F15 NET3900

Modules 5,6,7 Assignment

Instructions:

Please show all your calculations for numerical answers.

The grade for each question is shown next to the question number.

Note the provided slide references.

Please submit this assignment via Bb, email or via paper to me at a lecture or lab.

The solutions will be posted to Bb following the due date.

This assignment is due by midnight Sunday October 11.

1/2. Briefly explain Layer 2 authentication and Layer 3 authentication. Provide a couple of examples of each.

Ref: Module 5 page 11.

Layer 2 authentication operates at Layer 2. Layer 2 auth protocols include 802.1X and MAC authentication.

Layer 3 authentication operates at or above Layer 3 after the client gets basic L2 and L3 connectivity including an IP address. Layer 3 Auth protocols include Web page authentication portal and some VPN access.

2/2. What is the difference between WPA2 Enterprise and WPA2 Personal in terms of the authentication methods used and their strength.

Ref: Module 7 Slides 5-11

WPA2 Personal uses a pre-shared key

Method is weak because: (1) same shared key available to all users, (2) some keys may be crackable

WPA2 Enterprise uses strong EAP methods such as 802.1X/PEAP

Method is strong because of (1) use of encrypted tunnels to pass credentials, (2) dynamic key generation for each user (i.e. no shared key) and use of individual username/password.

3/2. What are the key steps to create a digital signature for a server certificate.

Ref: Supplement Slide 12

Step 1: Make a HASH of the certificate using SHA1 or SHA256

Step 2: Encrypt the HASH using the private key of the Certificate Authorithy

4/2. What are the key steps the client uses to verify the digital signature of a certificate.

FYI, the client also takes additional steps to validate the signature including checking the expiring date and validating the FQDN in the Common Name.

Ref: Supplement Slide 13

Step 1: Decrypt the digital signature using the public key of the Certificate Authority to get the original HASH of the certificate.

Step 2: Create a local HASH of the certificate

Step 3: Compare the original HASH to the local HASH. If they are the same then the signature is verified.

5/2. The 802.1X protocol defines three devices. What are their names and functions as defined by 802.1X.

Ref: Supplement Slide 17

1. Supplicant: requests authentication and access to the network resources
2. Authenticator: blocks or allows traffic to pass through its port and to the network
3. Authentication Server: validates the credentials of the supplicant and notifies the authenticator

6/2. 802.1X/PEAP is a bidirectional authentication protocol. What does this mean and provide example authentication protocols for each direction.

Ref: Module 5 page 8; Supplement Module page 18.

It means that the user must authenticate to the auth server and the auth server must authenticate to the user

1. User to Auth server: MSCHAPv2
2. Auth Server to user: Digital Certs

7/1. During 802.1X/PEAP authentication, what steps are taken by the authentication protocol to ensure the user credentials are passed securely to the RADIUS server?

Ref: Supplement

The protocol includes establishing an encrypted TLS tunnel. The user credentials are passed from the supplicant to the auth server via this tunnel.

8/2. During 802.1X/PEAP negotiation, and after the user credential is validated, why does RADIUS pass the PMK to the wireless controller?
Ref: Supplement slide 19.
The PMK is the pairwise master key which was created during the EAP negotiation. The PMK is passed to the controller/authenticator.
The client and controller use PMK to create a temporal key called the PTK pairwise temporal key. Temporal keys increase the robustness of the security. It also speeds roaming by avoiding the need to reauthenticate when roaming to another AP or controller.

9/1. As the wireless client roams from an AP to another AP, the client reassociates to the second AP. The client does not need to reauthenticate and the PMK (Pairwise Master Key) remains. However for security reasons, which Encryption Key is regenerated?
Ref: Supplement Slide 22.
The PTK is regenerated. Use of temporal keys increases security.

10/1. The EAP negotiation occurs between the client and the Authentciation Server. Aruba has a feature to offload the authentication server and move the EAP negotiation to the wireless controller. What is the name of this feature?
Ref: Module 6, slides 9,10
FastConnect

11/2. When using multiple Authentication Servers, what is the difference between FALL THROUGH and FAIL THROUGH? These are Aruba Networks features.
Ref: Module 6, slides 4, 5
Fall Through: When the auth server does not reply, the next auth server is used.
Fail Through: When the auth server replies with an Auth Deny, the controller attempts to authorize against the next server in the group.

12/1. During 802.1X/EAP negotiation, the supplicant warns the user that it cannot validate the server certificate. What is the risk of over-riding the warning and accepting the certificate anyway?

Failure to validate the server certificate means that the auth server cannot be authenticated. This could mean that the user is connected to a rogue server via a rogue connection. This rogue connection is possibly being used for nefarious purposes.