802.11 Security

Inaccessible Star ?

Philippe TEUWEN
Cédric BLANCHER

Hack.lu
2006 October 19-21
`http://hack.lu/`

EADS CCR

Agenda

EADS CCR

Agenda

EADS CCR

Public WiFi networks

Open wireless networks

- Anybody can access network
- Zero conf. or so
- Services open to anyone

Anybody can access/play/attack...

Public WiFi networks

Open wireless networks

- Anybody can access network
- Zero conf. or so
- Services open to anyone

Anybody can access/play/attack...

Security specifics

Security ?

- No authentication/authorization
- No message authenticity
- No confidentiality
- Etc.

Some clients isolation measures

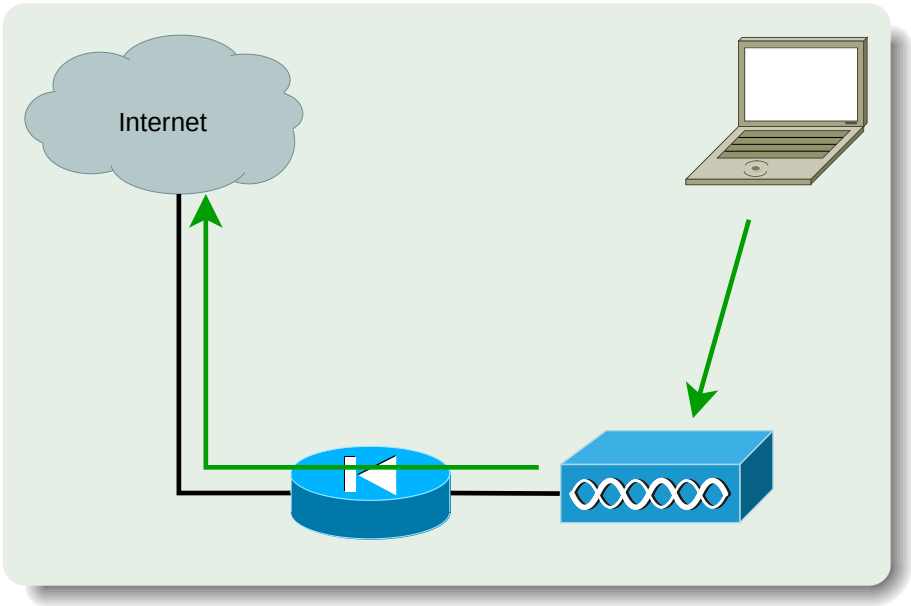
EADS CCR

Open networks

Open infrastructure network : anyone can join

- Generous users who share their access
- Any traffic allowed to Internet
- Sometimes some restrictions (ports, bandwidth)

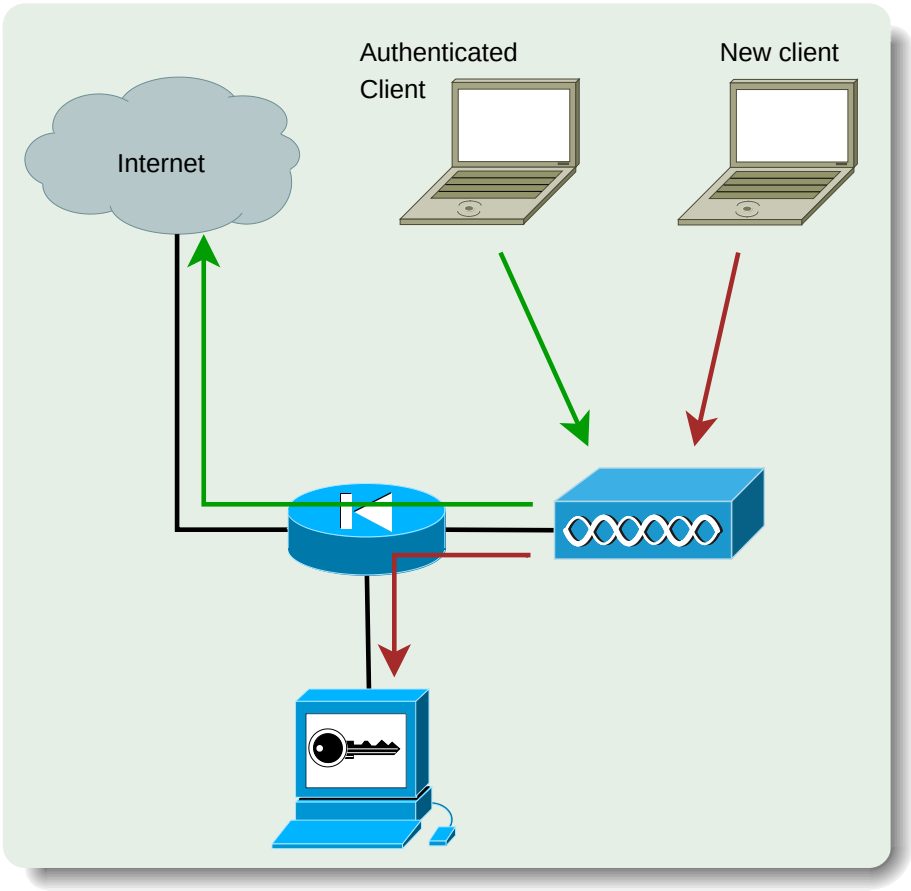
Legal issues ?



