

# WLAN Security

## 10. VPN Guidelines

(C) Herbert Haas 2006/4/1

### Content

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

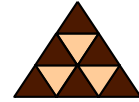
This subchapter provides guidelines for a legacy VPN design for WLANs.

### 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

# IPsec

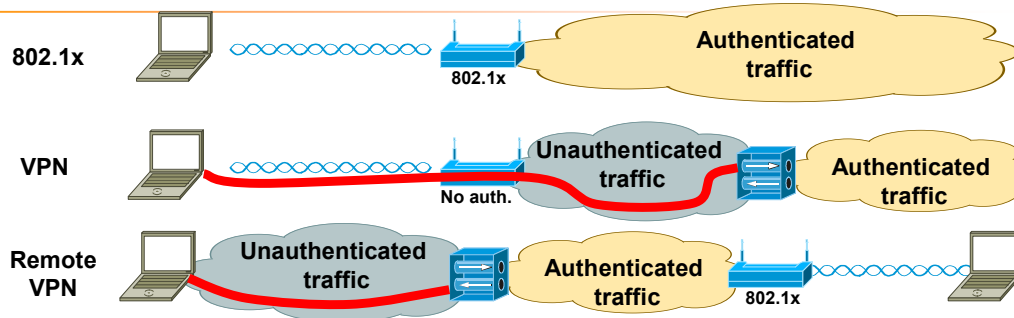
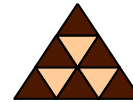


- **Trusted technique but requires open APs (!)**
  - Only remote-access VPN useful—for users in the unprotected guest VLAN
- **Required devices:**
  - Concentrator behind APs
  - VPN clients (SW-based 3DES)
  - DHCP and DNS servers (DoS vulnerability)
- **High WLAN data rates (54 Mbit/s) compared to traditional VPN rates => CPU demanding**
- **Tedious VPN reinitialization during AP roaming**
- **Allow only VPN related protocols (DHCP, DNS, IKE, ESP)**
- **Install firewall software on the WLAN clients—IPsec could be down**
- **Prevent network access if a VPN gateway or RADIUS service fails but consider important production traffic demanding for reliability**

A **VPN solution** is independent on the underlying L1/L2 network and seems appropriate if important clients participate in the unsecured "Guest"-VLAN.

- VPN relies on DNS and DHCP. But DNS and DHCP servers are always vulnerable for DoS. Therefore apply latest patches and OS updates and consider the usage of a host-based IDS (HIDS).
- Consider using dedicated hosts for DHCP and DNS. DoS attacks against the DHCP and DNS services could affect wired users. Network reconnaissance could be performed through the use of DNS queries or reverse-lookups.
- Alternatively consider hard-coding the IP address of the VPN gateway for the VPN clients. If the IP address of the VPN gateway changes, every client will need to update his gateway entry.
- Failure scenarios should be considered: What happens to wireless clients if a VPN gateway or Radius service fails? Typically, a "fuse" concept is implemented, that is, the wireless client heavily depend on the uptime of these central points of failure. If critical production traffic is aggregated via the WLAN, then redundant designs should be discussed.
- Note that WLAN users come with a much higher data rate as traditional wired VPN users who arrive on a WAN link. If many VPN-WLAN users are expected then the CPU load on the VPN concentrator must be controlled.

# VPN Solution



- **Note: only allow WLAN access to VPN-related devices**
  - ◆ DHCP, DNS, and VPN termination device
  - ◆ Consider anti-DoS configuration for DHCP and DNS servers

**Note:** Using a VPN concentrator as authentication and privacy method is typically used as alternative to 802.1x. However, note that any WLAN client can pass the APs and only the VPN concentrator in the network backbone will provide a barrier.

Therefore only use VPN for the guest VLAN to gain secure Internet access. Of course, remote-VPN solutions are always a good idea.