Chapter 31
Hardware Hacking

- **Module Hardware Hacking: Turning Ethernet into Æthernet**

“Taps are used in security applications because they are non-obtrusive, are not detectable on the network,…”

(Wikipedia.org)

DeepSec Vienna 2007
7 Layers of Insecurity

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

Chapter 31
Hardware Hacking

- Agenda
  - Wire Tapping
  - Modifying Network Devices
  - Access to Network Hardware
  - Wireless Networks

DeepSec Vienna 2007
7 Layers of Insecurity

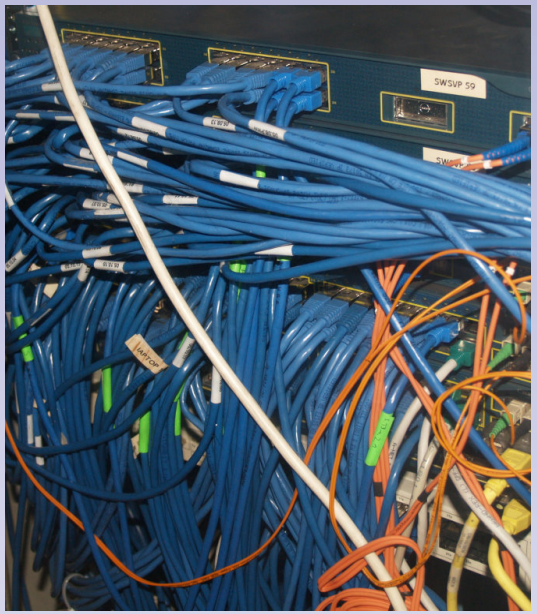
Layer 1 Basics

- But my Network Hardware is behind locked Doors, isn't it?

Layer 1 Basics

- Ashes to ashes, bits to bits
  - Basically we deal with 0 and 1
  - Electronically we have signals
- Access to wiring is crucial
  - Devices access wires for us
- Thin air provides access to wireless networks

Layer 1 View



Can you spot the rogue port or wire?

Is your cabling longer than it should be?

Layer 1 Organisation

- Know your cabling closet
  - Know every port
  - Know every connected device
- Know every aerial for wireless networks
- Disable unused segments
  - Disabling means “0 volts”
  - No stand-by mode

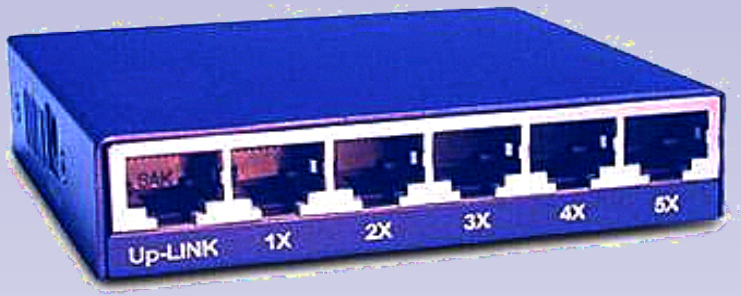
Network Taps

- Thick Ethernet uses taps by design
- Network taps exist for
  - FDDI
  - ATM
  - Ethernet
- Full duplex can be a problem
- Mirror ports (are in layer 2)

Tap Gallery

Network tap for optical connection

Rogue Hub



Tap-like Intrusions

- Small hubs
  - Can be inserted and used as tap
  - Very tiny models exist
- Small computers
  - Computers-on-a-stick
  - CPU, Ethernet & 16 MB RAM
  - Runs Linux 2.6.x

Detecting Taps

- Installation can cause short outages
- Taps introduce single points of failure
- Devices may add latency
- Larger collision domains
- Taps require additional hardware

