Switched environments security...
A fairy tale.

Cédric Blancher <blancher@cartel-securite.fr>

—

July 10, 2002

- Network basics
  - Ethernet basics
  - ARP protocol
- Attacking LAN
  - Several ways to redirect network streams on a LAN.
- ARP cache poisoning, how and why...
  - ARP cache poisoning study
  - Exploiting
- How to protect yourself ?
  - Defending against LAN attacks

- Network basics
  - Ethernet basics
  - ARP protocol

- Attacking LAN
  - Several ways to redirect network streams on a LAN.
- ARP cache poisoning, how and why...
  - ARP cache poisoning study
  - Exploiting
- How to protect yourself ?
  - Defending against LAN attacks

Ethernet :

- Layer 1 and layer 2 protocol
- Different media : 10base2, 10base5, 10baseT, 100baseTX, 100baseFX, etc.

↪ Focus on star-like physical architectures such as 100baseTX or 100baseFX.

Ethernet as layer 1 protocol :

- Relies on CSMA/CD
- Layer 1 network using hubs
- Constitutes a collision domain
- Electrical signal is sent to whole collision domain
- ↪ Within a collision domain, frames are sent to everyone

Ethernet as layer 2 protocol :

- Ethernet frame :

Ethernet frame

- Layer 2 addressing : MAC addresses
- Layer 2 networks using switches

Switches : designed for bandwidth improvement

- Is able to read ethernet adresses in frames
- Associates a port to a MAC addresses list
- Reads source MAC address to keep list up to date
- Reads destination MAC address to switch frame

Consequences :

- Network is split into collision domains
- Frames are only sent to the concerned port
- Bandwidth is improved
- ↪ Urban legend : can’t sniff a switched network

Communicating with upper layers

- Layer 2 addressing : ethernet
- Layer 3 addressing : IP
- Need to associate IP addresses to MAC addresses
- ARP : Address Resolution Protocol (RFC 826)

Hardware type		Protocol type
HW addr lth	P addr lth	Opcode
Source hardware address		
Source protocol address		
Destination hardware address		
Destination protocol address		

ARP message

- HW type : ethernet (0x1)
- Proto type : IP (0x800)
- HW address length : 48 bits
- Proto address length : 32 bits
- ARP request : Opcode=1
- ARP reply : Opcode=2

An ARP request : who has 192.168.1.11 tells 192.168.1.10

- From 00:10:A4:9B:6D:81
- To FF:FF:FF:FF:FF:FF (broadcast)

0x1		0x800
0x30	0x20	0x1
00:10:A4:9B:6D:81		
192.168.1.10		
00:00:00:00:00:00		
192.168.1.11		

ARP request

An ARP reply : 192.168.1.11 is at 00:04:76:40:65:5E

- From 00:04:76:40:65:5E
- To 00:10:A4:9B:6D:81

0x1		0x800
0x30	0x20	0x2
00:04:76:40:65:5E		
192.168.1.11		
00:10:A4:9B:6D:81		
192.168.1.10		

ARP reply

ARP cache

- Need to cache ARP informations
- Need for a mecanism to keep cache up to date
- Aging timers
- Update processes
- “Keep alive” stuff

↪ According to RFC, we are very opportunist when gathering informations

We gather informations wherever they are to keep cache up to date

- ARP requests source informations
- ARP replies informations (even unasked for !)
- ⮑ ARP cache is a good target for attackers ;)

OK... We're done with the basics, let's move on to attacks now.

- Network basics
  - Ethernet basics
  - ARP protocol
- Attacking LAN
  - Several ways to redirect network streams on a LAN.
- ARP cache poisoning, how and why...
  - ARP cache poisoning study
  - Exploiting
- How to protect yourself ?
  - Defending against LAN attacks

LAN attacks

- Layer 1 : sniffing
- Layer 2 : MAC spoofing and “disturbing” switches
- ARP level : ARP spoofing
- ARP level : ARP cache poisoning
- Other attacks

Ethernet frames sniffing

- You can sniff all frames within your collision domain using promiscuous mode
- Pros
  - Passive if done the right way
- Cons
  - Passive
  - Acting on traffic is tricky (ACK storm)
  - Useless in full switched environments

MAC spoofing

- Use a spoofed MAC address as ethernet source
- Relies on MAC/port association table update
- Promiscuous mode to get interesting frames
- Pros
  - Redirects traffic : we can act on it
- Cons
  - Spoofed host is no longer reachable by anyone
  - Creates port/MAC association conflicts
  - Easily detectable behaviour
  - Often leads to port shutdown

