Chapter 41
Data Layer

- **Module Data Layer: Subverting Frames**

"Duct tape is like the force. It has a light side, and a dark side, and it holds the universe together."

-- Carl Zwanzig

Copyright Information

- Some rights reserved / Einige Rechte vorbehalten
- Michael Kafka, René Pfeiffer, Sebastian Mayer
  C.a.T. Consulting and Trainings, Vienna, Austria
- You may freely use, distribute and modify this work under following agreement:
- Diese Arbeit darf frei genutzt, verbreitet und bearbeitet werden unter folgenden Bedingungen:

Authors must be referenced (also for modification)
Autoren müssen genannt werden (auch bei Bearbeitung)

Only for non commercial use
Nur für nichtkommerzielle Nutzung

Derivative work under same licence
Derivative Arbeit unter selber Lizenz

creative commons http://www.creativecommons.com

Chapter 41
Data Layer

- Agenda
  - Ethernet & ARP
  - Rogue DHCP Servers
  - Device Discovery
  - Spanning Tree Protocol
  - VLAN Attacks
  - Wireless (802.11☒)

Ethernet & ARP

- **Attacking the Network Glue.**

Address Resolution Protocol

- Address Resolution Protocol (ARP)
  - Matches layer 2 to 3 addresses
  - Can also match layer 3 to 2 addresses
  - Works for different protocols
    - Ethernet, Token Ring, ATM, …
- ARP information is dynamic
  - Hosts keep track by using caches
  - ARP caches can be changed!

ARP Packets

- ARP request
  - *Who has MAC of IP 23.23.23.1?*
- ARP reply
  - *IP 23.23.23.1 is at 00:17:31:91:13:29*
- Gratuitous ARP
  - Send updates to other hosts
  - Useful when links migrate (clusters)
  - Preloading of ARP caches

ARP Spoofing

- Entries in ARP caches expire
- Flooding network with fake ARP packets
  - Announce rogue system to all clients
  - First answer always wins
  - Traffic gets redirected
- Tools ettercap and dsniff, among others

Securing ARP

- Protect local Ethernet segment
- Activate port security
- Use ARP inspection on switches
- Use static ARP cache entries (only for hosts)
- Use sensors for detecting deviations
  - arpwatch
- Deploy DHCP snooping on switches
  - Tracking of hosts
  - Maintaining a list of “clean” MAC/IPs

Rogue DHCP Servers

- All Your Addresses Are Belong To Us.

DHCP Operation

- Dynamic Host Configuration Protocol (DHCP)
  - Autoconfiguration of clients in segments
  - DHCP servers send network parameters
- DHCP relies on layer 2 broadcasts
- DHCP configures
  - Default gateway
  - DNS server(s)
  - other options…
- DHCP leases expire and must be renewed

DHCP Lease Exhaustion

- Send lots of DHCP requests
- Acknowledge every DHCP server reply
- DHCP server runs out of free addresses
  - DHCP unusable
  - Disrupts service (and probably net boots)
- Can be done with a simple client
- Risk: medium Impact: high

Rogue DHCP Servers

- Insert your own DHCP server
  - Publish default gateway and DNS
  - Intercept all DNS queries and traffic
- DHCP servers are active components
  - Detection possible (IDS/IPS)
  - Switches can counter rogue servers
- Risk: high Impact: high

Device Discovery

- **Methods to Identify Network Devices.**

Link Layer Discovery Protocol

- Link Layer Discovery Protocol (LLDC)
  - Vendor neutral layer 2 protocol
  - Allows devices to advertise
    - identity (model, version)
    - capabilities
- IEEE 802.1AB is the formal standard
- LLDC uses *01:80:c2:00:00:0e* for multicast

LLDC Information

- LLDP data units (LLDPDUs) carry
  - IEEE 802.1 management information and
  - IEEE 802.3 media information
- Very useful for topology detection
- Many devices “speak” LLDP
  - Look for implementation bugs
  - LLDP fuzzing tool

Cisco Discovery Protocol (CDP)

- Cisco Discovery Protocol (CDP)
  - Proprietary discovery protocol
  - Uses *01-00-0c-cc-cc-cc* for multicast
- Devices cache CDP information
- *show cdp neighbors* shows other devices
- CDP can be used for detection of
  - topology
  - capabilities
  - versions

CDP Spoofing

- CDP spoofing to impersonate devices
- Useful to gain access to voice VLAN
  - VoIP devices may be CDP-capable
  - CDP packet allows access to voice VLAN
  - CDP ID of phones bypasses 802.1X
- Risk: medium Impact: high

CDP Routing

- On-Demand Routing (ODR) uses CDP
  - CDP transports routing information (prefix)
  - Used for stub networks (hub & spoke)
- ODR routes can be redistributed
  - Export to other routing protocols
- Inserting routes via CDP possible

Spanning Tree Protocol

- **Building and Reconnecting Bridges.**

Spanning Tree Protocol (STP)

- STP allows for loop-free networks
  - Connected bridges elect a root bridge
  - Calculate least cost path to root bridge
  - Disable all other root paths
- STP decides on layer 2 topology
  - Dynamic changes possible
- IEEE 802.1D is the standard for STP
- Rapid STP & Per-VLAN STP also exist

STP Port Status

- STP introduces port status
  - Blocking
  - Listening
  - Learning
  - Forwarding (normal operation)
  - Disabled
- Port status can change

STP Root Bridge

- Every switch assumes root role
- Switches exchange management frames
  - Bridge Protocol Data Units (BPDUs)
  - BPDUs contain bridge ID, port & path
  - Paths are weighted by bandwidth
- Root bridge is logical center of segment

STP Re-Election

- Blocked and disabled ports see BPDUs
  - Needed to detect failed links
  - No authentication
- Injection of suitable BPDUs
  - may trigger new election
  - may change topology
  - may give you r00t (bridge)
- Tools Yersinia or stp-packet

STP Defence

- Disable STP if possible
- Enable port security
- Use one STP process per VLAN
- Enable BPDU guard
- Disable 802.1q signaling for user ports
- Disable auto-trunking
- Gather all unused ports in a special VLAN
- Avoid bugs in your network devices ☺

