

Alberto Ornaghi <alor@antifork.org>
Marco Valleri <naga@antifork.org>

Man in the middle attacks

- What they are
- How to achieve them
- How to use them
- How to prevent them

Table of contents

Different attacks in different scenarios:

LOCAL AREA NETWORK:

- ARP poisoning
- Port stealing
- DNS spoofing
- STP mangling

FROM LOCAL TO REMOTE (through a gateway):

- ARP poisoning
- ICMP redirection
- DNS spoofing
- IRDP spoofing
- DHCP spoofing
- route mangling

REMOTE:

- DNS poisoning
- traffic tunneling
- route mangling

Once in the middle...

Sniffing

- It is the easiest attack to launch since all the packets transit through the attacker.
- All the “plain text” protocols are compromised (the attacker can sniff user and password of many widely used protocol such as telnet, ftp, http)

Hijacking

- Easy to launch
- It isn't blind (the attacker knows exactly the sequence numbers of the TCP connection)

Injecting

- Possibility to add packets to an already established connection (only possible in full-duplex mitm)
- The attacker can modify the sequence numbers and keep the connection synchronized while injecting packets.
- If the mitm attack is a “proxy attack” it is even easier to inject (there are two distinct connections)

Filtering

- The attacker can modify the payload of the packets by recalculating the checksum
- He/she can create filters on the fly
- The length of the payload can also be changed but only in full-duplex (in this case the seq has to be adjusted)

Attacks examples

Attacks examples (1)

Command injection

- Useful in scenarios where a one time authentication is used (e.g. RSA token). In such scenarios sniffing the password is useless, but hijacking an already authenticated session is critical
- Injection of commands to the server
- Emulation of fake replies to the client

Attacks examples (2)

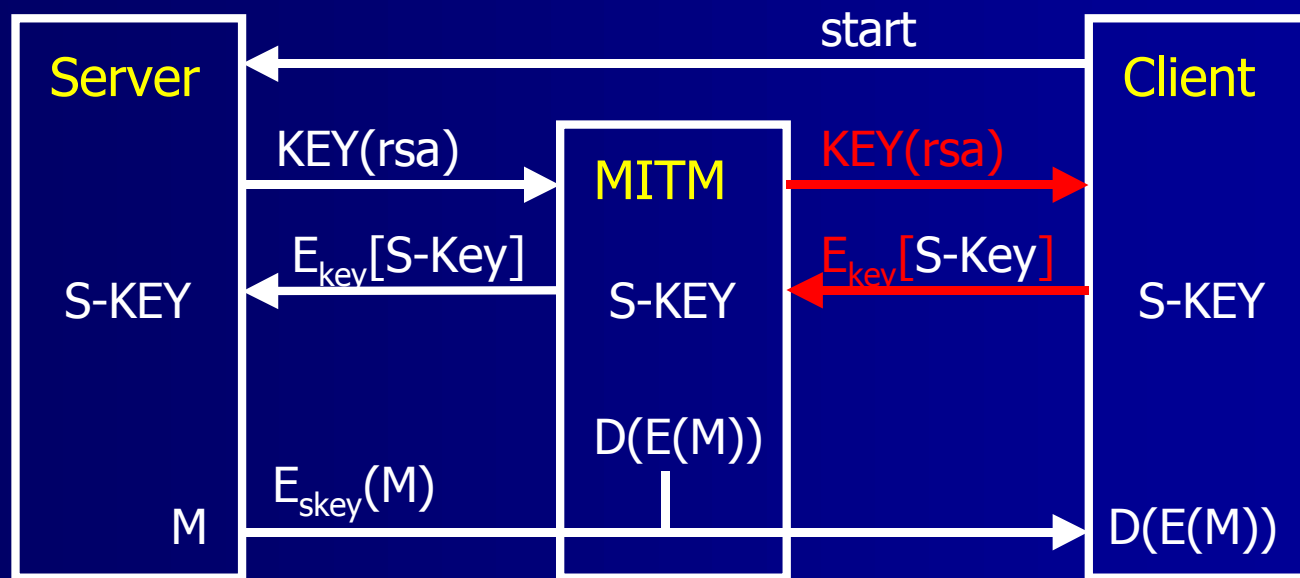
Malicious code injection

- Insertion of malicious code into web pages or mail (javascript, trojans, virus, ecc)
- Modification on the fly of binary files during the download phase (virus, backdoor, ecc)

Attacks examples (3)

Key exchanging

- Modification of the public key exchanged by server and client. (eg SSH1)



Attacks examples (4)

Parameters and banners substitution

- Parameters exchanged by server and client can be substituted in the beginning of a connection. (algorithms to be used later)
- Example: the attacker can force the client to initialize a SSH1 connection instead of SSH2.
 - The server replies in this way:
 - SSH-1.99 -- the server supports ssh1 and ssh2
 - SSH-1.51 -- the server supports ONLY ssh1
 - The attacker makes a filter to replace "1.99" with "1.51"
- Possibility to circumvent known_hosts

Attacks examples (5)