Captive portal

Open infrastructure network : anyone can join

- Outbound traffic is filtered out
- HTTP traffic is redirected to auth. portal
- Once registered, client can access Internet

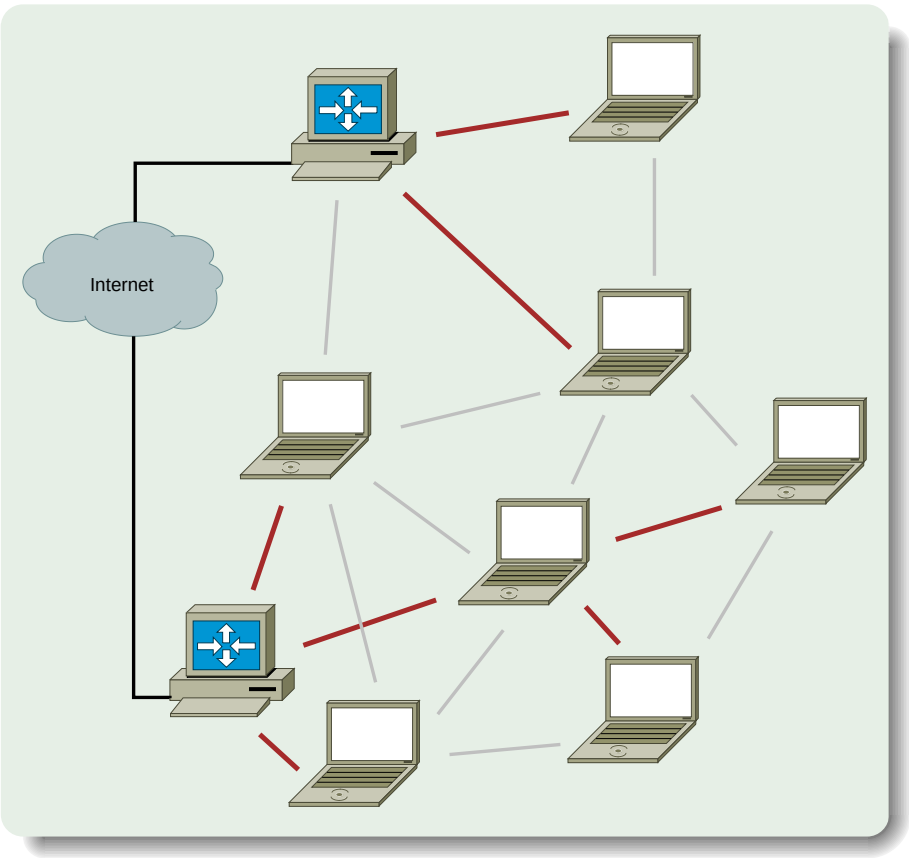


Mesh networks

Adhoc based network

- Clients to clients links
- Clients can join/move/leave
- Dynamic and adaptative routing

AODV, OLSR provide dynamic and adaptative routing



EADS CCR

Agenda

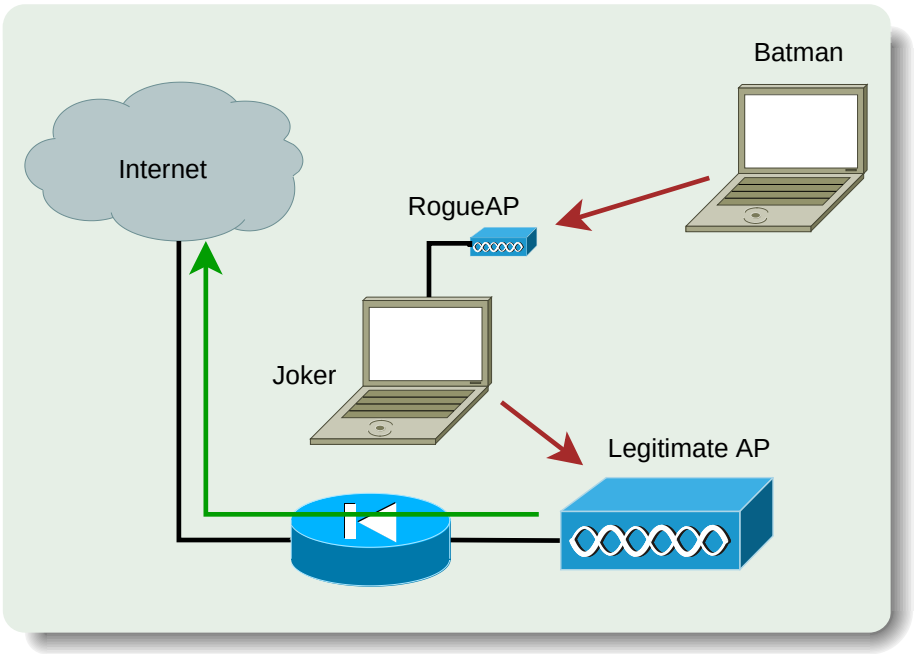
EADS CCR

Rogue AP
Attack principles

Classical, unexpensive, well known layer 1/2 attack

- Set up AP with same configuration
- Power-up and associate clients
- Divert client traffic and play

Easy, efficient, powerful tools available[KRM]