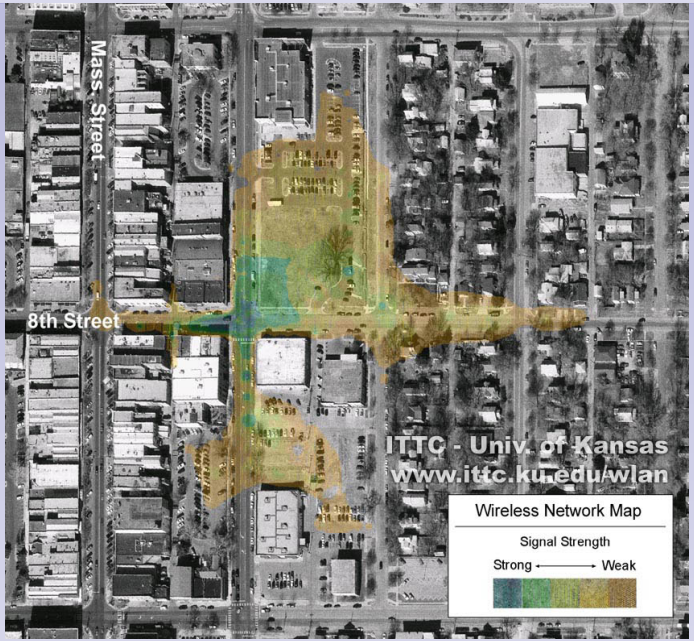
Reconfiguring Devices

- Gaining access to
  - firmware
  - management ports
- “A Bridge Too Far”
  - Changing to bridge mode
- Reconfiguring ports

Wireless Networks

- Wireless transmissions are accessible
  - Passive attacks can't be avoided
- Adding senders may disrupt transmissions
- Wireless taps easier to deploy
  - Line of sight
  - Next to office buildings
  - Carefully chosen aerial

Layer 1 Wireless Expansion



DeepSec Vienna 2007
7 Layers of Insecurity

Wireless Taps

- WLAN devices are small
  - “Forgot” your PDA
  - Modified access points
  - Directed aerials
- Can be placed at greater distances
- Risk: high Impact: high

Wireless/Wired Bridge

Wireless MITM

- Placement of powerful sender
  - Identical ESSID(s)
  - No encryption and Free DHCP/DNS
- Collect MACs and traffic
- Offer services and collect passwords
- Rogue access point(s)

Rogue Access Point

Serious War Driving

Module 31
Hardware Hacking

- Summary
  - Hardware can be abused.
  - Control configuration and cabling.
  - Be careful with wireless signals.
  - Check for taps and rogue hardware.

Thank you for your attention!

- Questions?

DeepSec Vienna 2007
7 Layers of Insecurity

Chapter 31
Hardware Hacking

- **Module Hardware Hacking: Turning Ethernet into Æthernet**

"Taps are used in security applications because they are non-obtrusive, are not detectable on the network,…"

(Wikipedia.org)

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 **31 - Hardware Hacking** **1**

Fingerprinting is a reconnaissance technique which allows to identify systems, versions of operating systems, patch levels, services packs etc. by observing a target for individual responses or actions.

This chapter presents the latest developments in different techniques and discusses methods how risks can be mitigated.

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 31 - Hardware Hacking 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 31
Hardware Hacking

- Agenda
  - Wire Tapping
  - Modifying Network Devices
  - Access to Network Hardware
  - Wireless Networks

DeepSec Vienna 2007
7 Layers of Insecurity

Layer 1 Basics

- But my Network Hardware is behind locked Doors, isn't it?

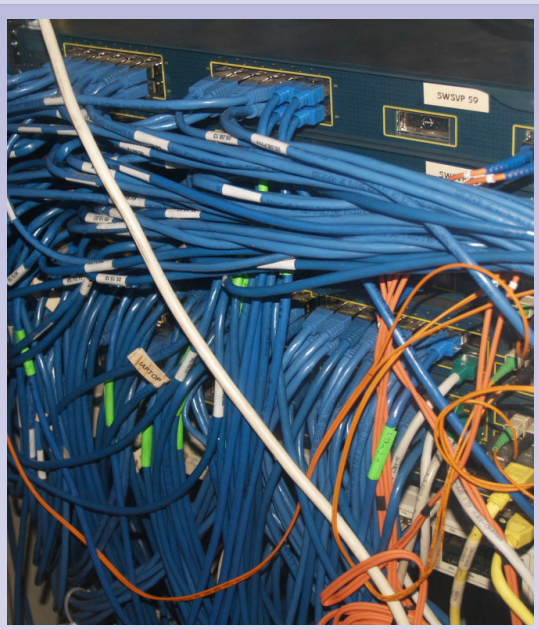
DeepSec Vienna 2007
7 Layers of Insecurity