IPSEC Failure

- Block the keymaterial exchanged on the port 500 UDP
- End points think that the other cannot start an IPSEC connection
- If the client is configured in rollback mode, there is a good chance that the user will not notice that the connection is in clear text

Attacks examples (6)

PPTP (1) - description

- Uses GRE as transport layer (no encryption, no authentication)
- Uses the same negotiation scheme as PPP (req, ack, nak, rej)
- Negotiation phases are not authenticated
- MS-CHAPv2 mutual authentication can't prevent this kind of mitm

Attacks examples (6)

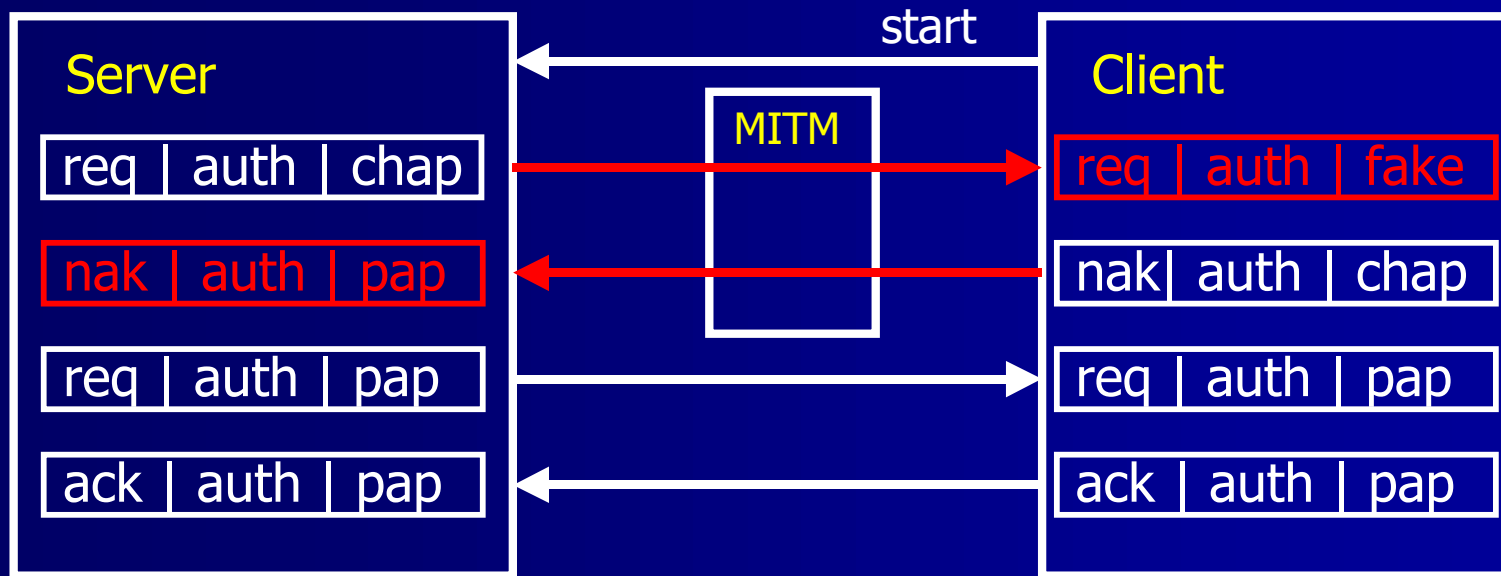
PPTP (2) - attacks

- During negotiation phase
 - Force PAP authentication (almost fails)
 - Force MS-CHAPv1 from MS-CHAPv2 (easier to crack)
 - Force no encryption
- Force re-negotiation (clear text terminate-ack)
 - Retrieve passwords from existing tunnels
 - Perform previous attacks
- Force “password change” to obtain password hashes
 - Hashes can be used directly by a modified SMB or PPTP client
 - MS-CHAPv2 hashes are not usefull (you can force v1)

Attacks examples (6)

PPTP (3) - attack example

Force PAP from CHAP



We don't have to mess with GRE sequences...

Attacks examples (6)

PPTP (4) - L2TP rollback

- L2TP can use IPSec ESP as transport layer (stronger than PPTP)
- By default L2TP is tried before PPTP
- Blocking ISAKMP packets results in an IPSec failure
- Client starts a request for a PPTP tunnel (rollback)
- Now you can perform PPTP previous attacks

Attacks examples (6)

PPTP (5) - tools

- **Ettercap** (<http://ettercap.sf.net>)
 - Hydra plugins suite
- **Anger** (<http://packetstormsecurity.org/sniffers/anger.tar.gz>)

Attack techniques

LOCAL SCENARIO

Local Attacks (1)

ARP poisoning

- ARP is stateless (we all know how it works and what the problems are)
- Some operating systems do not update an entry if it is not already in the cache, others accept only the first received reply (e.g. solaris)
- The attacker can forge a spoofed ICMP packet to force the host to make an ARP request. Immediately after the ICMP it sends the fake ARP reply
- Request attack against linux (IDS evasion)

