CNL Lab2 Report

2017.04.12

Contribution by each team member

ID	Name	Contribution
b03902080	黃子賢	1/6
b03902022	于建民	1/6
b03902024	鄭筱樺	1/6
b03902026	徐新凱	1/6
b03902084	王藝霖	1/6
b03902126	高翊軒	1/6

WLAN Authentication Mechanism

1. 說明目前市面上對於無線區域網路所提出之認證機制其優缺點。
2. 說明提出之認證機制的運作原理。
3. 說明對於所提出之認證機制其漏洞預防措施為何。

Below list four types of WLAN authentication mechanisms. AP may use several authentication mechanisms at the same time by configuring multiple SSIDs.

Open (System) Authentication

- Allow any device to authenticate and then attempt to communicate with AP. Client doesn't need to provide its credentials.
- Client can communicate only if its Wired Equivalent Privacy (WEP) keys match the WEP keys in AP.
- Pro : does not rely on a Remote Authentication Dial-in User Service (RADIUS) server on network.
- Con : any WLAN client can connect to the AP.

Shared Key Authentication

- Shared WEP key is used in a four-step authentication following Challenge-Handshake Authentication Protocol (CHAP).
    - Client sends an authentication request to AP.
    - AP replies with a clear-text challenge.
    - Client encrypts it using the shared key and sends it back in another authentication request
    - AP decrypts and responds.
- After authentication and association, the WEP key is also used for encrypting data.
- Pro : does not rely on a RADIUS server on network.
- Con : since the shared key is used both for CHAP and for data encryption, this is vulnerable to eavesdropping attack and even less secure than open authentication.

MAC Address Authentication

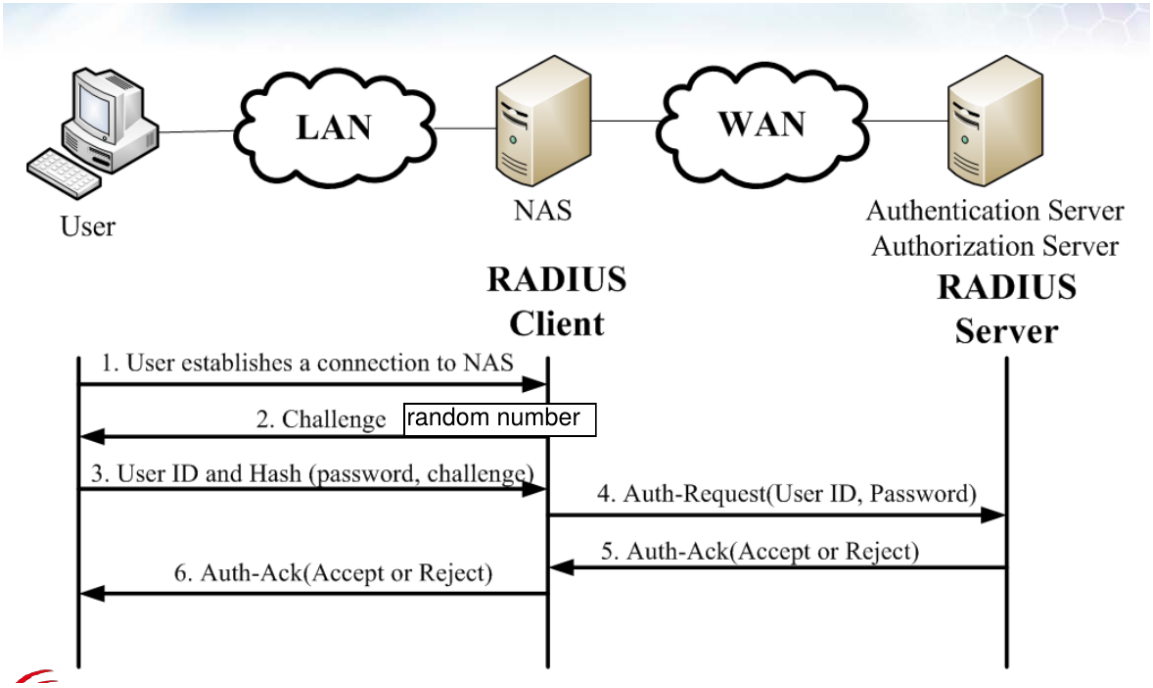
- AP relays client's MAC address to RADIUS server, and RADIUS server checks if it's on the list of allowed MAC addresses.
- Another way is to create a list of allowed MAC addresses on AP.
- Pro : only designated devices have access.
- Con : need to add MAC address manually if new devices want to join the network.

EAP Authentication

- Wireless client device and a RADIUS server on the wired LAN use 802.1x and Extensible Authentication Protocol (EAP) to perform authentication through AP.
- EAP is an authentication framework, not a specific authentication mechanism. There are many types of EAP authentication.
- Pro :
    - Avoid replay attack by using CHAP.
    - Avoid man-in-the-middle attack (MITM) if mutual authentication is used.
    - Avoid traffic-injection attack if re-authentication is used.
    - Safest and widely used.
- Con : overheads at RADIUS server (such as key management and storage).

Below are two types of EAP Authentication mechanism.

