Dalton Murray

INT 7223 Cybersecurity

Dr. Hany Othman

July 17, 2023

Chapter 23 & 24 Review

Question

23.1 What are the principal elements of a Kerberos system?

The principal elements of a Kerberos system are: having clients, application servers, and a Kerberos server (Stallings & Brown, 2018. p. 685). There is also the potential to use an authentication server, AS, which knows the passwords of the clients and stores them in a centralized database which allows for identity verification (Stallings & Brown, 2018. p. 686).

23.2 What is Kerberos realm?

A Kerberos realm is a full-service Kerberos environment which has a Kerberos server, clients, application servers, the Kerberos server have user IDs and passwords in a database and all users are registered with the Kerberos server, and the Kerberos server shares a secret key with each server and each server is registered with the Kerberos server (Stallings & Brown, 2018. p. 689). In other words, a full environment is referred to as a realm and each network of clients and servers which are under different administrative organizations are different realms (Stallings & Brown, 2018. p. 689).

23.3 What are the differences between versions 4 and 5 of Kerberos?

Version 4 of Kerberos was published on the late 1980s, and the improved and extended version, version 5, was released in 1993 and updated more recently in 2005 (Stallings & Brown, 2018. p. 690). In version 5, an encrypted message is tagged with an encryption algorithm identifier allowing Kerberos to use an algorithm other than DES such as AES as the new default (Stallings & Brown, 2018. p. 690). Version 5 also supports authentication forwarding while version 4 does not allow credentials issued to one client to be forwarded to another host and used by another client (Stallings & Brown, 2018. p. 691). Version 5 also supports interrealm authentication which requires fewer secure key exchanges compared to version 4 (Stallings & Brown, 2018. p. 691).

23.4 What is X.509?

X.509 is a ITU-T standard which is the most widely accepted format for public-key certificates, they are used in most network security applications such as IPSEC or IP Security, Secure Sockets Layer, SSL, Transport Layer Security, TLS, Secure Electronic Transactions, SET, and S/MIME and in some e-commerce or e-business applications (Stallings & Brown, 2018. p. 692).

23.5 What key elements are included in a X.509 certificate?

In an X.509 certificate the key elements included are: the key owning subject's X.500 name and public-key information, the dates or period of validity, the CA's issuer name, their signature that binds it all together, and in version 3 a general extension mechanism which provides more flexibility to convey information needed in special circumstances (Stallings & Brown, 2018. p. 692).

24.1 What is the basic building block of an 802.11 WLAN?

The basic building block of an 801.11 WLAN, or the smallest building block, is a basic service set, BSS, and this consists of wireless stations which execute the same MAC protocol and compete for access to the same shared wireless medium (Stallings & Brown, 2018. p. 711). A basic service set, BSS, can be isolated or it can connect to a backbone distribution system, DS, through an access point, AP, which functions as a bridge and relay point (Stallings & Brown, 2018. p. 711).

24.2 Define an extended service set

An extended service set are composed of two or more basic service sets that are interconnected by a distribution system, the ESS, or extended service set, then appears as a set logical LAN at the LLC level (Stallings & Brown, 2018. p. 712).

24.4 Is a distribution system a wireless network?

It is possible for a distribution system to be a wireless network, a WDS, wireless distribution system, however, it is also possible for it to be a wired network, a standard DS, distribution system (Stallings & Brown, 2018. p. 709 & 711).

24.6 What security areas are addressed by IEEE 802.11i?

802.11i addresses all areas of authentication, access control, and privacy with message integrity (Stallings & Brown, 2018. p. 715).

Authentication – Authentication uses a protocol to define an exchange between a user and an authentication server, this provides mutual authentication and generates temporary keys in order to be used between the client and the AP over the wireless link (Stallings & Brown, 2018. p. 715).

Access control – Access control enforces the use of the authentication function, it routes the messages properly, and it facilitates key exchange and works with a variety of authentication protocols (Stallings & Brown, 2018. p. 715).

Privacy with message integrity – With privacy with message integrity we used MAC-level data, such as an LLC PDU, and encrypt it along with the message integrity code that ensures that the data has not been altered (Stallings & Brown, 2018. p. 715).

24.7 Briefly describe the four IEEE 802.11i phases of operation

802.11i has five phases of operation, these are as follows: discovery, authentication, key management, protected data transfer, and connection termination (Stallings & Brown, 2018. p. 717 - 718).

Discovery – In the discovery phase an AP uses messages which are called beacons and probe responses in order to advertise its IEEE 802.11i security policy, the STA then uses these to identify an AP for a WLAN, the STA associated with the AP and selects a cipher suite and authentication mechanism (Stallings & Brown, 2018. p. 717).

Authentication – In authentication the STA and AS prove their identities to each other (Stallings & Brown, 2018. p. 717).

Key management – In key management the AP and STA perform several operations that cause cryptographic keys to be generated and placed on the AP and the STA (Stallings & Brown, 2018. p. 717).

Protected data transfer – In protected data transfer frames are exchanged between the STA and the end station through the AP (Stallings & Brown, 2018. p. 718).

Connection termination – In connection termination the AP and STA exchange frames which tear down the secure connection and restore it to its original state (Stallings & Brown, 2018. p. 718).

Problem

23.4 Using your Web browser, visit any secure Web site (i.e., one whose URL starts with “https”). Examine the details of the X.509 certificate used by that site.

This is usually accessible by selecting the padlock symbol. Answer the same questions as for Problem23.3.

a. Identify the key elements in this certificate, including the owner's name and public key, its validity dates, the name of the CA that signed it, and the type and value of signature.

The site I will be using is https://www.google.com/. The certificate was issued to *.google.com, and it was issued by GTS CA 1C3, Google Trust Services LLC. It was issued on Monday, 29 may 2023 and expires on Monday, 21 August 2023. It uses the fingerprint sha-256 2A A9 7C A4 5C 98 E1 4D 3C D1 2A F6 5B 39 6F 1A 51 73 1B 94 EC 4B 5F 70 5A 89 20 11 67 75 AD C2 and the fingerprint sha-1 A8 B5 2B DE 3B DB FB AB 1B 78 7A E6 8F DE 23 23 6C AB 86 3B.

b. State whether this is a CA or end-user certificate, and why.

This is a CA despite it being issued by Google to Google, it uses the official certificate authority of Google. However, in a sense it could be considered a end-user certificate because it is technically issued by themselves to themselves despite them using an official certificate authority.

c. Indicate whether the certificate is valid or not, and why.

This is a valid certificate as it is within its issue and expiration date and has been properly signed by an authority.

d. State whether there are any other obvious problems with the algorithms used in this certificate.

There are no obvious problems with the algorithms used in this certificate.

References

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice*. Pearson.

I have neither given nor received unauthorized aid in completing this work, nor have I presented someone else's work as my own.

Dalton Murray