Virtual LAN Attacks

- **Virtual doesn't mean Secure.**

VLAN Basics

- VLANs logically group network segments
- VLAN modifies the frame headers
  - IEEE 802.1Q
  - Cisco Inter-Switch Link (ISL)
  - 3com Virtual LAN Trunk (VLT)
- Modified frames carry VLAN ID
- VLANs can be
  - static (by port)
  - dynamic (by MAC, port or login)

VLAN Tags

- IEEE 802.1Q adds 16 bit to frame
  - 3 bit priority
  - 1 bit bridging information
  - 12 bit VLAN ID
- VLAN ID 1 is *for management only*
- Double & triple tagging possible

Synchronising VLANs

- All switches need VLAN information
- Trunk ports are VLAN “uplinks”
  - Cisco VLAN Trunking Protocol (VTP)
  - Cisco Dynamic Trunking Protocol (DTP)
  - Other vendors use similar mechanisms
- VTP may operate unauthenticated
- VTP belongs to management segments only

Dynamic Trunking Procotol (DTP)

- Trunking modes on Catalyst switches
  - On (permanent trunking)
  - Off (permanent non-trunking)
  - Desirable (trunk creation wanted)
  - Auto/negotiate (trunking possible if other end is on/desirable)
  - Non-negotiate (no DTP possible)
- Default is *desirable*

DTP Abuse

- DTP offers no authentication
- Send DTP frames to switch port
  - Port in desirable mode creates trunk
  - New trunk may enable packet sniffing
- Best combined with STP attacks
- Risk: medium Impact: high

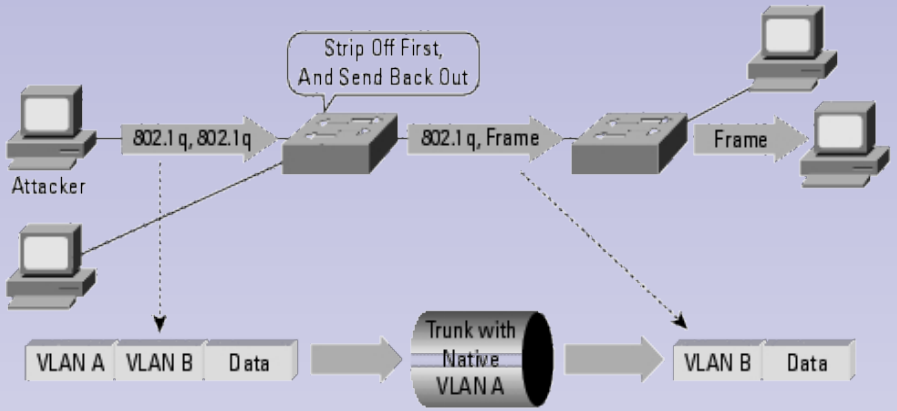
VTP Attacks

- Add rogue switch to VTP domain
  - Create trunk with DTP attack
  - Prepare VTP config with high revision
  - Revision number forces updates
- Modification of VLANs possible
- Risk: medium Impact: high

Switch Spoofing

- Insert device/software that knows
  - tagging protocols
  - trunking protocols
- VLAN information can be decoded
- Frames can be intercepted/rerouted

Double Encapsulation Attack



Note: Only Works if Trunk Has the Same Native VLAN as the Attacker.

Wireless (802.11☒)

- **Managing Wireless Frames**

802.11☒ Protocol Family

- 802.11b is famous “WLAN standard”
- 802.11g is faster
- 802.11n is very cool ☺
- WLAN is more complex than that
  - Frequency modulations & signal loss
  - Roaming / handover
  - Authentication & encryption

Components

- Aerials (mandatory for every member)
- Clients (with WLAN adapter)
- Access points (APs)
  - Relay between wired/wireless worlds
  - Can act as repeater
  - Can act as arbitrator for clients
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
  - Ethernet uses CSMA/CD

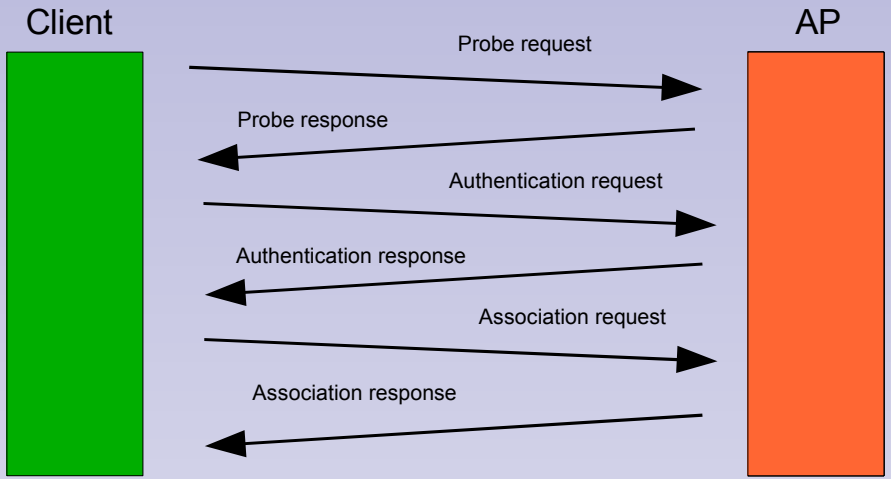
Wireless Modes

- ad-hoc mode
  - Peer-to-peer connection
  - Direct connectivity
- AP mode
  - AP provides connectivity
  - AP requires NIC association

Frame Types

- Control frames
  - Request to send, clear to send, ack
- Management frames
  - Association/Deassociation/Reassociation
  - Authentication/Deauthentication
  - Beacon frames
  - Probes
- Data frames

Authentication/Association



Wireless Encryption Protocol (WEP)

- Adds encryption and integrity
  - Stream cipher RC4
  - CRC-32 checksum
- Pre-shared keys
  - 40 or 104 bit key
  - 24 bit initialisation vector (IV)

WEP Initialisation

- Open System authentication
  - Client authenticates & associates
  - Client must have correct key
- Shared Key authentication
  - Client sends authentication request
  - AP send clear-text challenge
  - Client must encrypt clear-text
  - AP decrypts and compares message
- Open System authentication more “secure”