“Disturbing” switches

- Associations table can be flooded
- Too much conflicts can lead to strange behaviour
- When disturbed, some switches falls into repeater mode (hub-like)

- Pros
  - Hub-like behaviours
- Cons
  - Relies on flooding
  - Easily detected
  - Works on equipements with old firmware
  - Often leads to port shutdown

ARP spoofing

- ARP request are sent to broadcast
- It is possible to reply to arbitrary requests, with arbitrary replies
- Pros
  - No need to attack switch
  - Allows traffic redirection
- Cons
  - Leads to conflicts

ARP cache poisoning

- We force changes into victim ARP cache
- See next part ;)
- Pros
  - Allows traffic redirection
  - Quite difficult to prevent
- Cons
  - Not much...

Other protocols

- Spanning tree protocol (STP)
- Discovery protocols (CDP)
- Automatic VLAN exportation protocols (VTP, DTP)
- Failover protocols (HSRP, VRRP)

↪ Can lead to traffic redirection and DoS

Let’s focus on ARP cache poisoning...

- Network basics
  - Ethernet basics
  - ARP protocol
- Attacking LAN
  - Several ways to redirect network streams on a LAN.
- ARP cache poisoning, how and why...
  - ARP cache poisoning study
  - Exploiting
- How to protect yourself ?
  - Defending against LAN attacks

ARP cache updates

- Opportunistic behaviour
- Entry insertion
- Entry update
- Entry deletion
- ↪ Let’s see how we can fool this...

Available parameters

- Ethernet source MAC address
- Ethernet destination MAC address
- ARP HW source address
- ARP Proto source address
- ARP HW destination address
- ARP Proto destination address

ARP cache entry creation

- When communicationg with unkown IP (ARP request is sent)
- When unknown IP wants to talk to us (ARP request is received)

↪ Acting on first case is ARP spoofing

↪ Acting on second case is OK if sent directly to target

ARP cache entry creation forcing using spoofed request

- Ethernet destination MAC is target address instead of broadcast
- arp-sk -w -d Target -S Spoofed -D Target

0x1		0x800
0x30	0x20	0x1
Spoofing MAC		
Spoofed IP		
00:00:00:00:00:00		
Target IP		

Fooled ARP request

ARP cache entry creation forcing using spoofed reply

- Does not work on all OS (can't fool Linux 2.4, Windows XP)
- arp-sk -r -d Target -S Spoofed -D Target

0x1		0x800
0x30	0x20	0x2
Spoofing MAC address		
Spoofed IP		
Target MAC address		
Target IP		

Fooled ARP reply

- We prefer use spoofed requests to create entries

ARP cache entry update forcing

- Can be done using spoofed ARP requests
- Can be done using spoofed ARP replies
- Must be sent regularly to avoid legitimate cache update !
- ↪ Interesting entries are always cached : gateways, DNS servers, etc.