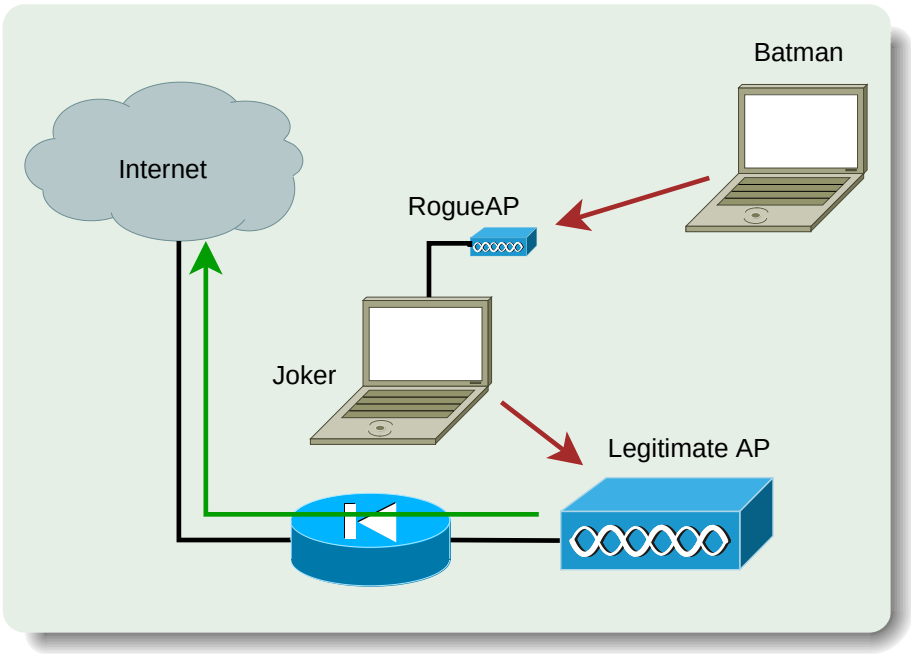


Rogue AP
Application to hotspots

Take advantage from traffic redirection

- Credentials interception
- Crypto MiM attack[a]
- Assisted registration

Not very practical if not gifted with impressive 6th sense



[a] Who cares about that f**kin' popup anyway ?

Tracking authenticated clients

Captive portal can only rely on network addresses for clients identification

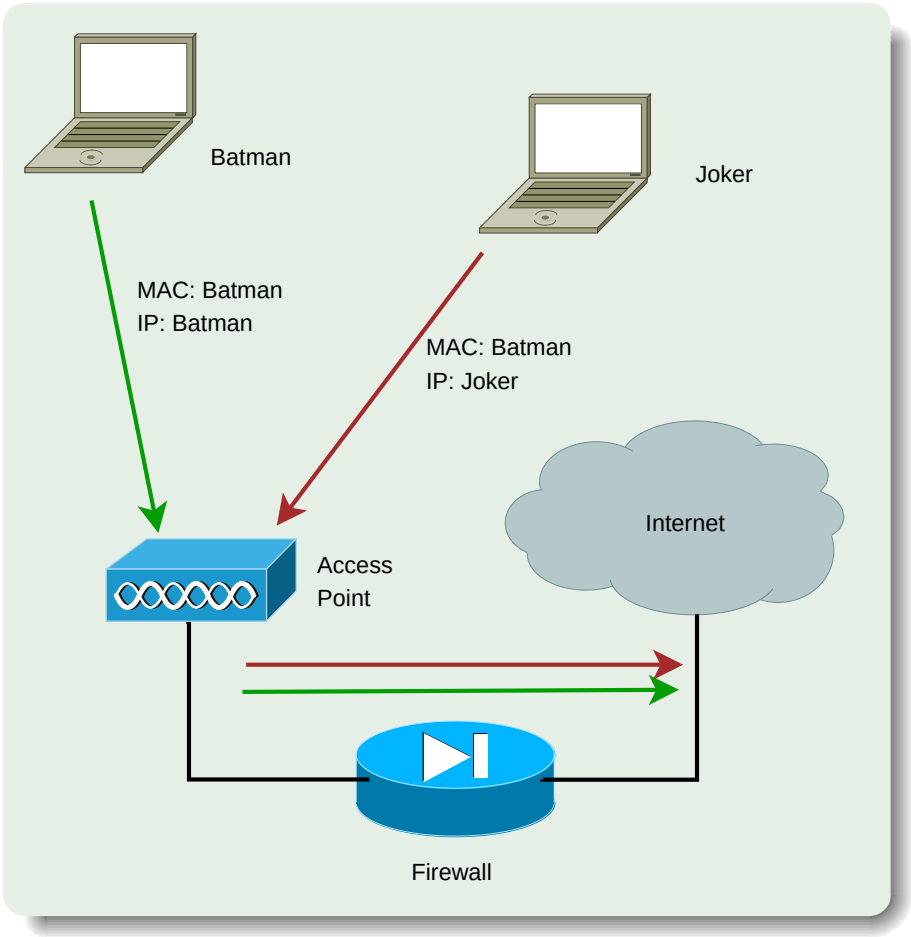
- MAC address
- IP address

Being able to spoof thoses addresses allows existing authorization takeover

MAC based authorization tracking

Registered clients are identified by their MAC address

- MAC address is easy to spoof
- No MAC layer conflict on WiFi network
- Just need a different IP



MAC based tracking practical bypass

Change WiFi interface MAC address

MAC spoofing

```
joker# ifconfig wlan0 hw ether $MAC
joker# ifconfig wlan0 $IP $NETMASK $BROADCAST
joker# route add default $FIREWALL
```