WEP is Weak

- Multiple attacks on WEP known
  - IV too small (statistical attacks)
  - No cryptographic integrity protection
  - Traffic injection possible
- WEP offers minimal to no protection
  - Can't be fixed
  - Don't lean on WEP for security

Enhanced Wireless Security

- Wi-Fi Protected Access
  - WPA, WPA2 or IEEE 802.11i
  - Dynamically changing WEP keys (TKIP)
  - Better encryption (AES)
  - Integrity check (MIC)
- Extensible Authentication Protocol (EAP)
  - EAP-TLS, EAP-TTLS, PEAP, EAP-SIM, ...
  - IEEE 802.1X for wireless netsworks

Standard Confusion

- Vendors were quicker than standards work groups
- A short summary:
  - IEEE 802.11i defines wireless security
  - WPA = IEEE 802.11i - AES
  - WPA2 = IEEE 802.11i + AES
  - WPA2 is approved by Wi-Fi Alliance

802.11i Authentication

- AP authenticates to user and vice versa
- Authentication by Pre-Shared Key (PSK)
- Authentication by EAP
  - APs relay requests
  - Authentication servers handle requests
  - RADIUS is common
- Use of certificates possible (EAP-TLS)

802.11i Encryption

- 802.11i introduces key hierarchy
  - Pairwise Master Key (PMK) for sessions
  - Pairwise Transient Key (PTK)
  - TKIP uses 4 additional keys
  - CCMP uses 3 additional keys
- PTK contains temporal key

802.11i Integrity

- Message Integrity Check (MIC)
  - Message Authentication Code
  - Hash of packet and temporal key
  - Encrypted in frame
- Replay protection
  - Serial number added to frames
  - Last *n* packets will be processed (*n*≈16)
  - Not encrypted in frame

Rogue Access Points

- Mimic authentic AP
  - Copy ESSID, use no authentication
  - Provide strong signal
- KARMA tools provide framework
  - AP-in-the-middle mit DHCP
  - Detects active ESSIDs and offers them
  - Redirects DNS, FTP, POP3 & HTTP traffic
- Risk: medium Impact: high

RTS/CTS Attack

- Management frames are not encrypted
- Client prepares to send large packet
  - Client sends *Request To Send* to AP
  - AP agrees by *Clear To Send* reply
  - CTS prevents every device from sending
- Disable connectivity
  - Flood network with CTS
  - Flood AP with RTS
- Risk: low Impact: high

Dictionary Attack

- Use dictionaries and guess PMK
- PMK depends on PSK and SSID
  - PSK is hashed 4096 times
  - SSID varies hashes
- Capture WPA handshakes and brute-force
  - cowpatty
  - aircrack-ng (works for WEP too)
- Avoid PSK or change often
- Risk: medium Impact: high

Attacking LEAP

- Lightweight EAP (LEAP)
  - Cisco proprietary, older than WPA
- LEAP is based on MS-CHAP-v2
  - NT hash & 3DES cryptography
  - Usernames & passwords
- Attack similar to WEP
  - Tool asleap
- Risk: medium Impact: high

Attacking EAP-TLS

- EAP-TLS is pretty secure
  - Strong cryptography
  - Certificates and client keys
  - Unique PMKs, no sniffing possible
- Steal certificate and key
  - Configure client to use them
  - Enter network and deploy other attacks
- Risk: low Impact: high

Attacking PEAP/EAP-TTLS

- Use TLS tunnel as encapsulation
- TLS tunnel is created without authentication
- PMK is derived from this TLS tunnel
- Attacker can act as MITM
  - Mimic AP operation
  - Confirm victim's authentication
  - Offer fake certificate
- Client must verify certificate to avoid this
- Risk: low Impact: high

Attacking RADIUS

- RADIUS delivers PMK to AP
- RADIUS secret is MD5 hash
  - RADIUS secret protects PMK and
  - authenticates messages to/from AP
- Try dictionary attack on MD5 hash
  - Game's over if attacker can choose PMK
- Protect RADIUS servers
- Protect RADIUS↔AP communication

ATA over Ethernet (AoE)

- **And Now For Something Completely Different...**

SAN in Layer 2

- AoE packs ATA commands in frames
  - IEEE 802.3 type 0x88A2
  - No protocol overhead
- AoE is stateless
- AoE offers no security mechanisms
  - Replay attacks possible
  - Access to segment sufficient
  - Read/write access to block devices
- AoE security assessment

Module 41
Data Layer

- Summary
  - Layer 2 is critical for infrastructure.
  - Securing data layer is as critical.
  - Denying attacks early supports security in upper layers.

Thank You

- Questions?

Chapter 41
Data Layer

- **Module Data Layer: Subverting Frames**

DeepSec Vienna 2007
7 Layers of Insecurity

"Duct tape is like the force. It has a light side, and a dark side, and it holds the universe together."

-- Carl Zwanzig

Copyright Information

- Some rights reserved / Einige Rechte vorbehalten
- Michael Kafka, René Pfeiffer, Sebastian Mayer
  C.a.T. Consulting and Trainings, Vienna, Austria
- You may freely use, distribute and modify this work under following agreement:
- Diese Arbeit darf frei genutzt, verbreitet und bearbeitet werden unter folgenden Bedingungen:

Authors must be referenced (also for modification)
Autoren müssen genannt werden (auch bei Bearbeitung)

Only for non commercial use
Nur für nichtkommerzielle Nutzung

Derivative work under same licence
Derivative Arbeit unter selber Lizenz

creative commons http://www.creativecommons.com

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 41 - Data Layer 2

This presentation is published under the CreativeCommons License which can be viewed in detail on their hompage: http://creativecommons.org/licenses/by-nc-sa/2.0/at/

Read more on http://www.creativecommons.com

You are free:

to Share — to copy, distribute and transmit the work

to Remix — to adapt the work

Under the following conditions:

Attribution. You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Noncommercial. You may not use this work for commercial purposes.