ARP cache entry deletion forcing

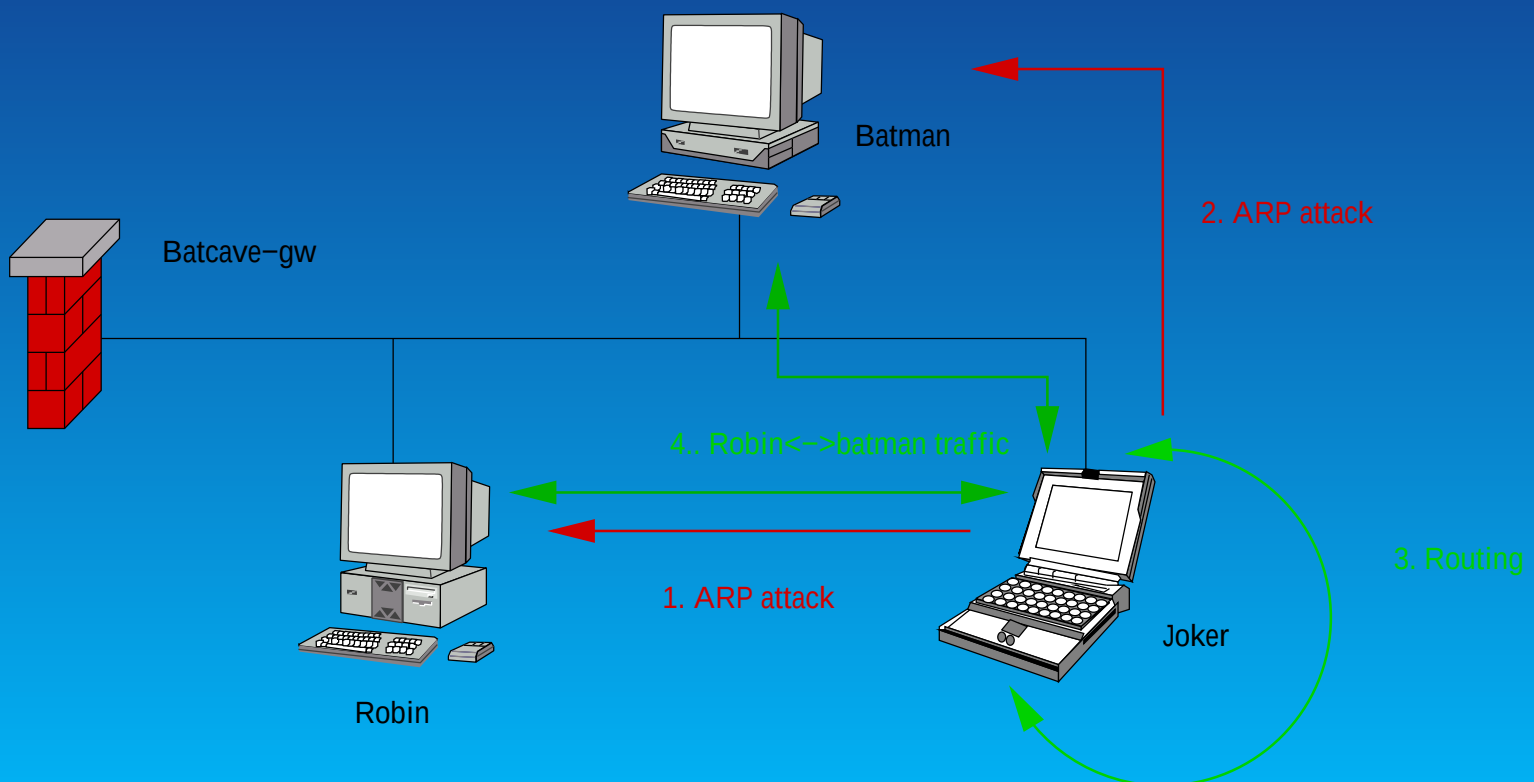
- Entries can expire
- Entries number is limited (about 500 for Linux)

