

# WLAN Security

## 11. Guidelines

(C) Herbert Haas 2006/4/1

## Recall

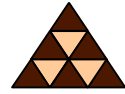


- **Original 802.11 Security is VERY weak**
  - ♦ WEP encryption can be broken within minutes to hours
  - ♦ Shared-key authentication harms more than it helps
  - ♦ Packet integrity can never be protected by a linear function such as CRC
- **Recommended native solutions:**
  - ♦ WPA with TKIP and MIC ideal for legacy devices
  - ♦ Prefer WPAv2 (802.11i) with AES-CCM where possible
  - ♦ Care for strong authentication
    - LEAP – simple but use strong passwords!
    - PEAP – secure if MITM can be prevented (=> PEAPv2)
    - EAP-TLS – secure but 1) username visible and 2) PKI required
    - EAP-FAST – secure but not yet widely supported

(C) Herbert Haas 2006/4/1

2

## Security Guidelines (1)



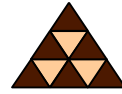
- **Hiding the SSID**
  - ♦ Does NOT provide security
  - ♦ Any WLAN scanner will find every SSID quickly
  - ♦ Nevertheless: if possible try to avoid SSID-broadcasting in beacons ("Guest SSIDs")
  - ♦ Consider "Honeypots"
- **Disable ad-hoc mode on clients**
  - ♦ Even in a well secured wireless network client stations can be a security hole
  - ♦ Consider Network Access Control (NAC) solutions in order to control your clients
- **NEVER use shared key authentication**
  - ♦ Better use open system authentication
  - ♦ Even better combine open auth with 802.1x

## Security Guidelines (2)



- **Enable 802.1x**
  - ♦ For strong mutual authentication and Rogue-AP mitigation
  - ♦ Prefer one of {EAP-FAST, EAP-TLS, PEAP}
  - ♦ If LEAP is needed
    - Ensure good passwords with at least 10 chars (Active Directory settings)
    - Ensure frequent password change (depending on situation)
- **Enable Broadcast Key Rotation**
  - ♦ TKIP and AES will use different session keys for each user
  - ♦ But there can be only a single static key for the broadcast
  - ♦ WPA supports broadcast key "rotation"
    - That is a new key will be generated after certain events (client leaving cell, timer expiration)

## Security Guidelines (3)



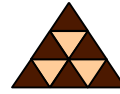
- **HW-based encryption**
  - ◆ Otherwise up to 20% performance impact
  - ◆ TKIP is even more expensive
  - ◆ HW-AES support in all Cisco devices which support 802.11g
- **Protect management interfaces and traffic**
  - ◆ Management VLAN (=untagged) should NOT be reachable via wireless interfaces
  - ◆ Consider IPsec tunnels for RADIUS traffic
- **MAC address filtering**
  - ◆ Only as additional barrier
  - ◆ Actually it requires more administration work than it helps
- **Consider PSPF**
  - ◆ Then APs prevent communication between clients

## Security Guidelines (4)



- **Use IPsec or TLS VPNs:**
  - ◆ If native WLAN solutions cannot be deployed reliably
  - ◆ If a VPN solution is already available
  - ◆ Also mitigates MITM
  - ◆ But if the APs are "open" then DoS attacks might be possible
    - Use firewalls: clients should only reach VPN concentrators, nothing else !!!
    - Best solution is to combine with 802.1x authentication

## Security Guidelines (5)



- **RF jamming**
  - ◆ There are no reliable solutions against it !!!
    - WLAN is a comfortable access network, nothing else
    - Mission critical applications should use the wired network only !!!
  - ◆ Mitigation only involves
    - "Inward-oriented" antennas
    - RF-shielding
      - Expensive and still no 100% solution
- **Enable monitoring**
  - ◆ To detect Rogue APs, scanning devices, DoS attacks, intrusion attacks
    - Consider WLSE, WLSM, etc

## 802.1x and WAN Congestion



- Congestion on WAN links: prioritize 802.1x packets
  - ◆ Otherwise no client can authenticate !!!
- Classify and mark RADIUS packets
  - ◆ E. g. using the Cisco Modular QoS Command Line (MQC)
    - Method to determine the appropriate queue size for the 802.1x/RADIUS packets
    - And to determine how to enable queuing on router interfaces

```
ip access-list extended LEAPACL                               !!! Create ACL for interesting traffic
 permit udp any host 172.24.100.156 eq 1645

class-map match-any LEAPCLASS                                !!! Classify
 match access-group name LEAPACL

policy-map MARKLEAP                                         !!! Specify a policy group
 class LEAPCLASS                                           !!! Corresponds to AF31 (Class=3, l=low drop)
  set ip dscp 26

interface FastEthernet0/0.100                               !!! Attach marker on interface
 encapsulation dot1Q 100
 service-policy input MARKLEAP                               !!! Mark inbound (input) packets only

policy-map LEAPQUEUE                                        !!! 8kb/s if needed (dynamical management)
 class LEAPCLASS
  bandwidth 8

interface Serial3/0:0                                       !!! Attach policy-map on WAN interface
 ip address 172.24.100.66 255.255.255.252
 load-interval 30
 service-policy output LEAPQUEUE
```