

WLAN Security

9. Universal Subscriber Gateway

(C) Herbert Haas 2006/4/1

Content

In this chapter a detailed overview about today's WLAN security problems and solutions are presented.

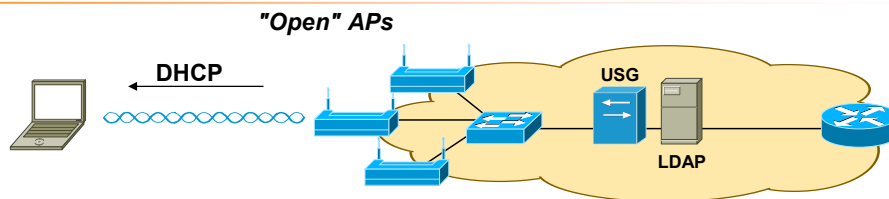
This subchapter provides an introduction into Universal Subscriber Gateways which provide a common and simple method for WLAN authentication.

Objective

After completing this chapter the following tasks could be solved:

- Emphasize the basic vulnerabilities of WLAN
- Explain why WEP is insecure and give a mathematical example
- Compare WEP and TKIP/MIC
- Highlight the design flaws of the WLAN standard authentication
- Explain the design idea of 802.1x
- Compare EAP-TLS, LEAP, PEAP, EAP-TTLS, EAP-FAST with each other and emphasize important security features
- Explain the design concept of WPA and WPA2
- Implement a reliable 802.1x infrastructure over a WAN connection
- List important issues to be considered when choosing a VPN design
- Explain PSPF

Universal Subscriber Gateway (USG)



- **USG catches first HTTP of clients and redirects clients to an authentication page (HTTPS)**
 - ♦ After authentication, client can access the Internet
 - ♦ USG authenticates, authorizes, tracks, and bills users
- **Simple and practical implementation, therefore often used by public service providers**
 - ♦ No authentication settings on APs and clients needed
- **No encryption (!)**
 - ♦ After authentication, eavesdropping of session possible
- **Centralized user management possible (Radius, LDAP)**
- **Might also support 802.1x authentication (typically not used)**

(C) Herbert Haas 2006/4/1

2

A completely different authentication method involves the usage of "**Universal Subscriber Gateways**" (USGs). Here the authentication method is "outsourced" and performed by a layer-4 device which **redirects** any new client to an authentication webpage.

After the client authenticates him-/herself via **HTTPS**, the firewall allows access to the core network or, most often, the Internet.

Using USGs is simple and practical. Clients **do not need to install special 802.1x software drivers** or similar. Any WLAN-device with Web-browser will do. Therefore this method is often implemented by public WLAN service providers. It is often seen in coffee shops or at universities.

The main drawback of this method is that there is **no encryption** supported.

Products: e.g. Nomadix.