

Assignment #3

Due: October 13

Problem 1 (40 pts) Network Security The Dribble Corporation¹ uses its website as the primary source for selling dribbles. The corporation, and its top IT administrator John Ipsec, are asking you for help in making sure that it is protected from a number of different types of attacks. The information used to create a dribble is considered top secret to the Dribble Corporation, so much so that employees are not allowed to bring anything into the building that might possibly record information. Use the information provided in professor Cristina Nita-Rotaru's lecture to answer the following questions.

- a) The John Ipsec has heard a lot of news lately about denial of service and distributed denial of service attacks. John is very worried that the company's website might fall victim to this type of an attack. He suspects that an attacker would launch a SYN flood attack against the company's website. He is considering installing a firewall to help control this type of an attack. The firewall he will install is 3 times faster at completing request than the web server.
- i) What is the difference between a denial of service attack and a distributed denial of service attack? (One sentence answer.)
 - ii) Which is usually more effective?
 - iii) What are the two types of distributed denial of service attacks, and which is harder to trace back?
 - iii) Describe what a SYN flood attack is, and what resources it consumes during an attack.
 - iv) Which type of a firewall approach should John use to prevent SYN flood attacks against the company's website, and why?
- b) A lot of the people working at Dribble Corp have been asking John to allow instant messaging to be enabled on their machines. Assuming a 100% completely secure instant messaging client, what is the top security issue surrounding allowing employees to use instant messaging clients?
- c) E-mail inside of the Dribble Corp is highly sensitive because it can possibly contain specifications on how to create a dribble that their competitors could use against them. John is aware of this, and only allows e-mail from employees to employees, and not outside the company's network. However, the Dribble Corp is considering opening a new office overseas in which all communication must flow over the Internet.
- i) What is the main security issue with allowing e-mail to flow from one office to another via the Internet?
 - ii) If a program like PGP were used to encrypt e-mail, what type of a solution would this be in networking terms?
 - iii) If John installed IPSec on all employee machines, which protocol would be used to protect communications?
 - iv) Which IPSec mode would John need to use?

¹Not my name, see the text pg 733.

- v) Does IPSec, regardless of the mode, encrypt packets from the highest OSI level to the lowest, or the lowest to the highest?
- d) Jonh Ipsec was looking at the RFC for IPSec and did not understand it completely. His question to you is, “Why are the mutable fields in the AH protocol set to zero when the IVC is computed?”

Problem 2 (25 pts) Access Control ORCON (Originator Control) is a decentralized system of access control in which each originator determines who needs access to the data. No centralized set of rules controls access to data; access is at the complete discretion of the originator. ORCON is a hybrid scheme which is neither MAC nor DAC. Here the originator of the object may not be the owner of that object.

Please read Section 7.3 of Matt Bishop and answer the following questions:

- a [Ex. 4, Section 7.8] Consider using MACs and compartments to implement an ORCON control. Assume that there are k different organizations. Organization i will produce $n(i, j)$ documents to be shared with organization j .
 1. How many compartments are needed to allow any organization to share a document with any other organization?
 2. Now assume that organization i will need to share $n_m(i, i_1, \dots, i_m)$ documents with organizations i, i_1, \dots, i_m . How many compartments will be needed?
- b ORCON provides controls that are different from DAC and MAC. Give one distinct example of a situation where DAC, MAC and ORCON do not work.

Problem 3 (35 pts) RBAC a Consider a Hierarchical RBAC model and suppose that the permission inheritance semantics is used. Revise the specification of the *avail_session_perms()* function, defined in class for Core RBAC, in order to take role hierarchies into account.

b Discuss how a RBAC system can be configured to in order to simulate a MAC system.