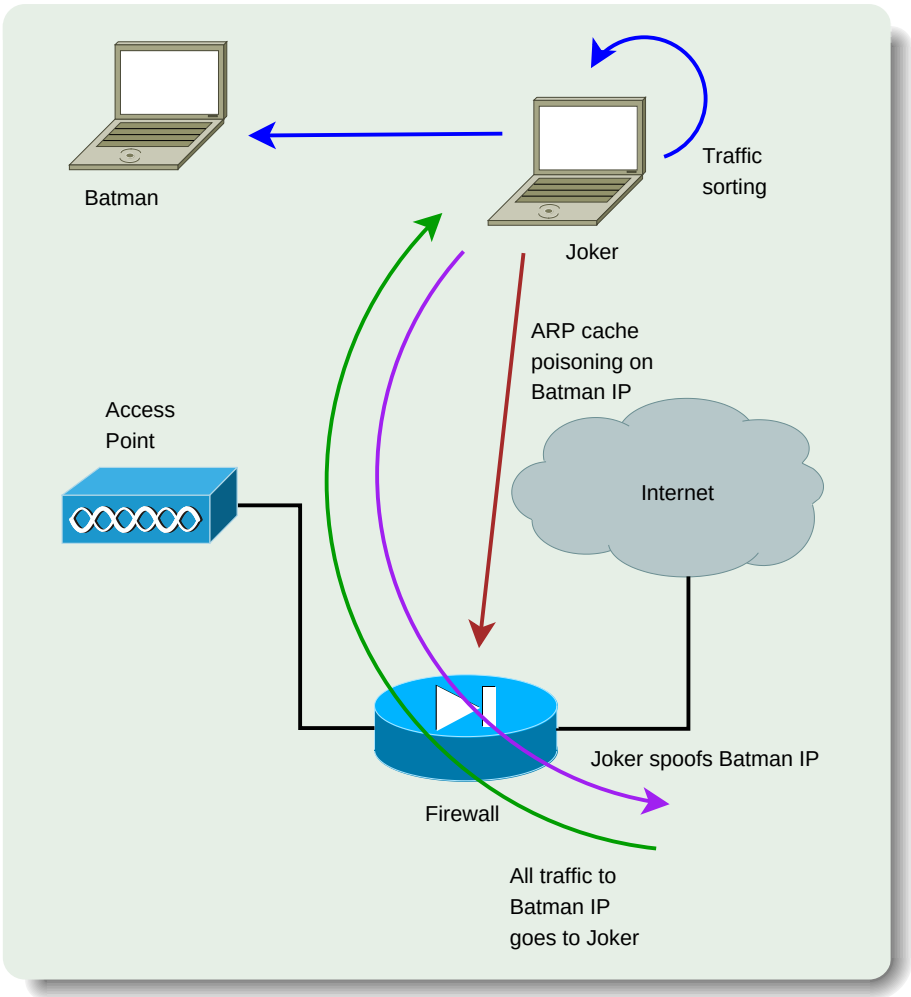
IP based authorization tracking

Registered clients are identified by their IP address

- IP address are just a little more tricky to spoof
- ARP cache poisoning helps redirecting traffic
- Traffic redirection allows IP spoofing

So called Smart Spoofing[a]

[a] See my LSM 2002 talk[BLA02], arp-sk website[ARPS] for details



IP based tracking practical bypass

"Smart spoofing"

IP spoofing

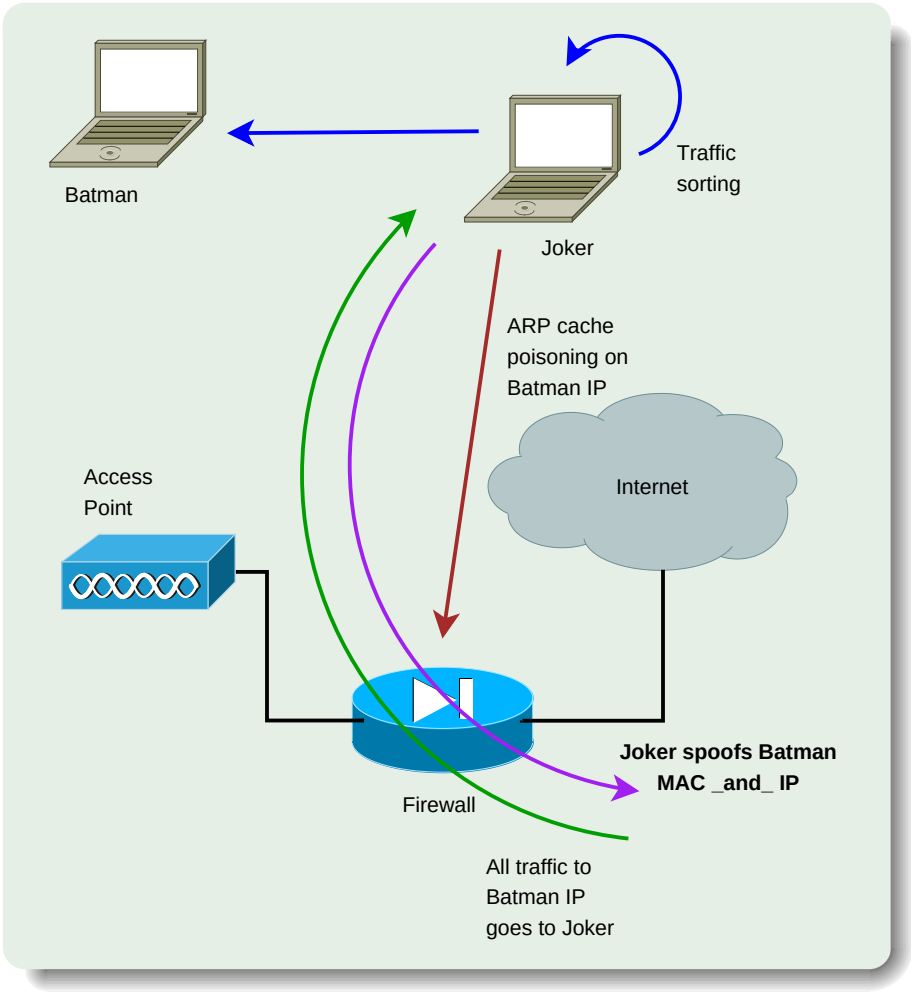
```
joker# echo 1 > /proc/sys/net/ipv4/ip_forward
joker# arp-sk -i ath0 -w -d $FIREWALL -S $BATMAN \
                                      -D $FIREWALL
joker# iptables -t nat -A OUTPUT -d ! $LAN \
                                      -j SNAT --to $BATMAN
joker# iptables -t mangle -A FORWARD -d $BATMAN \
                                      -j TTL --ttl-inc 1
```

EADS CCR

MAC+IP addresses based authorization tracking

Teh-Smart tracking technic ?