One-way Authentication Mechanism

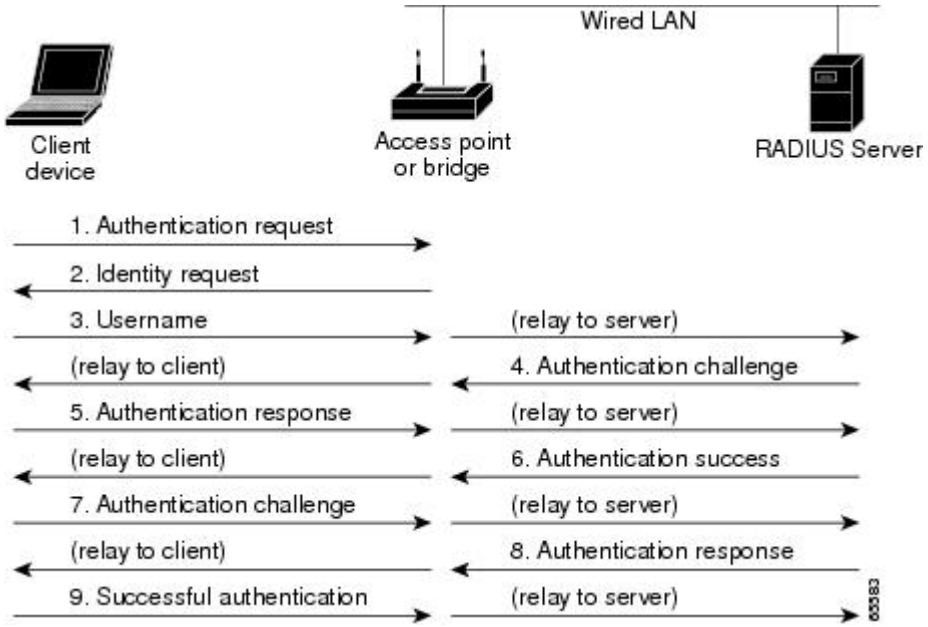


1. The user establishes a connection to NAS.
2. NAS transmits a challenge which is a random number back to the user. The use of a random challenge is to avoid the possibility for a replay attack.
3. The user responds with user ID, password, and the corresponding challenge response.
4. NAS forwards an Authentication Request Packet to the RADIUS Server, containing user identification, encrypted password, and NAS identification.
5. RADIUS server validates and sends back accept or reject.
6. NAS forwards the Authentication Acknowledgement packet to user.

Prevention of replay Attack

- If a malicious person records the exchanged data and retransmits it later, it can disguise that it has correct password and challenge result. This is called replay attack.
- In order to prevent replay attack, NAS uses Challenge–response authentication and periodically send challenges to the user.
- Since challenge varies from time to time, a malicious person can’t replay what he records.

Mutual Authentication Mechanism



- AP relays between client and RADIUS server.
- RADIUS server challenges client first, and then client challenges back.

Prevention of MITM Attack

- An attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.
- Since there is no “safe” channel in wireless network, mutual authentication is the only way to prevent this attack.

WPA/WPA2 instead of WEP

- Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are security protocols designed to replace WEP, strongly increasing the safety of data protection and access control in wireless network.
- Avoid related-key attack by using dynamic keys and longer initialization vector (IV).
- Add message integrity check to prevent an attacker from altering and resending data packets.
- Problems :
    - In some old devices WEP is the default option.
    - Still contains some security issues such as weak password, WPA packet spoofing and decryption, lack of forward secrecy …

References

1. Authentication Types for Wireless Devices
2. Wikipedia: Wired_Equivalent_Privacy
3. Wikipedia: Wi-Fi Protected Access
4. Wikipedia: Challenge–response authentication
5. Wikipedia: Man-in-the-middle attack

Web

1. 說明使用之 web 介面技術。
2. 說明你們設計的網頁的運作方式。

Web interface

- HTML, PHP, JavaScript, MySQL.

Functions of our web

Register

- connect to database by mysqli_connect()
- Get username and password from url by `$_GET`
- Check if the username has already existed
- Insert username, password into radcheck, and also insert username to radusergroup
- Redirect to login page by `header("Refresh: 3;url=$_SERVER[HTTP_REFERER]");`

Login

- Refresh the page and let RADIUS server check whether the username and password are both correct. The server will also check whether the user has exceeded his maximum daily quota. Login will fail if the user fails to meet the requirement.
- If login succeeds, PHP will store username and user data in SESSION for later use.

Logout

- When the user presses the logout button, the URL will be changed and the page will be refreshed. The server will logout the user.

Set max quota, timeout value

- When the user registers its account, a default session time and a maximum quota will be inserted into radreply.
- Note we also need to insert max quota value into radcheck to prevent a user who exceeds his quota from login.
- We count the amount of time the user has used in the front end. If timeout occurs, redirect the user back to login page with `res=timeout` and display timeout.
- We get the amount of quota the user has used by `$_SESSION`. If it exceeds max quota, redirect the user back to login page with `res=exceed` and display exceed.

Display used time

- get the value by `$_SESSION['logintime']`
- calculate the difference between current time and login time
- print it in the front end

Display used quota

- get the value by `$_SESSION['inputoctets']+$_SESSION['outputoctets']`
- print it in the front end

Reference

1. Github chillispot-hotspotlogin-php