Share Alike. If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

- **For any reuse or distribution, you must make clear to others the license terms of this work. The best way to do this is with a link to this web page.**
- **Any of the above conditions can be waived if you get permission from the copyright holder.**
- **Nothing in this license impairs or restricts the author's moral rights.**

Chapter 41
Data Layer

- Agenda
  - Ethernet & ARP
  - Rogue DHCP Servers
  - Device Discovery
  - Spanning Tree Protocol
  - VLAN Attacks
  - Wireless (802.11☒)

DeepSec Vienna 2007
7 Layers of Insecurity

The ☒ in 802.11☒ indicates the whole family of protocols connected with the wireless standards. We did use a special symbol since a lot of letters where used and we'll probably see 802.11a to 802.11z provided the pace at which standards are defined continues.

Ethernet & ARP

- Attacking the Network Glue.

DeepSec Vienna 2007
7 Layers of Insecurity

Address Resolution Protocol

- Address Resolution Protocol (ARP)
  - Matches layer 2 to 3 addresses
  - Can also match layer 3 to 2 addresses
  - Works for different protocols
    - Ethernet, Token Ring, ATM, …
- ARP information is dynamic
  - Hosts keep track by using caches
  - ARP caches can be changed!

DeepSec Vienna 2007
7 Layers of Insecurity

ARP Packets

- ARP request
  - *Who has MAC of IP 23.23.23.1?*
- ARP reply
  - *IP 23.23.23.1 is at 00:17:31:91:13:29*
- Gratuitous ARP
  - Send updates to other hosts
  - Useful when links migrate (clusters)
  - Preloading of ARP caches

DeepSec Vienna 2007
7 Layers of Insecurity

ARP Spoofing

- Entries in ARP caches expire
- Flooding network with fake ARP packets
  - Announce rogue system to all clients
  - First answer always wins
  - Traffic gets redirected
- Tools ettercap and dsniff, among others

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 41 - Data Layer 7

Ettercap allows for “port stealing” in a switched environment by using specially crafted ARP packets. The authors of the software describe the techniques in their presentation slides (showed at Black Hat 2003).

Securing ARP

- Protect local Ethernet segment
- Activate port security
- Use ARP inspection on switches
- Use static ARP cache entries (only for hosts)
- Use sensors for detecting deviations
  - arpwatch
- Deploy DHCP snooping on switches
  - Tracking of hosts
  - Maintaining a list of “clean” MAC/IPs

DeepSec Vienna 2007
7 Layers of Insecurity

Important note: Some OS variants allow ARP packets to overwrite static ARP entries. Therefore static ARP entries should be taken with a grain of salt. Make sure your network code really does what you expect it to do.

Rogue DHCP Servers

- All Your Addresses Are Belong To Us.

DeepSec Vienna 2007
7 Layers of Insecurity

DHCP Operation

- Dynamic Host Configuration Protocol (DHCP)
  - Autoconfiguration of clients in segments
  - DHCP servers send network parameters
- DHCP relies on layer 2 broadcasts
- DHCP configures
  - Default gateway
  - DNS server(s)
  - other options…
- DHCP leases expire and must be renewed

DeepSec Vienna 2007
7 Layers of Insecurity

DHCP traffic can be transported between broadcast domains by use of DHCP Relay Agents on routers. These relay agents may increase the attack surface of DHCP servers assumed to be confined to Ethernet segments.

DHCP Lease Exhaustion

- Send lots of DHCP requests
- Acknowledge every DHCP server reply
- DHCP server runs out of free addresses
  - DHCP unusable
  - Disrupts service (and probably net boots)
- Can be done with a simple client
- Risk: medium Impact: high

DeepSec Vienna 2007
7 Layers of Insecurity

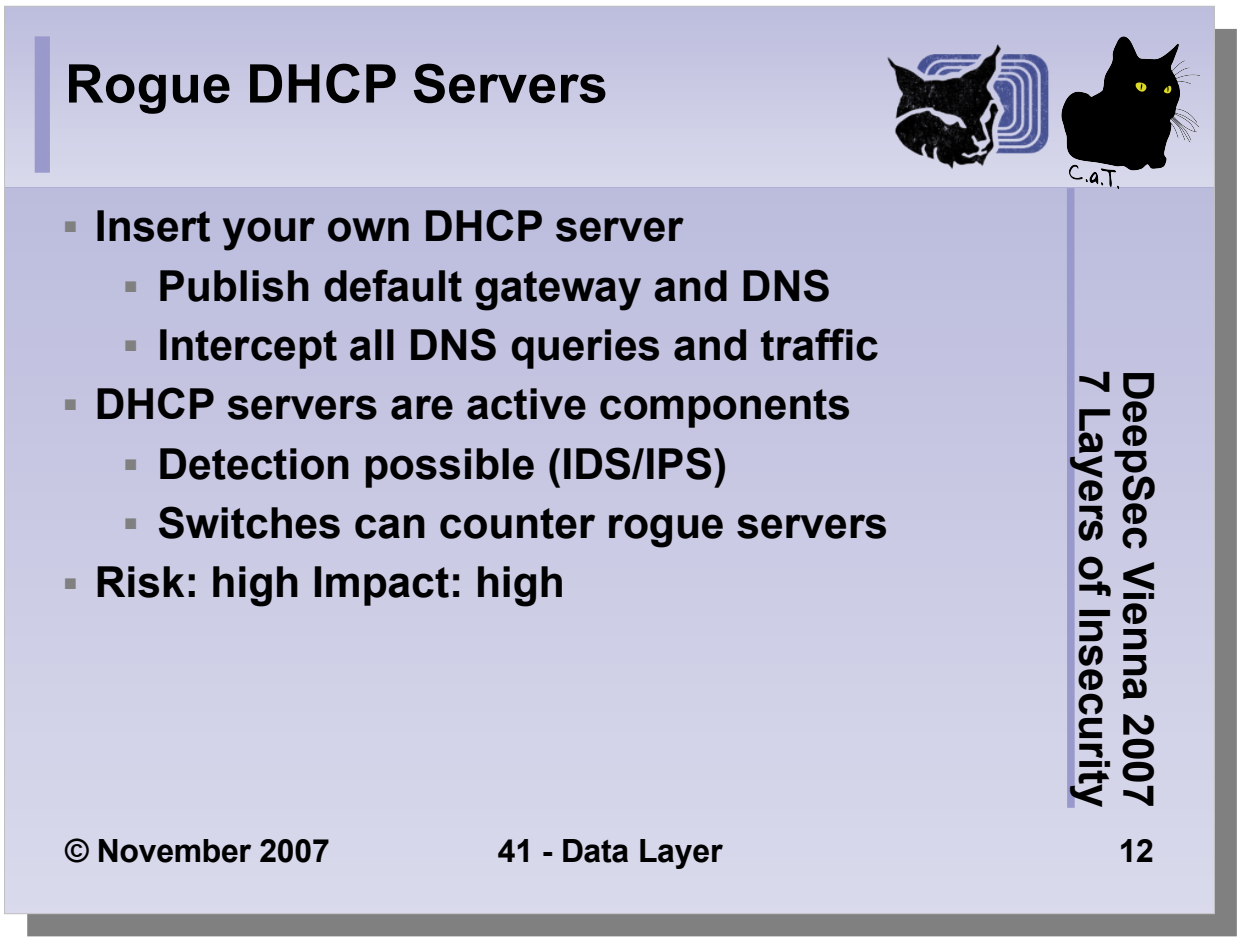
Mitigation:

• Monitor DHCP activity.

• Isolate guest networks from internal/production networks, use different DHCP servers for every network.

• Use suitable short lease times for dynamic address pools.

• Use reserved DHCP entries with static MAC address for important clients.



Mitigation:

• IDS/IPS can detect DHCP server signatures and alert administration.

• Software tools exists in order to scan for DHCP servers (dhcp_probe for UNIX® systems, dhcploc.exe from the Microsoft® Windows® Resource Kit)

• Multilayer switches can also detect and counter rogue DHCP servers (depending on vendor and firmware).

Device Discovery

- **Methods to Identify Network Devices.**

DeepSec Vienna 2007
7 Layers of Insecurity

Link Layer Discovery Protocol

- Link Layer Discovery Protocol (LLDC)
  - Vendor neutral layer 2 protocol
  - Allows devices to advertise
    - identity (model, version)
    - capabilities
- IEEE 802.1AB is the formal standard
- LLDC uses *01:80:c2:00:00:0e* for multicast

DeepSec Vienna 2007
7 Layers of Insecurity

LLDC Information

- LLDP data units (LLDPDUs) carry
  - IEEE 802.1 management information and
  - IEEE 802.3 media information
- Very useful for topology detection
- Many devices “speak” LLDP
  - Look for implementation bugs
  - LLDP fuzzing tool

DeepSec Vienna 2007
7 Layers of Insecurity

Cisco Discovery Protocol (CDP)

- Cisco Discovery Protocol (CDP)
  - Proprietary discovery protocol
  - Uses *01-00-0c-cc-cc-cc* for multicast
- Devices cache CDP information
- *show cdp neighbors* shows other devices
- CDP can be used for detection of
  - topology
  - capabilities
  - versions

DeepSec Vienna 2007
7 Layers of Insecurity

CDP Spoofing

- CDP spoofing to impersonate devices
- Useful to gain access to voice VLAN
  - VoIP devices may be CDP-capable
  - CDP packet allows access to voice VLAN
  - CDP ID of phones bypasses 802.1X
- Risk: medium Impact: high

DeepSec Vienna 2007
7 Layers of Insecurity

The CDP spoofing vulnerability was published by FishNet Security in 2005. They tested Cisco IOS and CatOS versions in combination with a VoIP setup consisting of CDP-capable IP telephones.

Mitigation:

• Disable all unused ports.

• Use VLAN for separation of networked devices (especially for VoIP equipment).

• Disable all administrative access from the LAN side.

• Use access lists or filters in order to enforce intended flow of data between networks.

• Use cryptographically secure management protocols if possible.

CDP Routing

- On-Demand Routing (ODR) uses CDP
  - CDP transports routing information (prefix)
  - Used for stub networks (hub & spoke)
- ODR routes can be redistributed
  - Export to other routing protocols
- Inserting routes via CDP possible

DeepSec Vienna 2007
7 Layers of Insecurity

Spanning Tree Protocol

- Building and Reconnecting Bridges.

DeepSec Vienna 2007
7 Layers of Insecurity

Spanning Tree Protocol (STP)

- STP allows for loop-free networks
  - Connected bridges elect a root bridge
  - Calculate least cost path to root bridge
  - Disable all other root paths
- STP decides on layer 2 topology
  - Dynamic changes possible
- IEEE 802.1D is the standard for STP
- Rapid STP & Per-VLAN STP also exist

DeepSec Vienna 2007
7 Layers of Insecurity

STP Port Status

- STP introduces port status
  - Blocking
  - Listening
  - Learning
  - Forwarding (normal operation)
  - Disabled
- Port status can change

DeepSec Vienna 2007
7 Layers of Insecurity

STP Root Bridge

- Every switch assumes root role
- Switches exchange management frames
  - Bridge Protocol Data Units (BPDUs)
  - BPDUs contain bridge ID, port & path
  - Paths are weighted by bandwidth
- Root bridge is logical center of segment

DeepSec Vienna 2007
7 Layers of Insecurity

STP Re-Election

- Blocked and disabled ports see BPDUs
  - Needed to detect failed links
  - No authentication
- Injection of suitable BPDUs
  - may trigger new election
  - may change topology
  - may give you r00t (bridge)
- Tools Yersinia or stp-packet

DeepSec Vienna 2007
7 Layers of Insecurity

The tools Yersinia and stp-packet give you the possibility to inject crafted BPDUs. The packets must be created manually and must fit into the existing topology in terms of bridge IDs.

STP Defence

- Disable STP if possible
- Enable port security
- Use one STP process per VLAN
- Enable BPDU guard
- Disable 802.1q signaling for user ports
- Disable auto-trunking
- Gather all unused ports in a special VLAN
- Avoid bugs in your network devices ☺

DeepSec Vienna 2007
7 Layers of Insecurity

Virtual LAN Attacks

- Virtual doesn't mean Secure.