Layer 1 Basics

- Ashes to ashes, bits to bits
  - Basically we deal with 0 and 1
  - Electronically we have signals
- Access to wiring is crucial
  - Devices access wires for us
- Thin air provides access to wireless networks

DeepSec Vienna 2007
7 Layers of Insecurity

Layer 1 View



Can you spot the rogue port or wire?

Is your cabling longer than it should be?

DeepSec Vienna 2007
7 Layers of Insecurity

Layer 1 Organisation

- Know your cabling closet
  - Know every port
  - Know every connected device
- Know every aerial for wireless networks
- Disable unused segments
  - Disabling means “0 volts”
  - No stand-by mode

DeepSec Vienna 2007
7 Layers of Insecurity

Network Taps

- Thick Ethernet uses taps by design
- Network taps exist for
  - FDDI
  - ATM
  - Ethernet
- Full duplex can be a problem
- Mirror ports (are in layer 2)

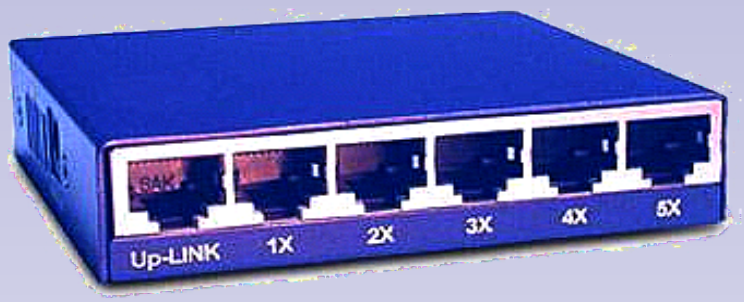
DeepSec Vienna 2007
7 Layers of Insecurity

Tap Gallery

Network tap for optical connection

DeepSec Vienna 2007
7 Layers of Insecurity

Rogue Hub



DeepSec Vienna 2007
7 Layers of Insecurity

Tap-like Intrusions

- Small hubs
  - Can be inserted and used as tap
  - Very tiny models exist
- Small computers
  - Computers-on-a-stick
  - CPU, Ethernet & 16 MB RAM
  - Runs Linux 2.6.x

DeepSec Vienna 2007
7 Layers of Insecurity

Detecting Taps

- Installation can cause short outages
- Taps introduce single points of failure
- Devices may add latency
- Larger collision domains
- Taps require additional hardware

DeepSec Vienna 2007
7 Layers of Insecurity

Reconfiguring Devices

- Gaining access to
  - firmware
  - management ports
- “A Bridge Too Far”
  - Changing to bridge mode
- Reconfiguring ports