↪ By creating enough entries, we force older entries deletion or ARP cache flush

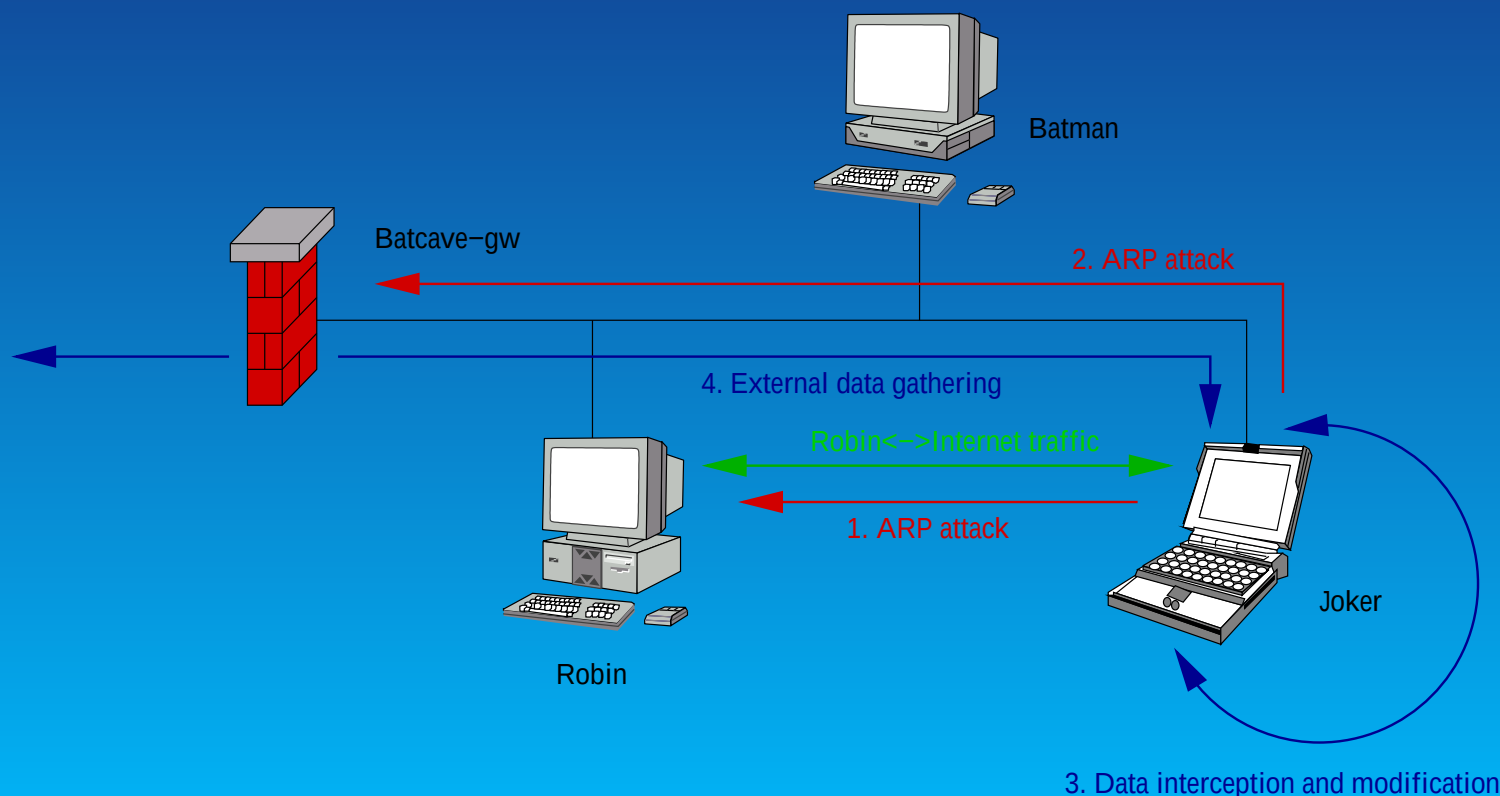
ARP cache poisoning applications

- Spying : you can read data without using promiscuous mode
- Interception : you can transparently proxy connections
- Decrypting : you can decrypt connections using Man in the Middle attack