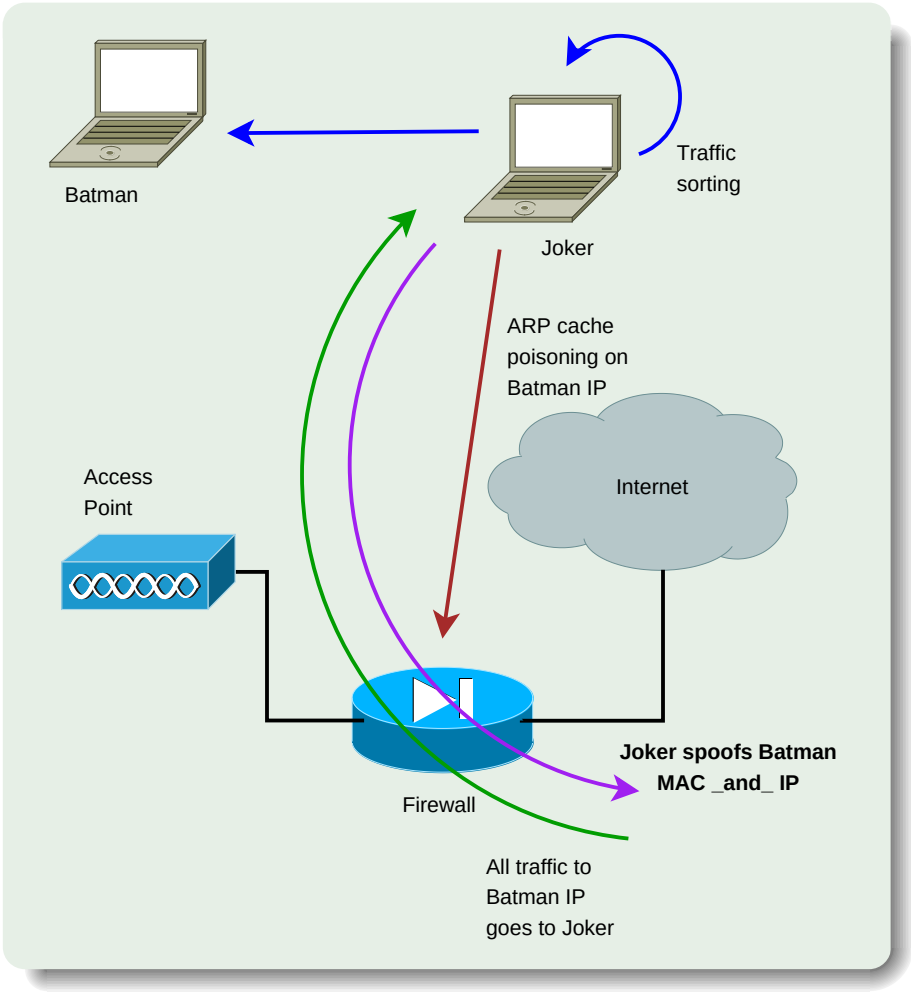
- Previous technic won't help because of MAC address checking
- Send traffic with spoofed MAC address
- ARP cache poisoning and IP spoofing for answers redirection



Why does MAC+IP does not help either ?

Layer2 and Layer3 are close to independant

- No correlation between ARP cache and filtering
- Joker's MAC spoofed frames are accepted
- Returning frames are sent with Joker's MAC address



MAC+IP tracking bypass

Joker uses ebtables[EBT] to have output frames spoofed

MAC+IP spoofing

```
joker# modprobe bridge
joker# brctl addbr br0; brctl addif br0 ath0
[configure bridge interface br0]
joker# ebtables -t nat -A POSTROUTING -o ath0 \
                -d $FW_MAC -j snat \
                --to-source $BATMAN_MAC
```

Then IP spoofing can be done, performing "Smarter spoofing" :)

Demo

Demo

- Captive portal bypass
- MAC+IP spoofing

Few other technics

- Misconfigurations
- DNS based communication[OZY] or tunneling[NSTX]
- Administration network on the same VLAN, accessible through WiFi
- ESTABLISHED,RELATED -j ACCEPT prevents connections drop when authorization expires on Linux based systems
- Etc.

