, and TCP SYN flood attacks are, and explain how a firewall can be used to protect against these attacks.

(b) Contrast the three types of malicious code, virus, worms and Trojan horse.

(c) There are three types of firewalls to choose from: packet filtering firewalls, stateful packet inspection firewalls, and application gateways. Describes the working mechanisms of the three types of firewalls.