DeepSec Vienna 2007
7 Layers of Insecurity

VLAN Basics

- VLANs logically group network segments
- VLAN modifies the frame headers
  - IEEE 802.1Q
  - Cisco Inter-Switch Link (ISL)
  - 3com Virtual LAN Trunk (VLT)
- Modified frames carry VLAN ID
- VLANs can be
  - static (by port)
  - dynamic (by MAC, port or login)

DeepSec Vienna 2007
7 Layers of Insecurity

VLAN Tags

- IEEE 802.1Q adds 16 bit to frame
  - 3 bit priority
  - 1 bit bridging information
  - 12 bit VLAN ID
- VLAN ID 1 is *for management only*
- Double & triple tagging possible

DeepSec Vienna 2007
7 Layers of Insecurity

Synchronising VLANs

- All switches need VLAN information
- Trunk ports are VLAN “uplinks”
  - Cisco VLAN Trunking Protocol (VTP)
  - Cisco Dynamic Trunking Protocol (DTP)
  - Other vendors use similar mechanisms
- VTP may operate unauthenticated
- VTP belongs to management segments only

DeepSec Vienna 2007
7 Layers of Insecurity

VLAN configuration tips can be found in the following publications.

- Article about VLAN security by Rik Farrow.
- Configuration Examples Related to VLAN Features on Cisco's web site.
- Virtual LAN Security by Steve A. Rouiller, Black Hat conference 2004.
- Hacking Layer 2 - Fun With Ethernet Switches by Sean Convery.

Dynamic Trunking Procotol (DTP)

- Trunking modes on Catalyst switches
  - On (permanent trunking)
  - Off (permanent non-trunking)
  - Desirable (trunk creation wanted)
  - Auto/negotiate (trunking possible if other end is on/desirable)
  - Non-negotiate (no DTP possible)
- Default is *desirable*

DeepSec Vienna 2007
7 Layers of Insecurity

DTP Abuse

- DTP offers no authentication
- Send DTP frames to switch port
  - Port in desirable mode creates trunk
  - New trunk may enable packet sniffing
- Best combined with STP attacks
- Risk: medium Impact: high

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 41 - Data Layer 30

Mitigation:

• Disable autotrunking on switch ports.

• Disable unused switch ports.

• Use dedicated VLAN IDs for trunking ports.

VTP Attacks

- Add rogue switch to VTP domain
  - Create trunk with DTP attack
  - Prepare VTP config with high revision
  - Revision number forces updates
- Modification of VLANs possible
- Risk: medium Impact: high

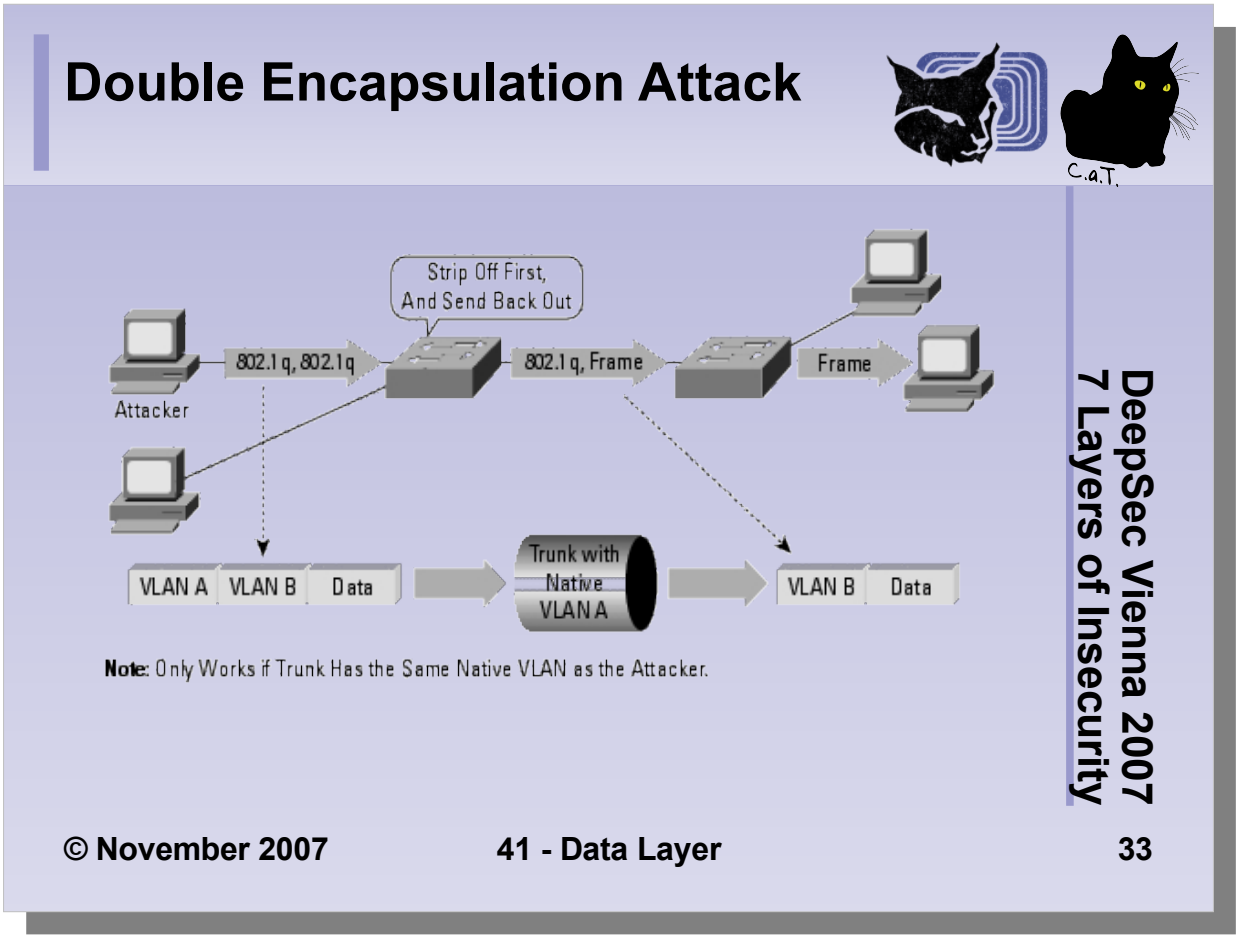
DeepSec Vienna 2007
7 Layers of Insecurity

The mitigation of these attacks is the same as for DTP attacks. The guidelines apply to standard administration tasks as well. Be very careful when inserting new switches into your existing configuration.