EADS CCR

Dynamic routing

Mesh networks relies on dynamic routing

- Neighbourhood discovery
- Network announces
- Link table
- Routing table

Lots of networks use OLSR

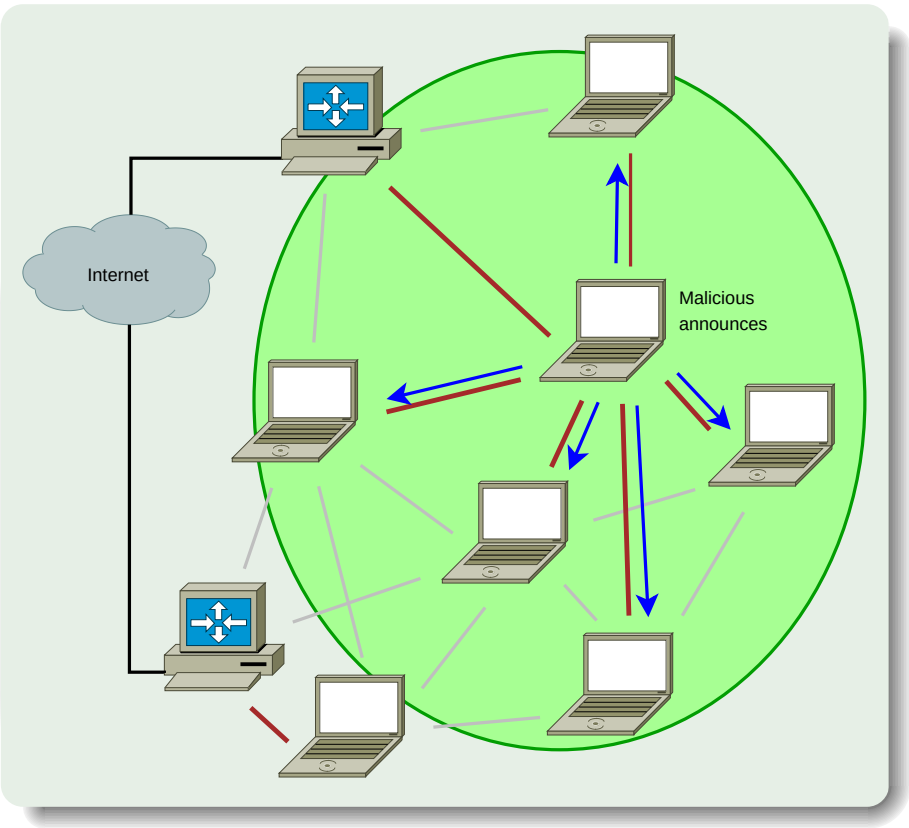
Dynamic routing abuse

No authentication/integrity measure

- Anybody can announce anything

Scenario

- Use a powerful antenna
- Announce Internet connectivity
- Gather traffic from part of network
- Play with connections



EADS CCR

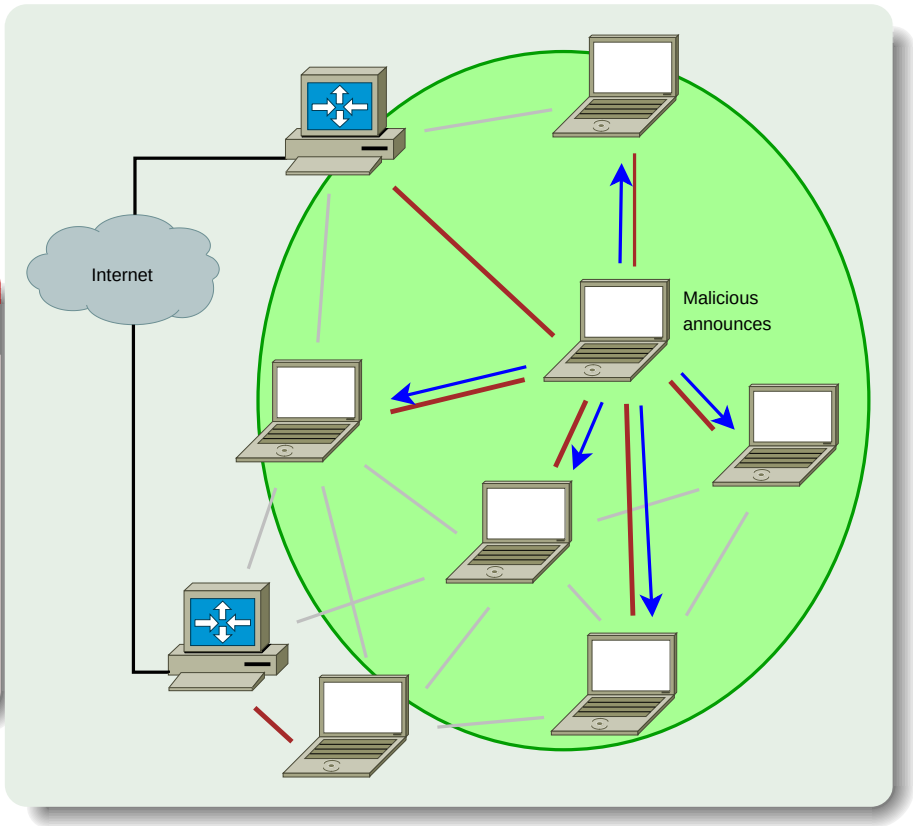
Dynamic routing abuse

No authentication/integrity measure

- Anybody can announce anything

Scenario

- Use a powerful antenna
- Announce Internet connectivity
- Gather traffic from part of network
- Play with connections