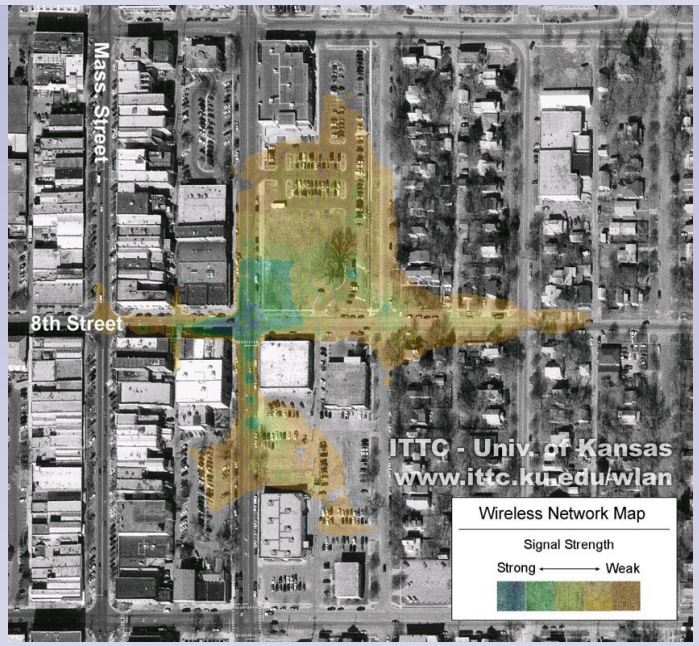
DeepSec Vienna 2007
7 Layers of Insecurity

Wireless Networks

- Wireless transmissions are accessible
  - Passive attacks can't be avoided
- Adding senders may disrupt transmissions
- Wireless taps easier to deploy
  - Line of sight
  - Next to office buildings
  - Carefully chosen aerial

DeepSec Vienna 2007
7 Layers of Insecurity

Layer 1 Wireless Expansion



DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 31 - Hardware Hacking 15

The image above was taken from the Wireless Network Visualization Project of the Information & Telecommunications Technology Center (University of Kansas). It was created by a mobile WLAN adapter coupled with a GPS module. The sensor was capturing data while driving around in a car. The spread of the signal strength in the picture was generated from a single ESSID on a specific channel. The blue part clearly shows the position of the access point. The brown part demonstrates how the 802.11b signal can be scattered by reflections and open spaces. This has to be taken into account when planning wireless networks.

Wireless Taps

- WLAN devices are small
  - “Forgot” your PDA
  - Modified access points
  - Directed aerials
- Can be placed at greater distances
- Risk: high Impact: high

DeepSec Vienna 2007
7 Layers of Insecurity

Mitigation:

• Scan for unauthorised wireless equipment.

• Include portable electronic in your security policy.

- PDAs, cell phones
- Laptops
- Game consoles
- Digital cameras

• Make sure your users don't confuse offered wireless networks.

- Use encryption and authentication.
- Verify configuration on user's wireless equipment.

Wireless/Wired Bridge

DeepSec Vienna 2007
7 Layers of Insecurity

The device shown in the picture is a miniature access point. It can act as a bridge between the connected Ethernet and the wireless network. This mode can be activated with a single switch located on the side of the device.

Wireless MITM

- Placement of powerful sender
  - Identical ESSID(s)
  - No encryption and Free DHCP/DNS
- Collect MACs and traffic
- Offer services and collect passwords
- Rogue access point(s)

DeepSec Vienna 2007
7 Layers of Insecurity

Rogue Access Point

DeepSec Vienna 2007
7 Layers of Insecurity

Serious War Driving

DeepSec Vienna 2007
7 Layers of Insecurity

This WLAN box has 6 different wireless adapters. All can be fitted with suitable aerials. It has a Routerboard 532A motherboard, a 266 MHz MIPS CPU, a 64MB DDR onboard memory chip, 128MB onboard NAND memory chip for storage, one IDT Korina 10/100 Mbit/s Fast Ethernet port and 8 VIA VT6105 10/100 Mbit/s Fast Ethernet ports (all nine ports have Auto-MDI/X), complete with serial port for the console. The wireless adapters use the Atheros AR5213 chipset. The hardware was described in a blog posting by Mark Hoekstra and can be ordered from the developers.

Module 31
Hardware Hacking

- Summary
  - Hardware can be abused.
  - Control configuration and cabling.
  - Be careful with wireless signals.
  - Check for taps and rogue hardware.

DeepSec Vienna 2007
7 Layers of Insecurity

Thank you for your attention!

- Questions?

DeepSec Vienna 2007
7 Layers of Insecurity