Switch Spoofing

- Insert device/software that knows
  - tagging protocols
  - trunking protocols
- VLAN information can be decoded
- Frames can be intercepted/rerouted

DeepSec Vienna 2007
7 Layers of Insecurity



The graphics shows the double encapsulation attack. The attacker creates Ethernet frames with two VLAN tags and sends them to a switch. The switch strips the first tag and forwards the frame to the VLAN indicated by the second tag. The attack only works if the trunk has the same VLAN ID as the attacker.

Wireless (802.11☒)

- **Managing Wireless Frames**

DeepSec Vienna 2007
7 Layers of Insecurity

802.11☒ Protocol Family

- 802.11b is famous “WLAN standard”
- 802.11g is faster
- 802.11n is very cool ☺
- WLAN is more complex than that
  - Frequency modulations & signal loss
  - Roaming / handover
  - Authentication & encryption

DeepSec Vienna 2007
7 Layers of Insecurity

Components

- Aerials (mandatory for every member)
- Clients (with WLAN adapter)
- Access points (APs)
  - Relay between wired/wireless worlds
  - Can act as repeater
  - Can act as arbitrator for clients
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
  - Ethernet uses CSMA/CD

DeepSec Vienna 2007
7 Layers of Insecurity

Wireless Modes

- ad-hoc mode
  - Peer-to-peer connection
  - Direct connectivity
- AP mode
  - AP provides connectivity
  - AP requires NIC association

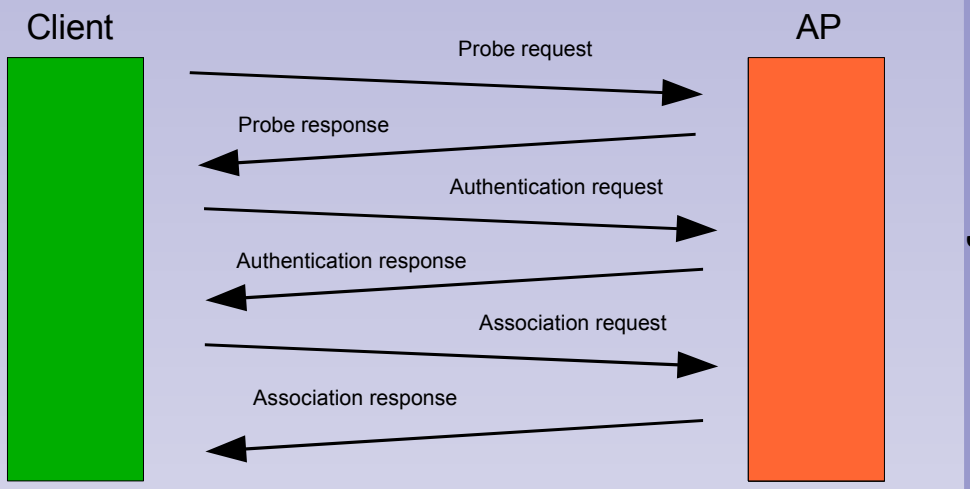
DeepSec Vienna 2007
7 Layers of Insecurity

Frame Types

- Control frames
  - Request to send, clear to send, ack
- Management frames
  - Association/Deassociation/Reassociation
  - Authentication/Deauthentication
  - Beacon frames
  - Probes
- Data frames

DeepSec Vienna 2007
7 Layers of Insecurity

Authentication/Association



DeepSec Vienna 2007
7 Layers of Insecurity

Wireless Encryption Protocol (WEP)

- Adds encryption and integrity
  - Stream cipher RC4
  - CRC-32 checksum
- Pre-shared keys
  - 40 or 104 bit key
  - 24 bit initialisation vector (IV)

DeepSec Vienna 2007
7 Layers of Insecurity

WEP Initialisation

- Open System authentication
  - Client authenticates & associates
  - Client must have correct key
- Shared Key authentication
  - Client sends authentication request
  - AP send clear-text challenge
  - Client must encrypt clear-text
  - AP decrypts and compares message
- Open System authentication more “secure”

DeepSec Vienna 2007
7 Layers of Insecurity

The shared key authentication has a major drawback. Provided an attacker can capture the packet exchange used for authentication, then two out of three pieces of information of the whole WEP security is known. The packets contain the clear text challenge string and what the challenge string looks like after it has been encrypted. Together with the RC4 encryption algorithm the attacker can deduce the shared authentication key which in turn is used for WEP itself.

Authentication type and WEP

WEP is Weak

- Multiple attacks on WEP known
  - IV too small (statistical attacks)
  - No cryptographic integrity protection
  - Traffic injection possible
- WEP offers minimal to no protection
  - Can't be fixed
  - Don't lean on WEP for security

DeepSec Vienna 2007
7 Layers of Insecurity

Enhanced Wireless Security

- Wi-Fi Protected Access
  - WPA, WPA2 or IEEE 802.11i
  - Dynamically changing WEP keys (TKIP)
  - Better encryption (AES)
  - Integrity check (MIC)
- Extensible Authentication Protocol (EAP)
  - EAP-TLS, EAP-TTLS, PEAP, EAP-SIM, ...
  - IEEE 802.1X for wireless netsworks

DeepSec Vienna 2007
7 Layers of Insecurity

Standard Confusion

- Vendors were quicker than standards work groups
- A short summary:
  - IEEE 802.11i defines wireless security
  - WPA = IEEE 802.11i - AES
  - WPA2 = IEEE 802.11i + AES
  - WPA2 is approved by Wi-Fi Alliance

DeepSec Vienna 2007
7 Layers of Insecurity

802.11i Authentication

- AP authenticates to user and vice versa
- Authentication by Pre-Shared Key (PSK)
- Authentication by EAP
  - APs relay requests
  - Authentication servers handle requests
  - RADIUS is common
- Use of certificates possible (EAP-TLS)

DeepSec Vienna 2007
7 Layers of Insecurity

802.11i Encryption

- 802.11i introduces key hierarchy
  - Pairwise Master Key (PMK) for sessions
  - Pairwise Transient Key (PTK)
  - TKIP uses 4 additional keys
  - CCMP uses 3 additional keys
- PTK contains temporal key

DeepSec Vienna 2007
7 Layers of Insecurity

802.11i tries to minimally expose the PMK, because this key lasts for the whole session. The PTK is generated from PMK, AP nonce (ANonce), STA nonce (SNonce), AP MAC address and STA MAC address. All pieces are then processed by a cryptographic hash function. The generated PTK is then divided into 5 separate keys.

