FIT3031: Tutorial 4

AUTHENTICATION APPLICATIONS

Q1 What problem was Kerberos designed to address?

Ans: The problem that Kerberos addresses is this: Assume an open distributed environment in which users at workstations wish to access services on servers distributed throughout the network. We would like for servers to be able to restrict access to authorized users and to be able to authenticate requests for service. In this environment, a workstation cannot be trusted to identify its users correctly to network services.√

Q2 What are the three threats associated with user authentication over a network or Internet?

Ans: **1.** A user may gain access to a particular workstation and pretend to be another user operating from that workstation. **2.** A user may alter the network address of a workstation so that the requests sent from the altered workstation appear to come from the impersonated workstation. **3.** A user may eavesdrop on exchanges and use a replay attack to gain entrance to a server or to disrupt operations.√

Q3 List three approaches to secure user authentication in a distributed environment.

Ans: **1.** Rely on each individual client workstation to assure the identity of its user or users and rely on each server to enforce a security policy based on user identification (ID). **2.** Require that client systems authenticate themselves to servers, but trust the client system concerning the identity of its user. **3.** Require the user to prove identity for each service invoked. Also require that servers prove their identity to clients.√

Q4 What four requirements were defined for Kerberos?

Ans: **Secure:** A network eavesdropper should not be able to obtain the necessary information to impersonate a user. More generally, Kerberos should be strong enough that a potential opponent does not find it to be the weak link. **Reliable:** For all services that rely on Kerberos for access control, lack of availability of the Kerberos service means lack of availability of the supported services. Hence, Kerberos should be highly reliable and should employ a distributed server architecture, with one system able to back up another. **Transparent:** Ideally, the user should not be aware that authentication is taking place, beyond the requirement to enter a password. **Scalable:** The system should be capable of supporting large numbers of clients and servers. This suggests a modular, distributed architecture.√

Q5 What are the essential ingredients of a public-key directory?

Ans: 1. The authority maintains a directory with a {name, public key} entry for each participant.
2. Each participant registers a public key with the directory authority. Registration would have to be in person or by some form of secure authenticated communication.
3. A participant may replace the existing key with a new one at any time, either because of the desire to replace a public key that has already been used for a large amount of data, or because the corresponding private key has been compromised in some way.
4. Periodically, the authority publishes the entire directory or updates to the directory. For example, a hard-copy version much like a telephone book could be published, or updates could be listed in a widelycirculated newspaper.
5. Participants could also access the directory electronically. For this purpose, secure, authenticated communication from the authority to the participant is mandatory.√

Q6 What are the requirements for the use of a public-key certificate scheme?
Ans: 1. Any participant can read a certificate to determine the name and public key of the certificate's owner.
2. Any participant can verify that the certificate originated from the certificate authority and is not counterfeit. **3.** Only the certificate authority can create and update certificates.
4. Any participant can verify the currency of the certificate.

Q7 What is the purpose of the X.509 standard?

Ans: X.509 defines a framework for the provision of authentication services by the X.500 directory to its users. The directory may serve as a repository of public-key certificates. Each certificate contains the public key of a user and is signed with the private key of a trusted certification authority. In addition, X.509 defines alternative authentication protocols based on the use of public-key certificates.√

Q8 What is a chain of certificates?

Ans: A chain of certificates consists of a sequence of certificates created by different certification authorities (CAs) in which each successive certificate is a certificate by one CA that certifies the public key of the next CA in the chain.

Q9 How is an X.509 certificate revoked?

Ans: The owner of a public-key can issue a certificate revocation list that revokes one or more certificates.

Problems:

1. There are 3 typical ways to use nonces as challenges. Suppose N_a is a nonce generated by A, A and B share key K, and f() is a function (such as increment). The three usages are:

Usage 1	**Usage 2**	**Usage 3**
(1) A → B: N_a (2) B → A:E(K, N_a)	(1) A → B: E(K, N_a) (2) B → A: N_a	(1) A → B: E(K, N_a) (2) B → A: E(K, f(N_a))

Describe situations for which each usage is appropriate.

Ans: All three really serve the same purpose. The difference is in the vulnerability. In **Usage 1**, an attacker could breach security by inflating N_a and withholding an answer from B for future replay attack, a form of suppress-replay attack. The attacker could attempt to predict a plausible reply in **Usage 2**, but this will not succeed if the nonces are random. In both Usage 1 and 2, the messages work in either direction. That is, if *N* is sent in either direction, the response is E[*K*, *N*]. In **Usage 3**, the message is encrypted in both directions; the purpose of function f is to assure that messages 1 and 2 are not identical. Thus, Usage 3 is more secure. √

2. Consider a one-way authentication technique based on asymmetric encryption:

   A → B: ID_A
   B → A: R_1
   A → B: E(PR_a, R_1)

   a. Explain the protocol.
   Ans: This is a means of authenticating A to B. R_1 serves as a challenge, and only A is able to encrypt R_1 so that it can be decrypted with A's public key.

   b. What type of attacks is this protocol susceptible to?
   Ans: Someone (e.g., C) can use this mechanism to get A to sign a message. Then, C will present this signature to D along with the message, claiming it was sent by A. This is a problem if A uses its public/private key for both authentication, signatures, etc. √

3. In Kerberos, when Bob receives a ticket from Alice, how does he know it is genuine?

   Ans: It contains the Alice's ID, Bob's name, and timestamp encrypted by the KDC-Bob shared secret key. √

4. In Kerberos, Alice receives a reply, how does she know it came from Bob (that it's not a replay of an earlier message from Bob)?

   Ans: It has a nonce (e.g., time stamp) encrypted with the session key. √

5. Consider the following protocol:

$$\begin{array}{ll} A \rightarrow KDC: & ID_A \parallel ID_B \parallel N_1 \\ KDC \rightarrow A: & E(K_a,[K_S \parallel ID_B \parallel N_1 \parallel E(K_b,[K_S \parallel ID_A])) \\ A \rightarrow B: & E(K_b,[K_S \parallel ID_A]) \\ B \rightarrow A: & E(K_S, N_2) \\ A \rightarrow B: & E(K_S, f(N_2)) \end{array}$$

   a. Explain the protocol

   Ans: A requests a session key for use between A and B from the KDC. A nonce is used for challenge-response.

   b. Can you think of a possible attack on this protocol, if an old key, K_S is compromised? Explain how it can be done.

   Ans: If someone manages to get an old *K_S*, they can replay the message from step 3 to B and communicate with B, pretending to be A.

   c. Mention a possible technique to get around the attack — not a detailed mechanism, just the basics of the idea.

   Ans: Timestamps included with the message can counter this vulnerability

6. Explain the problems with key management and how it affects symmetric cryptography?

   Ans: The primary weakness of symmetric encryption algorithms is keeping the single key secure. Known as key management, it poses a number of significant challenges.

   - If a user wants to send an encrypted message to another using symmetric encryption, he must be sure that she has the key to decrypt the message.

- How should the first user get the key to the second user? He would not want to send it electronically through the Internet, because that would make it vulnerable to eavesdroppers. Nor can he encrypt the key and send it, because the recipient would need some way to decrypt the key.
- And if he can even get the get securely to the user, how can be he certain that an attacker has not seen the key on that person's computer?

  Key management is a significant impediment to using symmetric encryption.