- Hijacking : you can steal proxied connections
- Tampering : you can inject traffic into proxied connections
- Firewall bypassing : you can bypass firewalling rulesets using IP spoofing
- DoS : packets are redirect to a dead MAC

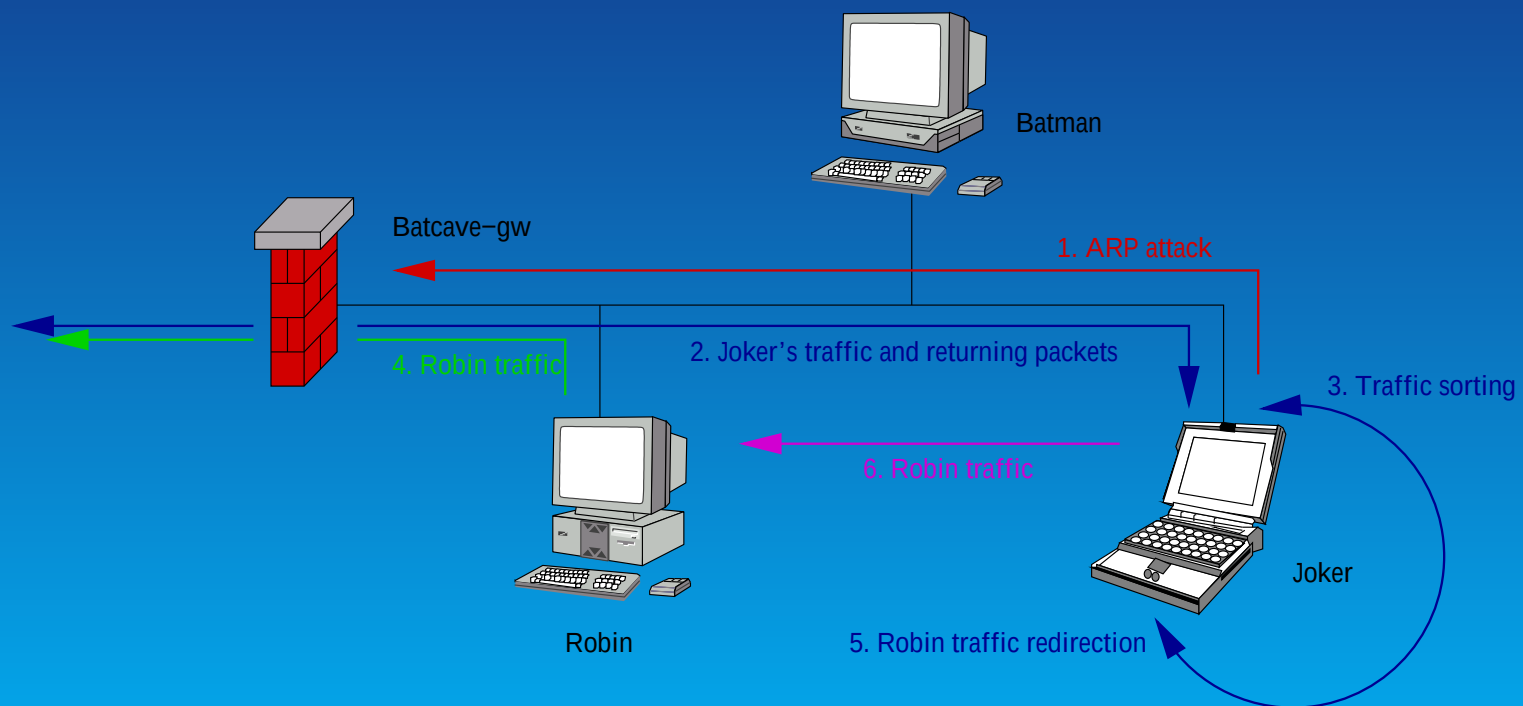
ARP MitM for spying, decrypting connections