Local Attacks (1)

ARP poisoning

- Useful to sniff on switched LANs
- The switch works at layer 2 and it is not aware of the poisoning in the hosts' ARP cache (unless some ARP inspection)

Local Attacks (1)

ARP poisoning - tools

- **Ettercap** (<http://ettercap.sf.net>)
 - Poisoning
 - Sniffing
 - Hijacking
 - Filtering
 - SSH sniffing (transparent attack)
- **Dsniff** (<http://www.monkey.org/~dugsong/dsniff>)
 - Poisoning
 - Sniffing
 - SSH sniffing (proxy attack)

Local Attacks (1)

ARP poison - countermeasures

- YES - passive monitoring (arpwatch)
- YES - active monitoring (ettercap)
- YES - IDS (detect but not avoid)

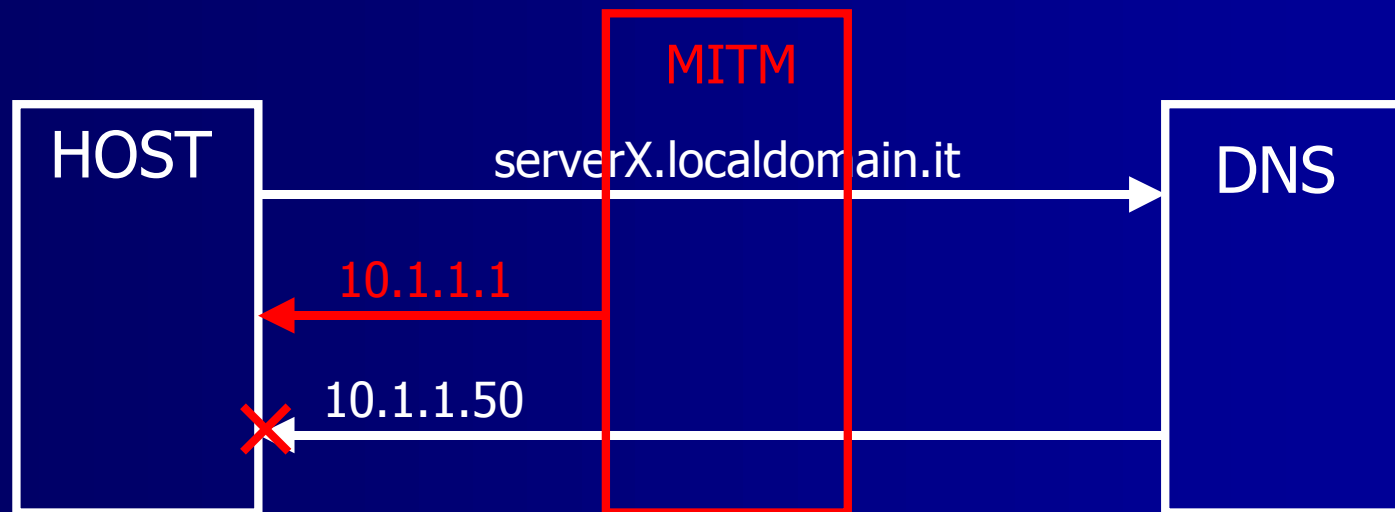
- YES - Static ARP entries (avoid it)
- YES - Secure-ARP (public key auth)

- NO - Port security on the switch
- NO - anticap, antidote, middleware approach

Local Attacks (2)

DNS spoofing

If the attacker is able to sniff the ID of the DNS request, he/she can reply before the real DNS server



Local Attacks (2)

DNS spoofing - tools

- **Ettercap** (<http://ettercap.sf.net>)
 - Phantom plugin
- **Dsniff** (<http://www.monkey.org/~dugsong/dsniff>)
 - Dnsspoof
- **Zodiac**
(<http://www.packetfactory.com/Projects/zodiac>)

Local Attacks (2)

DNS spoofing - countermeasures

- YES - detect multiple replies (IDS)
- YES - use /etc/hosts or host file for static resolution of critical hosts
- YES - DNSSEC

Local Attacks (3)

STP mangling

- It is not a real MITM attack since the attacker is able to receive only “unmanaged” traffic
- The attacker can forge BPDU with high priority pretending to be the new root of the spanning tree

Local Attacks (3)

STP mangling - tools

- **Ettercap** (<http://ettercap.sf.net>)
 - Lamia plugin

Local Attacks (3)

STP mangling - countermeasures

- YES - Disable STP on VLAN without loops
- YES - Root Guard, BPDU Guard.

