Securing Enterprise Wireless LANs with RADIUS Authentication

Chris Stutzman (Chris.Stutzman@asu.edu)
Dr. Feng Wang (fwang25@asu.edu)
Applied Computing
Division of Mathematical and Natural Sciences
New College of Interdisciplinary Arts & Sciences
ASU Arizona State University

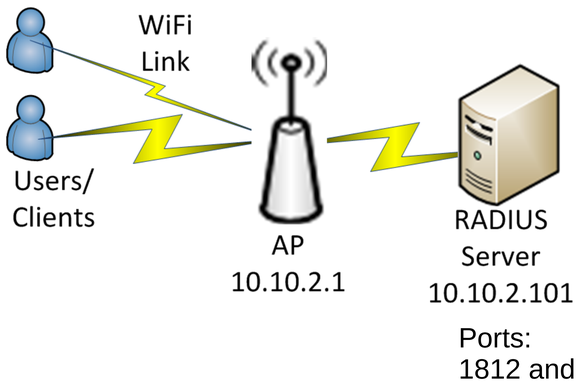
Purpose of the Project

- Understand how RADIUS works
- Setup RADIUS environment
- Capture and analyze RADIUS authentication process between clients, Access Point (AP) and RADIUS server

What is RADIUS

- RADIUS is used in the enterprise environment to secure wireless network access
- Authenticating wireless clients in an enterprise environment is challenging as you dont want to have to manage dozens or even hundreds of access control devices, this is where RADIUS comes in, there is only one device you need to manage the user credentials, it works across rooms, buildings and even campuses/locations
- Clients can use both certificates and a username and password for RADIUS authentication, we used a username and password

Network Topology



- RADIUS server:
  - freeRADIUS, the software that does the RADIUS functions and authentication
  - MySQL,the database used that stores the credentials
- Access Point (AP)
  - provide wireless connection to wireless clients and authenticate the clients with RADIUS
  - The AP is a Cisco 1811 router