ARP proxying for traffic tampering and connection hijacking

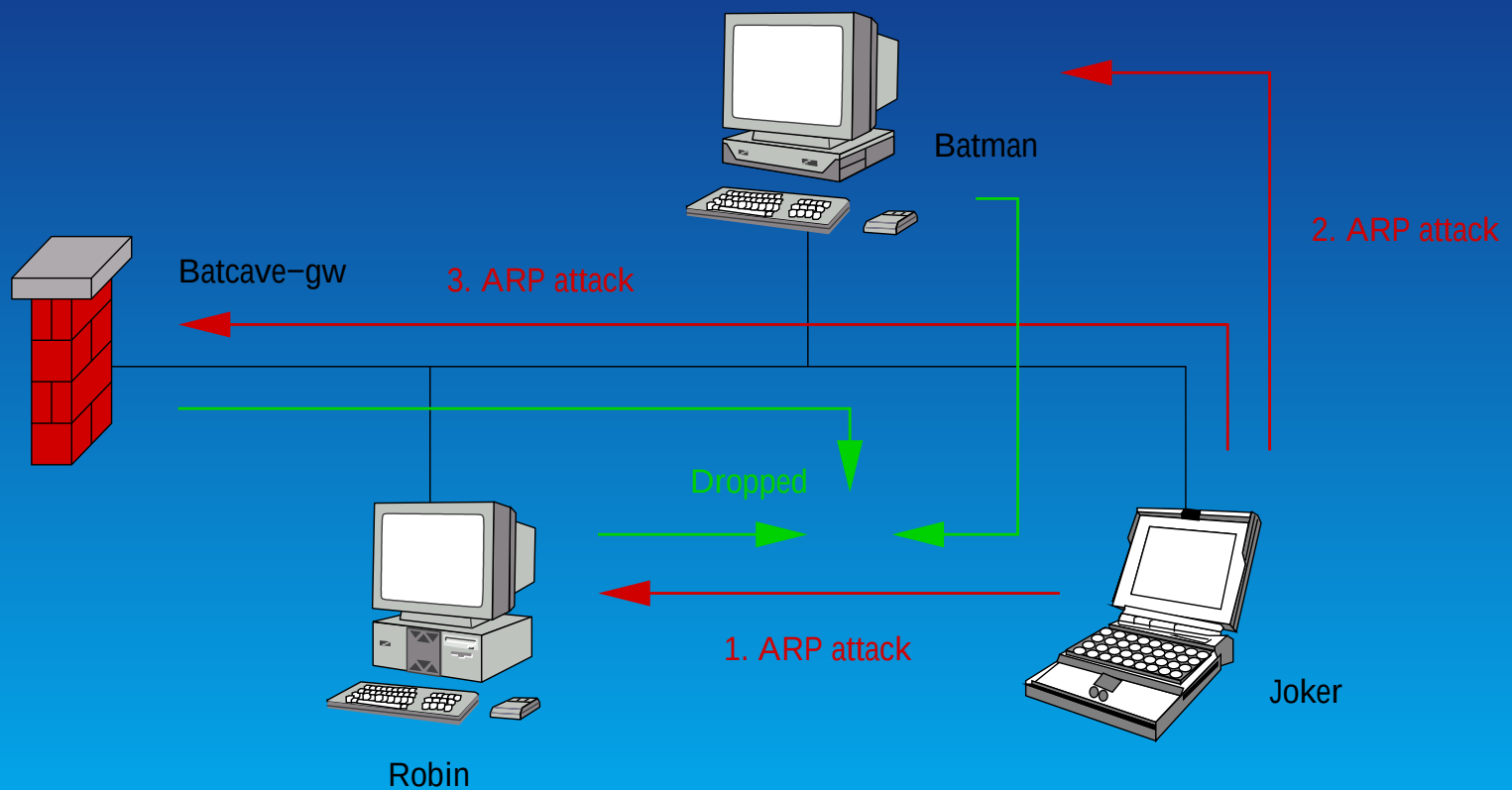


One way ARP cache poisoning for IP spoofing and firewall bypassing



↪ Can be done using MitM between robin and batcave-gw ;)

DoS using ARP cache poisoning



- DoSed hosts are likely to check their entries when things go wrong

Consequence

- Once an attacker is root on a network, the whole ethernet segment is no more secure

- Network basics
  - Ethernet basics
  - ARP protocol
- Attacking LAN
  - Several ways to redirect network streams on a LAN.
- ARP cache poisoning, how and why...
  - ARP cache poisoning study
  - Exploiting
- How to protect yourself ?
  - Defending against LAN attacks

Protections

- Maximum segmentation
- Switches security features
- Static ARP caches
- NIDS stuff
- Layer 2 and ARP filtering
- Strong authentication

↪ Theses protections are not easy to maintain, but are needed

Switches security features

- Use recent firmware to avoid strange behaviours
- Use static MAC/port associations when available
- Use administrative port shutdown when conflict occurs

↪ Prevents MAC spoofing or flooding, but not ARP attacks

↪ Some layer 3 switches feature IP/MAC/port associations

Static ARP caches

- ARP entries can be added “manually” using arp -s
- /etc/ethers like files can be loaded using arp -f
- Such entries are permanent : cannot be nor deleted nor updated

↪ Prevents ARP attacks

↪ Beware of the Windows world, in which permanent entries can be updated (except in XP)

↪ You can sometimes set ARP entries expiration time (Solaris, Linux)

↪ A lot of commercial products do not feature ARP cache tuning

NIDS stuff

- ARPWatch (and WinARPWatch) allows you to track IP/MAC associations through ARP messages
- Some NIDS feature an ARP plugin that monitors ARP messages (Prelude IDS)

↪ Allows detection, but reaction is tricky : fooled messages don’t violate RFC

↪ NIDS lack ARP support : you can’t specify specific rules for ARP

Layer 2 and ARP filtering

- Linux Netfilter has a MAC source address match
- Linux Netfilter will soon provide an ARP table for ARP messages filtering

↪ Lack of products that allow this kind of filtering

Strong authentication

- Relies on cryptographic authentication
- Use public keys, certificates or secure authentication protocols

↪ Reliable but quite painful to deploy

↪ Users can be fooled by well crafted false certificates

Check physical accesses to your network

- Social engineering
- Foreign computers, such as laptops
- Wireless access points (802.11b)

↪ Do not let anybody plug himself onto your network !

ARP is a weak protocol, easy to fool : it was not designed for security.

We need a more secure way to authenticate hosts.

Whatever, it is obvious that switches are not security tools.

<PUB>

- French security magazine MISC

</PUB>

Thanks to :

- Frédéric "Pappy" Raynal for convincing me into looking deeper in that stuff and writing arp-sk
- Éric Detoisien for writing Win32 tools winarp-sk and winarp-mim
- Daniel "Bozo" Polombo for having performed a heavy de-obfuscating task on my slides

- http://www.networksorcery.com/enp/default0402.htm
- http://www.arp-sk.org/
- http://www.monkey.org/~dugsong/dsniff/
- http://www.bitland.net/taranis/
- http://www.off.net/~jme/ols2000/html/img0.htm
- http://www.netfilter.org/
- http://letanou.linuxfr.org/arpwatch/arpwatch.html
- http://jota.sm.luth.se/~andver-8/warp/
- http://www.prelude-ids.org/
- http://www.cartel-securite.fr/