Local Attacks (4)

Port stealing

- The attacker sends many layer 2 packets with:
 - Source address equal to victim hosts' address
 - Destination address equal to its own mac address
- The attacker now has "stolen" victim hosts' ports
- When the attacker receives a packet for one of the victims it generates a broadcast ARP request for the victim's IP address.
- When the attacker receives the ARP reply from the victim, the victim's port has been restored to the original binding state
- The attacker can now forward the packet and restart the stealing process

Local Attacks (4)

Port stealing - tools

- **Ettercap** (<http://ettercap.sf.net>)
 - Confusion plugin

Local Attacks (4)

Port stealing - countermeasures

- YES - port security on the switch
- NO - static ARP

Attack techniques **FROM LOCAL TO REMOTE**

Local to remote attacks (1)

DHCP spoofing

- The DHCP request are made in broadcast.
- If the attacker replies before the real DHCP server it can manipulate:
 - IP address of the victim
 - GW address assigned to the victim
 - DNS address

Local to remote attacks (1)

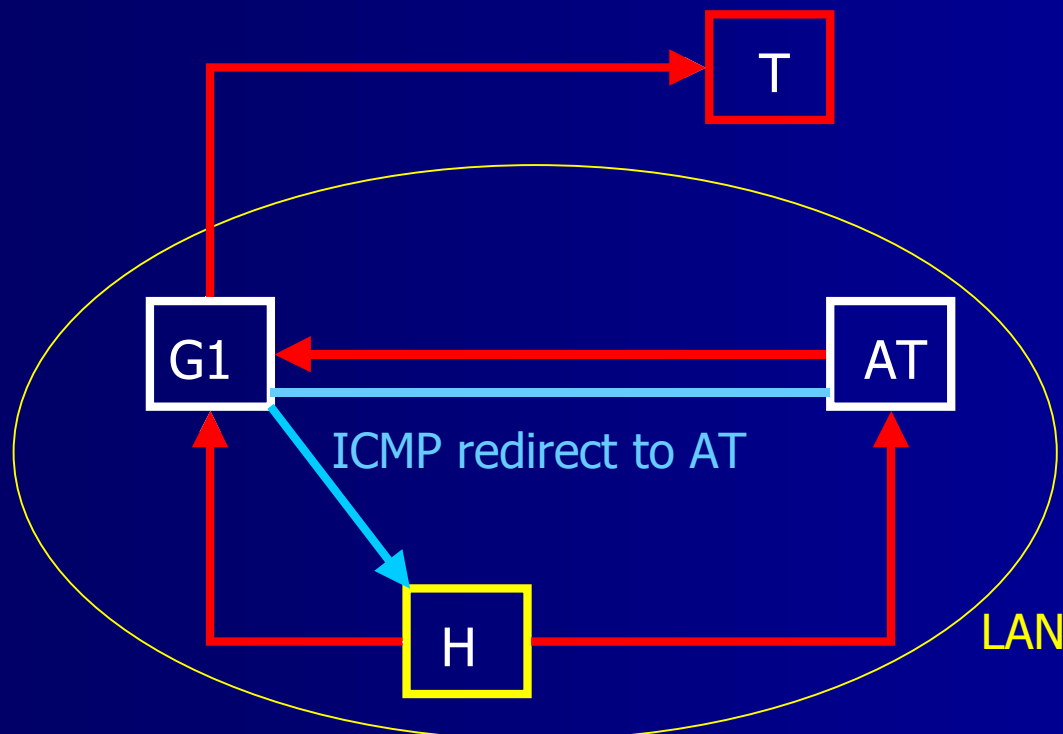
DHCP spoofing - countermeasures

- YES - detection of multiple DHCP replies

Local to remote attacks (2)

ICMP redirect

The attacker can forge ICMP redirect packet in order to Redirect traffic to himself



Local to remote attacks (2)

ICMP redirect - tools

- **IRPAS icmp_redirect** (Phenoelit)
(<http://www.phenoelit.de/irpas/>)
- **icmp_redir** (Yuri Volobuev)

Local to remote attacks (2)

ICMP redirect - countermeasures

- **YES** - Disable the ICMP REDIRECT
- **NO** - Linux has the "secure redirect" options but it seems to be ineffective against this attack

Local to remote attacks (3)

IRDP spoofing

- The attacker can forge some advertisement packet pretending to be the router for the LAN. He/she can set the “preference level” and the “lifetime” at high values to be sure the hosts will choose it as the preferred router.
- The attack can be improved by sending some spoofed ICMP Host Unreachable pretending to be the real router

Local to remote attacks (3)

IRDP spoofing - tools

- **IRPAS** by Phenoelit
(<http://www.phenoelit.de/irpas/>)

