CS419/ECE499 Fall 2018

Intro to Computer Security

Topics: Public-Key Cryptography and Digital Signatures, Trusted Computing, Key Exchange Protocols, Access Control

Public-Key Cryptography and Digital Signatures

1. [3pts] Name three differences between secret-key cryptographic schemes and public-key cryptographic schemes?

2. What is a digital signature? What security properties does it provide?

3. [3pts] How are digital signatures different from MACs?

4. [9pts] Alice owns a public-private key pair (PK_A, SK_A); Bob owns a public-private key pair (PK_B, SK_B); Assume that they know each other's public keys and answer the following questions:

    a) If Alice wants to send a secret message M to Bob, what should she do? Show what needs to be transmitted using the notaion used in class.

    b) Bob receives a 128-bit AES key and the message "from Alice: use this key to send me your credit card number", both enciphered with his public key. Should Bob do what the message says? Assume Bob does want to send Alice his credit card number. If yes, why? If not, how should the message have been enciphered?

    c) If M is a really long message, how should Alice transmit the message while keeping it secret and minimizing the effort? Please explain.

5. [3 pts] Do digital signatures and MACs increase the length of message to be transmitted? Explain Why?

6. [3 pts] Using the notation from the class, show how a message m is signed with an RSA key-pair (N, d, e).

7. [2pts] Contrast man-in-the-middle and meet-in-the-middle atatcks.

8. [4pts] Is it important to hash the message for digital signatures?

9. [3 pts] Does the hash function used in an RSA signature need to be a keyed hash function? Why or why not?

10. [4 pts] When encrypting and signing a message m, does the order of encryption and signature operations matter? Explain.

11. [4 pts] What is a digital certificate? And what is a certificate chain

12. Time-Variant Parameters.

a) [3 pts] 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) [2 pt] Why does Alice have to send r2-1 in the last message of Needham-Schroeder? Can she have not sent r3 instead?

c) [3pts] 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).

13. Trusted Computing

   a) [4 pts] What are the 4 sub-problems underlying the trusted computing problem?

   b) [4 pts] What is a hash chain? Compare and contrast the use of hash-chains vs. certificate chains for measuring the programs loaded?

   c) [4 pts] What is a manifest and why is it needed?

   d) [3 pts] Can TCB help us trust a remote machine to which an adversary has physical access? Why or why not?

   e) [3 pts] Can TCB help provide continuous attestation – that is attest to what software is currently running on the machine?

   f) [2 pts] What is the difference between secure boot and measured boot?

   g) [2 pts] What is sealed memory or storage?

   h) [2 pts] What are the two ownership models for trusted computing/TCB? Which model is currently implemented and why?

14. Long Lived and Session Keys

    a) [4 pts] What are pseudorandom numbers? Why are they used?

    b) [4 pts] 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) [6 pts] 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?

13. [2 pts] What is the difference between multi-factor authentication and mutual authentication?

14. Access Contol Concepts Concepts

a) [3 pts] The three most important components in access control, all starting with the letter 'A', are what?

b) [2 pts] What is the primary difference between DAC and MAC access model?

c) [2 pts] In access control, what does an "open policy" mean? What does a "closed policy" mean?

d) [3 pts] Explain the difference between Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC).

15. 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) [3 pts] 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) [3 pts] Design an access control matrix for the scenario for the users.

c) [2 pts] Assume the Access Matrix is being implemented by a system using Access Control Lists. Write the Access Control List for the Development Executables.

d) [2 pts] Assume the Access Matrix is being implemented by a Capability system. Write the Capability list for Alice.

16. 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

Key Establishment Protocols

$$A \longrightarrow B : SID, A, B, \{N_A, SID, A, B\}_{K_{AS}} \tag{1}$$

$$B \longrightarrow S : SID, A, B, \{N_A, SID, A, B\}_{K_{AS}}, \{N_B, SID, A, B\}_{K_{BS}} \tag{2}$$

$$S \longrightarrow B : \{N_A, k_{AB}\}_{K_{AS}}, \{N_B, k_{AB}\}_{K_{BS}} \tag{3}$$

$$B \longrightarrow A : \{N_A, k_{AB}\}_{K_{AS}}, \{N_B\}_{k_{AB}} \tag{4}$$

$$A \longrightarrow B : \{N_B - 1\}_{k_{AB}} \tag{5}$$

Listed above is a modified version of Otway-Rees Key Establishment Protocol. SID is a fresh session ID generated by A. N_A and N_B are fresh nonces generated by A and B respectively. K_{AS} and K_{BS} are long-term symmetric keys that A and B share respectively with a trusted server S. k_{AB} denotes a session key generated by the server S for use by A and B.

Please review the above protocol carefully and answer the following questions:

(a) **(3 pts)** At the end of message 1 from A to B, how does B know that it is talking to A? Please circle **one or more** of the following to indicate your answer. Use the space provided to state any assumptions you made or justify your answer if you want.

i. Because the plain text portion SID, A, B clearly indicates that the message is from A.

ii. Apart from reason (i) above, B can also see that $\{N_A, SID, A, B\}_{K_{AS}}$ is an encrypted message with a key K_{AS} shared between A and S

iii. Actually B can't be sure that it is talking to A until message 3 or later in the protocol

(b) **(5 pts)** At the end of message 3 from S to B, how does B know that the received key is a shared key for a communication session with A? Please circle **one or more** of the following to indicate your answer. Use the space provided to state any assumptions you made or justify your answer if you want.

i. Because B can see that the key k_{AB} has a subscript AB indicating it is to be shared between A and B

ii. Because B can see in message 3 that one ticket $\{N_A, k_{AB}\}_{K_{AS}}$ is encrypted with a key shared between A and S, while the other ticket $\{N_B, k_{AB}\}_{K_{BS}}$ is encrypted with a key shared between B and S,

iii. Because B's ticket $\{N_B, k_{AB}\}_{K_{BS}}$ that is encrypted by a key known only to a trusted entity S has N_B inside it, which is associated with SID, A, B from message 2.

iv. Actually B can't be sure that the key sent to it in the 3rd message is for communication with A until after message 5.

v. If SID, A, B outside and inside each of $\{N_A, SID, A, B\}_{K_{AS}}$, and $\{N_B, SID, A, B\}_{K_{BS}}$ in message 2 didn't match then S which is a trusted entity would not generate message 3.

(c) **(4 pts)** At the end of a correct message 4 from B, what does A know? Please circle **one or more** of the following to indicate your answer and state any assumption you made in the space provided.

i. A knows that k_{AB} generated by S is for communication between A and B.

ii. A knows that k_{AB} is associated with a specific session ID SID and is fresh.

iii. A knows that B also has the same key k_{AB} and that B is alive or online.

iv. A knows that k_{AB} generated by S is for communication between A and B but can't be sure that the key is fresh and that B also has it.

(d) **(4 pts)** At the end of a correct message 5 from A what does B know? Please circle **one or more** of the following to indicate your answer and state any assumption you made in the space provided.

i. B knows that k_{AB} is generated by S for communication between A and B, and that the key is fresh

ii. B knows that A also has the same key k_{AB} bus cannot be sure that the key is fresh.

iii. B knows both that A also has the same key k_{AB}, and that A is alive or online.

iv. B knows that k_{AB} is generated by S for communication between A and B, that the key is fresh, that A has the same key, but cannot be sure which session it is associated with when A starts two parallel sessions $SID1$ and $SID2$ with B.