CS370/ECE499 November 22, 2016

Intro to Computer Security

Problem Set 3: Public-Key Cryptography, Key Exchange Protocols and Access Control

1) Digital Signatures
   a) What is a digital signature? What security properties does it provide?
   b) Do digital signatures and MACs increase the length of message to be transmitted? Explain Why?
   c) Using the notation from the class, show how a message m is signed with an RSA key-pair (N, d, e).
   d) Does the hash function used in an RSA signature need to be a keyed hash function? Why or why not?
   e) When encrypting and signing a message m, does the order of encryption and signature operations matter? Explain.

2) Time-Variant Parameters.
   a) What is the role of R1 and R2 (or N_A and N_B in Handbook of Applied Cryptography) in Needham Schroeder Protocol? What properties should R1 and R2 have?
   b) Why does Alice have to send r2-1 in the last message of Needham-Schroeder? Can she have not sent r3 instead?
   c) Can a timestamp be used instead on R1? What is the advantage and disadvantage of using one over the other (i.e., R1 or N_A vs. timestamps) in security protocols? (Hint: see the discussion on this in Handbook of Applied Cryptography – 10.3.1).

3) Long Lived and Session Keys
   a) What are pseudorandom numbers? Why are they used?
   b) What is the difference between session keys and interchange keys? Why are session keys needed? Do we need session keys when there is a shared symmetric interchange key between two-parties or are they only needed when using asymmetric cryptography?
   c) Why is a trusted-third party desirable/needed for key-exchange? Is such an entity only desirable/needed when using symmetric keys or is such an entity also desirable/needed when using asymmetric keys as well?

4) Access Contol Concepts Concepts
   a) The three most important components in access control, all starting with the letter ‘A’, are what?
   b) What is the primary difference between DAC and MAC access model?
   c) In access control, what does an “open policy” mean? What does a “closed policy” mean?
   d) What is the difference between a “role” in RBAC and a “group” commonly used in UNIX?

e) Explain the difference between Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC).

5) Access Control Matrix

Consider the following scenario. An organization employs product managers, programmers and testers. The organization operates with the following kinds of files: development code and executables, testing code and executables, test reports, and production code and executables.

Product Managers can view, and execute the development executables and production executables to verify correctness. Programmers can create, edit, delete, and execute development code and executables. Programmers can also promote development code to the test level.

Testers can edit, delete, and execute test code and executables. The testers write test reports that can be read by everyone. The testers can promote test code to production level or demote it back to development.

Everyone can view and execute production code and executables. Eve is the product manager, Alice and Bob are programmers. Carol and Dave are testers

a) Define the rights the access control system would need to enforce the requirements for this scenario. Associate the abbreviation you will use in parts (b) and (c) with the definition.
b) Design an access control matrix for the scenario for the users.
c) Assume the Access Matrix is being implemented by a system using Access Control Lists. Write the Access Control List for the Development Executables.
d) Assume the Access Matrix is being implemented by a Capability system. Write the Capability list for Alice.

6) UNIX Permissions
   a) When a file in Unix is protected with mode “644” and is inside a directory with mode “730” describe ways in which the file can be compromised?

7) RBAC
   a) Would the access control for the scenario in Q5 above benefit from being implemented in a RBAC system? If yes, explain why and create access matrices that define an RBAC that would enforce this scenario? If not, describe why not and present another scenario that would be better defined as an RBAC system rather than a straight DAC.
   b) A company has 20 job functions. On average there are 200 employees in each job function. Similarly, on average an employee in each job function needs 1500 permissions to properly execute their task. Compare the number of assignments that need to be managed i) when using a DAC model vs. ii) when using RBAC model. Generalize the comparison to when the number of job functions is N, number of employees per job function is $U_{i,}$ where i indexes the job-function, and the number of permissions required per job function is $P_{i.}$

c) Consider a hierarchical Role-Based Access Control (RBAC) system where a role **Manager** inherits from a role **Clerk**. A **Manager** is permitted to perform operations *Review* and *Approve* on resource ***Report***, and a **Clerk** is permitted to perform operation *Edit* on resource ***Report***. User Alice is assigned to role **Manager**, and user Bob is assigned to role **Clerk**. For each statement below circle T if the statement is always true, and F if it can ever be false.

a. (T / F) Bob is necessarily also assigned to the role Manager.
b. (T / F) Alice necessarily has privileges to Edit.
c. (T / F) An RBAC session can have both Alice and Bob associated with it

8) Changing Access Control Matrix

	File 1	File 2	File 3	File 4	Subject A	Subject B	Subject C
Subject A	Own R W		Own R W		Control		Own
Subject B	R	Own R W	W	R*		Control	
Subject C	R W	R		Own R W			Control

Keeping in mind the rules governing access control matrix change covered in Section 4.3 (and discussed in class), and the access matrix shown above, answer whether or not the following changes to access matrix are allowed. **Explain in one sentence why or why not.**

a. (allowed / not allowed) Subject C wants to Transfer R on File 2 to Subject A

b. (allowed / not allowed) Subject A wants to Delete R on File 2 from Subject C