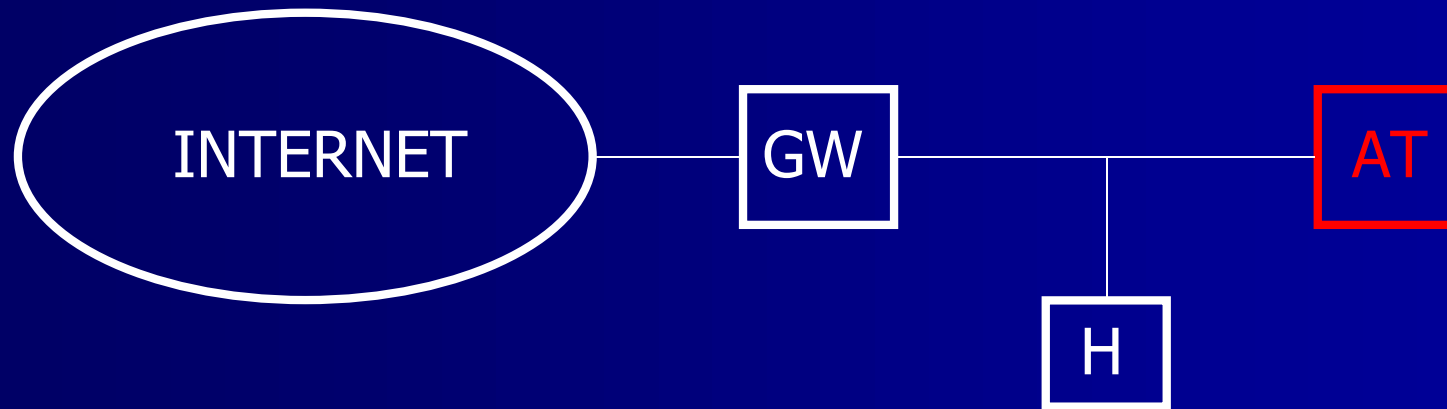
Local to remote attacks (3)

IRDP spoofing - countermeasures

- **YES** - Disable IRDP on hosts if the operating system permit it.

Local to remote attacks (4)

ROUTE mangling



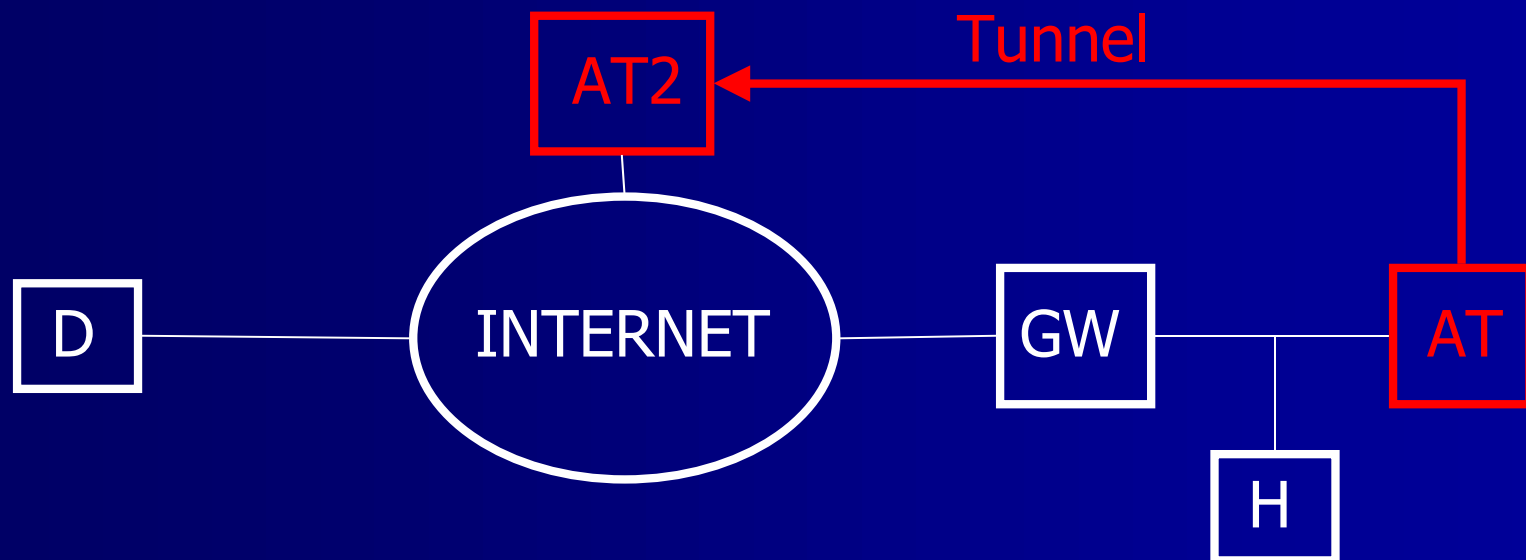
The attacker can forge packets for the gateway (GW) pretending to be a router with a good metric for a specified host on the internet

The netmask should be big enough to win against other routes

Local to remote attacks (4)

ROUTE mangling

- Now the problem for the attacker is to send packets to the real destination. He/she cannot send it through GW since it is convinced that the best route is AT.