• 16 bytes of EAPOL-Key Encryption Key (KEK) – the AP uses this key to encrypt additional data sent to the client

• 16 bytes of EAPOL-Key Confirmation Key (KCK) – used to compute MIC on WPA EAPOL Key message

• 16 bytes of Temporal Key (TK) – used to encrypt/decrypt Unicast data packets

• 8 bytes of Michael MIC Authenticator Tx Key – used to compute MIC on unicast data packets transmitted by the AP

• 8 bytes of Michael MIC Authenticator Rx Key – used to compute MIC on unicast data packets transmitted by the station

802.11i Integrity

- Message Integrity Check (MIC)
  - Message Authentication Code
  - Hash of packet and temporal key
  - Encrypted in frame
- Replay protection
  - Serial number added to frames
  - Last *n* packets will be processed (*n*≈16)
  - Not encrypted in frame

DeepSec Vienna 2007
7 Layers of Insecurity

Rogue Access Points

- Mimic authentic AP
  - Copy ESSID, use no authentication
  - Provide strong signal
- KARMA tools provide framework
  - AP-in-the-middle mit DHCP
  - Detects active ESSIDs and offers them
  - Redirects DNS, FTP, POP3 & HTTP traffic
- Risk: medium Impact: high

DeepSec Vienna 2007
7 Layers of Insecurity

Mitigation:

• Regularly conduct wireless sniffing in order to verify access point deployment and signal strength.

• Verify AP's MAC address, configuration, vendor string and firmware.

• Use 802.1X technology in order to control access of wireless network.

RTS/CTS Attack

- Management frames are not encrypted
- Client prepares to send large packet
  - Client sends *Request To Send* to AP
  - AP agrees by *Clear To Send* reply
  - CTS prevents every device from sending
- Disable connectivity
  - Flood network with CTS
  - Flood AP with RTS
- Risk: low Impact: high

DeepSec Vienna 2007
7 Layers of Insecurity

Mitigation:

• Monitor wireless network for signal strength.

• Use network adapters that don't use the CTS/RTS frame sequence.

• Configure access points not to use the CTS/RTS frame sequence.

• Authenticate RTS/CTS frames (requires firmware/vendor/driver support).

The RTS/CTS mechanism is solely used to overcome the *hidden node problem.* If your network coverage is tightly controlled and you have a good deployment of access points, then RTS/CTS are not necessary.

Dictionary Attack

- Use dictionaries and guess PMK
- PMK depends on PSK and SSID
  - PSK is hashed 4096 times
  - SSID varies hashes
- Capture WPA handshakes and brute-force
  - cowpatty
  - aircrack-ng (works for WEP too)
- Avoid PSK or change often
- Risk: medium Impact: high

DeepSec Vienna 2007
7 Layers of Insecurity

Mitigation:

• Avoid using PSK configuration.

• Use 802.1X authentication or X.509 certificates.

• Monitor wireless traffic and look for signatures of deauthentication and increased ARP activity.

Attacking LEAP

- Lightweight EAP (LEAP)
  - Cisco proprietary, older than WPA
- LEAP is based on MS-CHAP-v2
  - NT hash & 3DES cryptography
  - Usernames & passwords
- Attack similar to WEP
  - Tool asleap
- Risk: medium Impact: high

DeepSec Vienna 2007
7 Layers of Insecurity

Mitigation:

• Use strong password policy and periodically change user passwords.

• Migrate to EAP-TLS (RFC 2716), EAP-FAST (RFC 4851) or PEAP (Protected Extensible Authentication Protocol).

Attacking EAP-TLS

- EAP-TLS is pretty secure
  - Strong cryptography
  - Certificates and client keys
  - Unique PMKs, no sniffing possible
- Steal certificate and key
  - Configure client to use them
  - Enter network and deploy other attacks
- Risk: low Impact: high

DeepSec Vienna 2007
7 Layers of Insecurity

Mitigation:

- Make sure that you have a properly deployed PKI.
- Harden and protect client systems.
- Instruct users to be careful when certificate validation fails.
- Revoke certificates immediately after client systems are compromised or lost.

Attacking PEAP/EAP-TTLS

- Use TLS tunnel as encapsulation
- TLS tunnel is created without authentication
- PMK is derived from this TLS tunnel
- Attacker can act as MITM
  - Mimic AP operation
  - Confirm victim's authentication
  - Offer fake certificate
- Client must verify certificate to avoid this
- Risk: low Impact: high

DeepSec Vienna 2007
7 Layers of Insecurity

Mitigation:

• Requires a server-side PKI deployment (although not for the client systems as with EAP-TLS).

• MITM attacks are harder but still possible in certain circumstances.

Attacking RADIUS

- RADIUS delivers PMK to AP
- RADIUS secret is MD5 hash
  - RADIUS secret protects PMK and
  - authenticates messages to/from AP
- Try dictionary attack on MD5 hash
  - Game's over if attacker can choose PMK
- Protect RADIUS servers
- Protect RADIUS↔AP communication

DeepSec Vienna 2007
7 Layers of Insecurity

ATA over Ethernet (AoE)

- And Now For Something Completely Different...

DeepSec Vienna 2007
7 Layers of Insecurity

SAN in Layer 2

- AoE packs ATA commands in frames
  - IEEE 802.3 type 0x88A2
  - No protocol overhead
- AoE is stateless
- AoE offers no security mechanisms
  - Replay attacks possible
  - Access to segment sufficient
  - Read/write access to block devices
- AoE security assessment

DeepSec Vienna 2007
7 Layers of Insecurity

AoE is a typical internal protocol and is part of the infrastructure. It is not designed to provide strong protection. This is true for other protocols used for providing direct access to resources with low overhead (i.e. no protection).

Mitigation:

• Tightly limit access to network segments that have AoE traffic.

Module 41
Data Layer

- Summary
  - Layer 2 is critical for infrastructure.
  - Securing data layer is as critical.
  - Denying attacks early supports security in upper layers.

DeepSec Vienna 2007
7 Layers of Insecurity

Thank You

- Questions?

DeepSec Vienna 2007
7 Layers of Insecurity