RADIUS Authentication Process

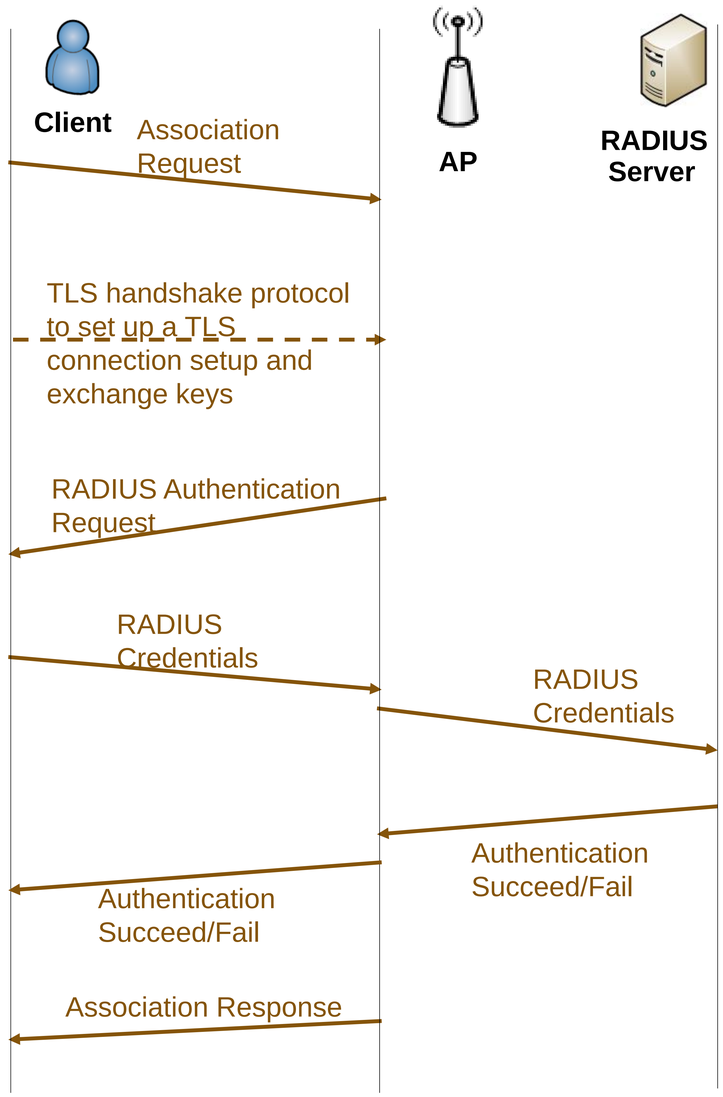


Figure 1: Messages and components involved in a RADIUS authentication

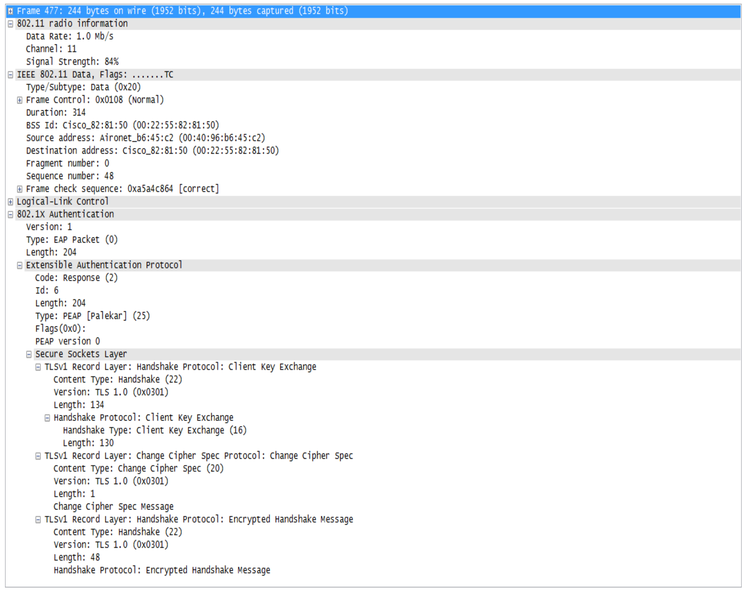
Components

- Clients
  - Configured to use PEAP-TLS to communicate with AP
- AP
  - configured to use PEAP-TLS to communication with clients
  - configured to use RADIUS for user authentication and specify RADIUS server IP address
- RADIUS
  - configured to authenticate user with username/password saved in mySQL server

Steps:

- Clients sends Association Request to request wireless access in plaintext
- AP and client sets up a secure TLS connection to secure using TLS handshake protocol. This is called PEAP-TLS and only AP's certificate is used
- AP prompts the client to do RADIUS authentication
- Clients sends back RADIUS credential which is protected with the key generated from the TLS handshake protocol
- AP forwards client's RADIUS credential to RADIUS server. This step is protected using the pre-shared key between AP and RADIUS server
- RADIUS server passes the credential to the mySQL database for verification
- RADIUS server sends authentication succeed/fail message to AP
- AP forwards the message to client
- If RADIUS authentication is successful, AP sends association response to client to give client wireless access

An Example of Captured Traffic



```
Frame 477: 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits)
802.11 radio information
    Data Rate: 1.0 Mb/s
    Channel: 11
    Signal Strength: 84%
IEEE 802.11 Data, Flags: .....TC
    Type/Subtype: Data (0x20)
  + Frame Control: 0x0108 (Normal)
    Duration: 314
    BSS Id: Cisco_82:81:50 (00:22:55:82:81:50)
    Source address: Aironet_b6:45:c2 (00:40:96:b6:45:c2)
    Destination address: Cisco_82:81:50 (00:22:55:82:81:50)
    Fragment number: 0
    Sequence number: 48
  + Frame check sequence: 0xa5a4c864 [correct]
+ Logical-Link Control
802.1X Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 204
Extensible Authentication Protocol
    Code: Response (2)
    Id: 6
    Length: 204
    Type: PEAP [Palekar] (25)
    Flags(0x0):
    PEAP version 0
Secure Sockets Layer
  TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 134
    Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 130
  TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.0 (0x0301)
      Length: 1
      Change Cipher Spec Message
  TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 48
      Handshake Protocol: Encrypted Handshake Message
```

Figure 2: A snapshot of the packet transmitted between the AP and client during a TLS handshake captured by Ominpeek

Conclusions

- The enterprise wireless networks can be secured with RADIUS for easier user management and robust authentication
- Cisco use EAP-TLS coupled with Radius to provide enterprise level user authentication and security