EADS CCR

Multipoint route injection

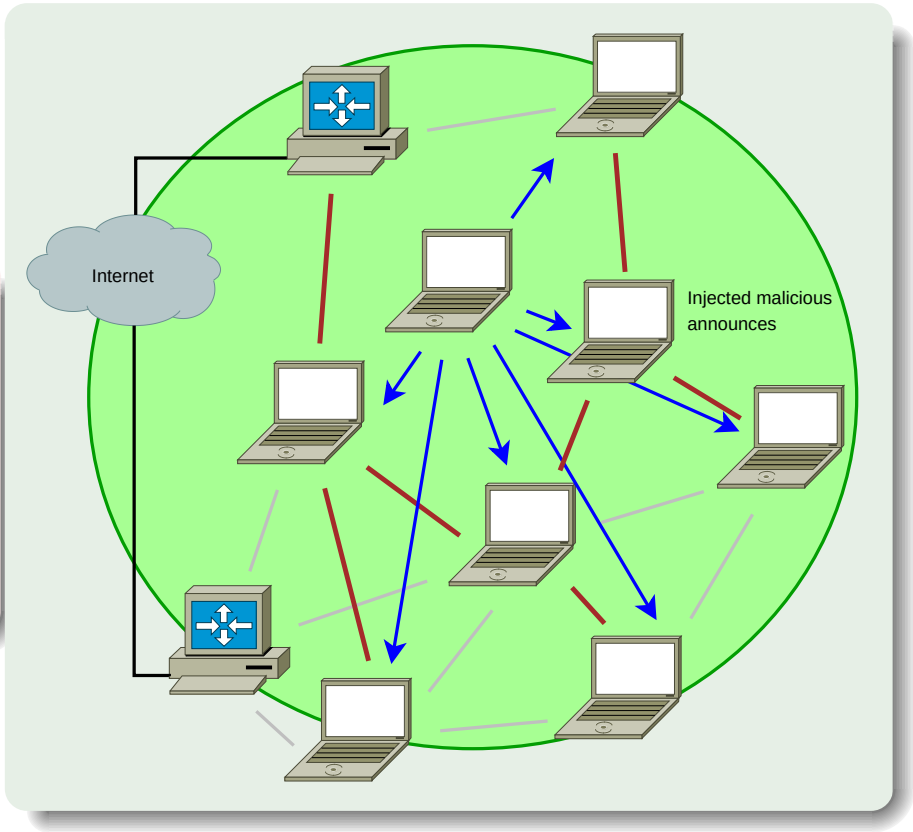
One can just inject OLSR messages

- without being part of network
- to multiple links

Route injection

- Includes neighbourhood
- Becomes more consistent
- Stays more stealth

Can use arbitrary messages using Wifitap



EADS CCR

Agenda

EADS CCR

All known "LAN attacks" are available

- LAN attacks (ARP, DHCP, DNS, etc.)
- Traffic interception and tampering
- Direct station attacks

Think of infamous personal firewalls exception for local network or loose firewall settings...

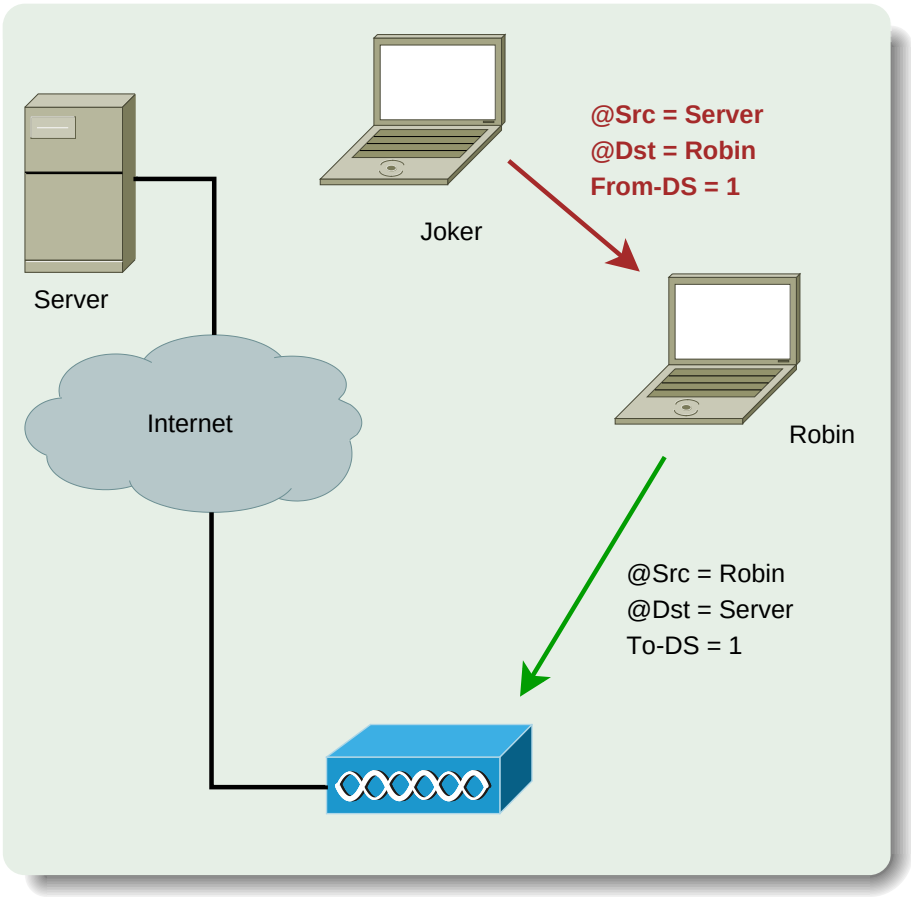
EADS CCR

Traffic tampering

WiFi communication can be listened on the air

- Listen to WiFi traffic
- Spot interesting requests
- Inject your own crafted answers
- You've done airpwn-like[AIRP] tool

Applications : ARP spoofing, DNS spoofing, malicious data injection, etc.