Local to remote attacks (4)

ROUTE mangling - tools

- **IRPAS** (Phenoelit)
(<http://www.phenoelit.de/irpas/>)
- **Nemesis**
(<http://www.packetfactory.net/Projects/nemesis/>)

Local to remote attacks (4)

ROUTE mangling - countermeasures

- **YES** - Disable dynamic routing protocols on this type of scenarios
- **YES** - Enable some ACL to block unexpected update
- **YES** - Enable authentications on the protocols that support them

Attacks techniques

REMOTE SCENARIOS

Remote attacks (1)

DNS poisoning

- Type 1 attack
 - The attacker sends a request to the victim DNS asking for one host
 - The attacker spoofs the reply which is expected to come from the real DNS
 - The spoofed reply must contain the correct ID (brute force or semi-blind guessing)

Remote attacks (1)

DNS poisoning

- Type 2 attack
 - The attacker can send a “dynamic update” to the victim DNS
 - If the DNS processes it, it is even worse because it will be authoritative for those entries

Remote attacks (1)

DNS poisoning - tools

- **ADMIdPack**
- **Zodiac**
(<http://www.packetfactory.com/Projects/zodiac>)

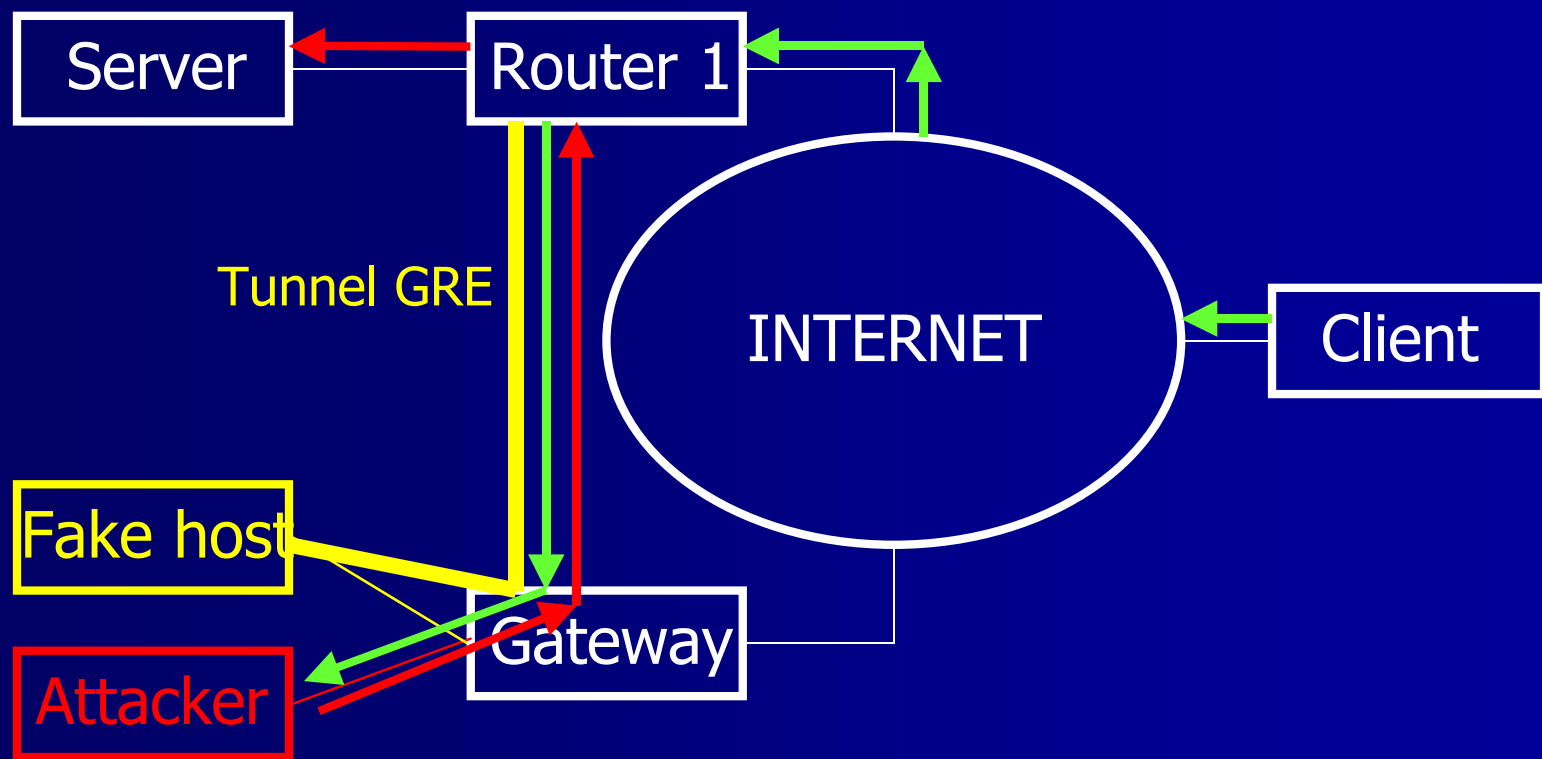
Remote attacks (1)

DNS poisoning - countermeasures

- **YES** - Use DNS with random transaction ID (Bind v9)
- **YES** - DNSSEC (Bind v9) allows the digital signature of the replies.
- **NO** - restrict the dynamic update to a range of IP (they can be spoofed)

Remote attacks (2)

Traffic Tunneling



Remote attacks (2)

Traffic Tunneling - tools

- **Ettercap** (<http://ettercap.sf.net>)
 - Zaratan plugin
- **TunnelX** (<http://www.phrack.com>)

Remote attacks (2)

Traffic Tunneling - countermeasure

- **YES** - Strong passwords and community on routers

Remote attacks (3)

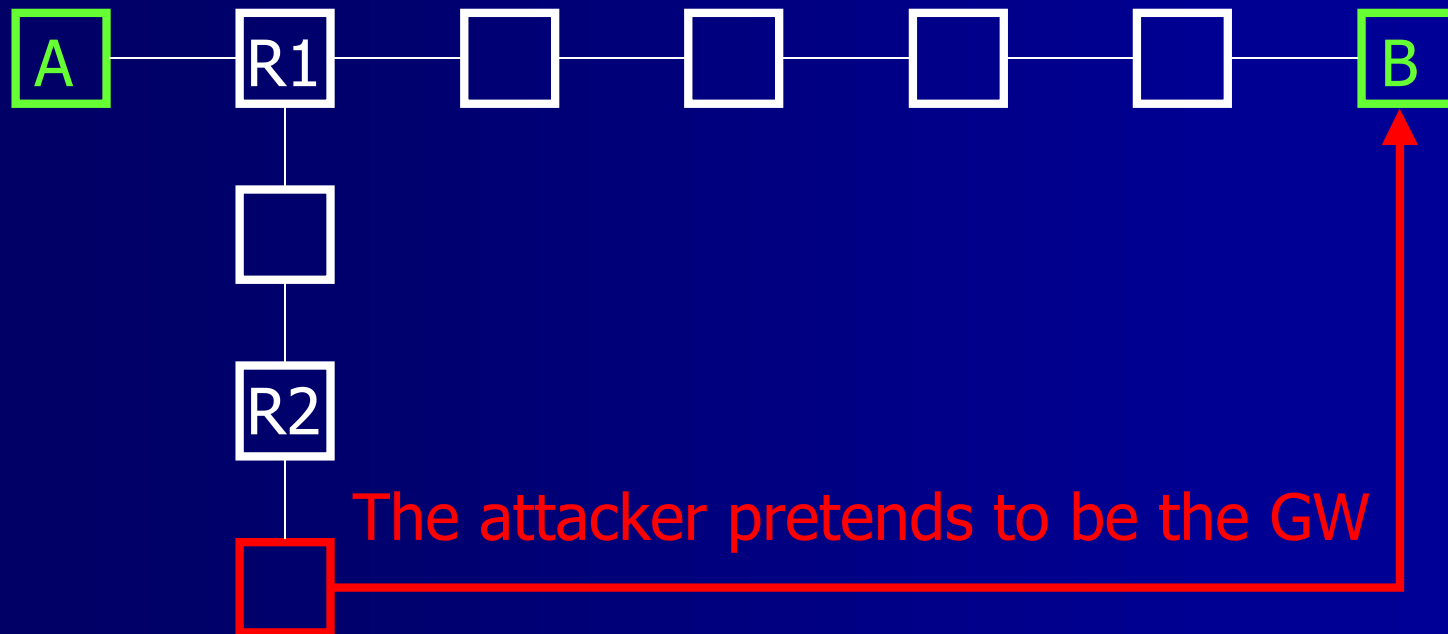
ROUTE mangling

- The attacker aims to hijack the traffic between the two victims A and B
- The attack will collect sensitive information through:
 - traceroute
 - portscanning
 - protoscanning
- Quite impossible against link state protocols

Remote attacks (3)

ROUTE mangling

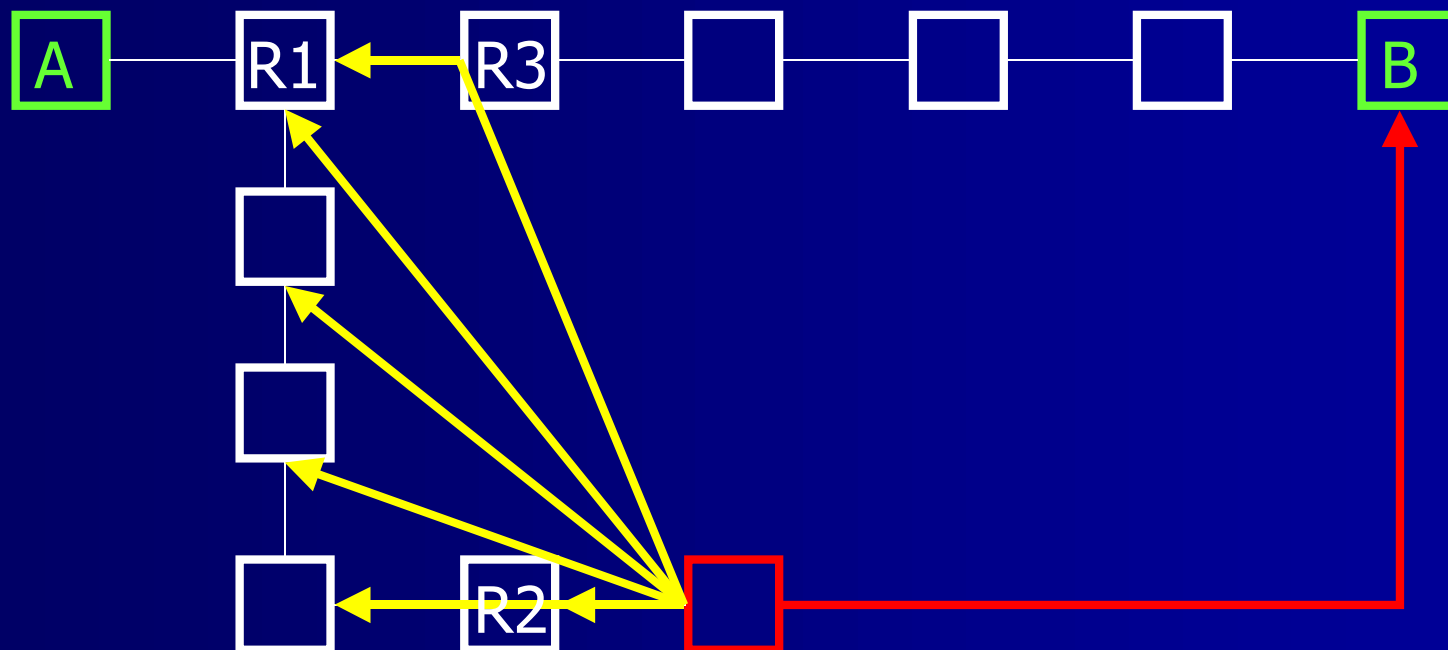
- Scenario 1 a
(IGRP inside the AS)



Remote attacks (3)

ROUTE mangling

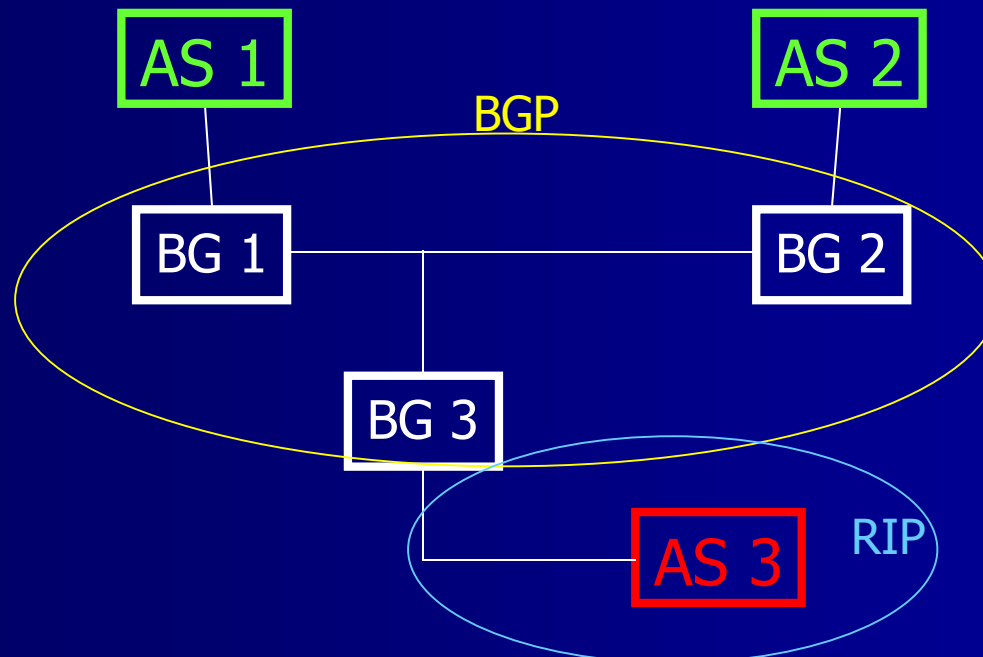
- Scenario 1 b
(IGRP inside the AS)



Remote attacks (3)

ROUTE mangling

- Scenario 2 a
(the traffic does not pass thru the AS)



Remote attacks (3)

ROUTE mangling

- **IRPAS** di Phenoelit

(<http://www.phenoelit.de/irpas/>)

- **Nemesis**

(<http://www.packetfactory.net/Projects/nemesis/>)

Remote attacks (3)

ROUTE mangling - countermeasure

- **YES** - Use routing protocol authentications

Conclusions

- The security of a connection relies on:
 - a proper configuration of the client (avoiding ICMP Redirect, ARP Poisoning etc.)
 - the other endpoint infrastructure (es. DNS dynamic update),
 - the strongness of a third party appliances on which we don't have access (es. Tunnelling and Route Mangling).
- The best to protect a communication is the correct and conscious use of cryptographic suites
 - both client and server side
 - at the network layer (ie. IPSec)
 - at transport layer (ie. SSLv3)
 - at application layer (ie. PGP).

- Marco Valleri <naga@antifork.org>
- Alberto Ornaghi <alor@antifork.org>