CCR

Demo

Demo

- DNS Spoofing
- Ping answering machine

EADS CCR

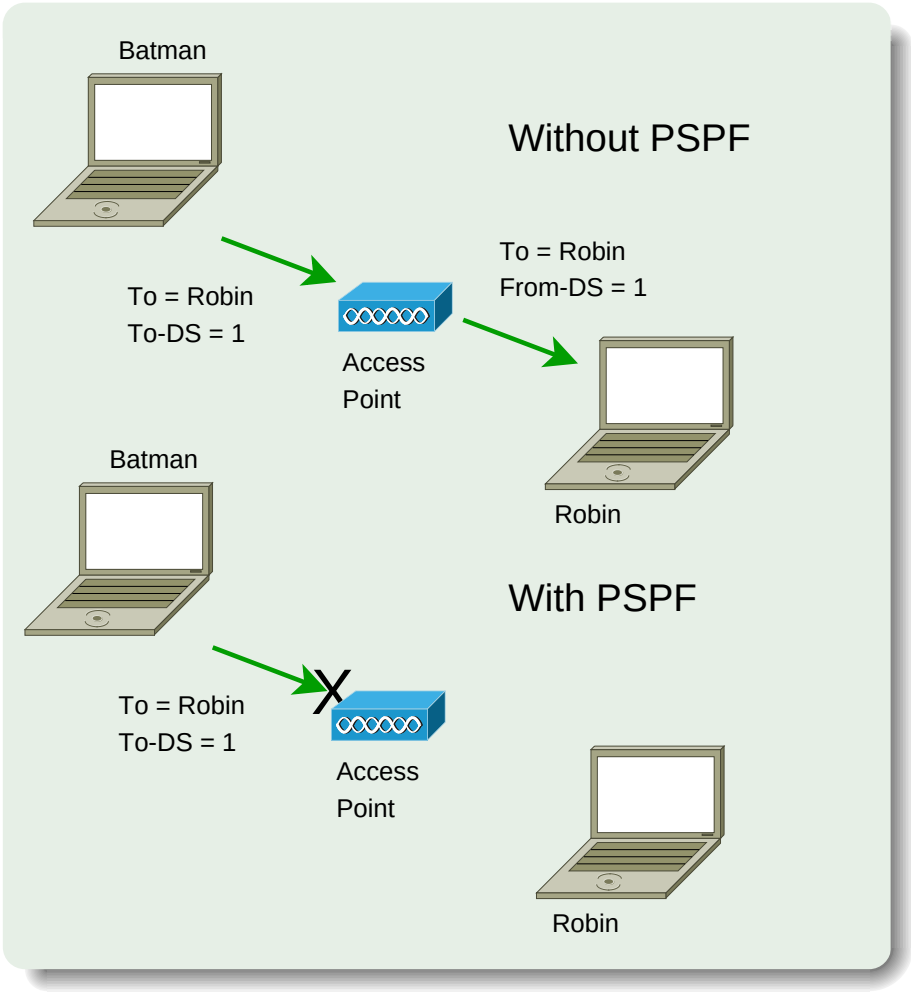
Stations isolation

Security feature that blocks traffic within BSS
Usually known as *station isolation*

- Station sends To-DS frame
- AP sees destination is in BSS
- AP drops the frame

No From-DS frame, so no communication[a] : stations can't talk to each other...

[a] Does not work between 2 APs linked via wired network

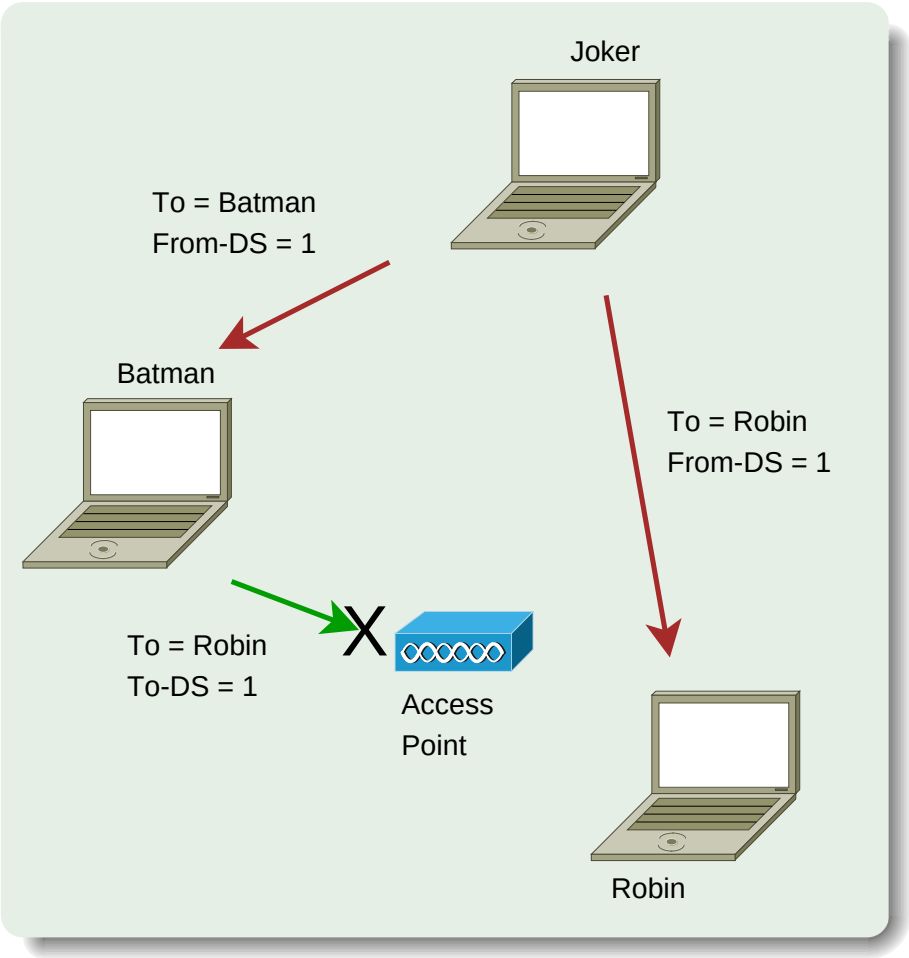


Isolation bypass using traffic injection

Joker can inject From-DS frames directly

- No need for AP approval
- You can spoof about anyone
- You're still able to sniff traffic

Traffic injection allows complete isolation bypass



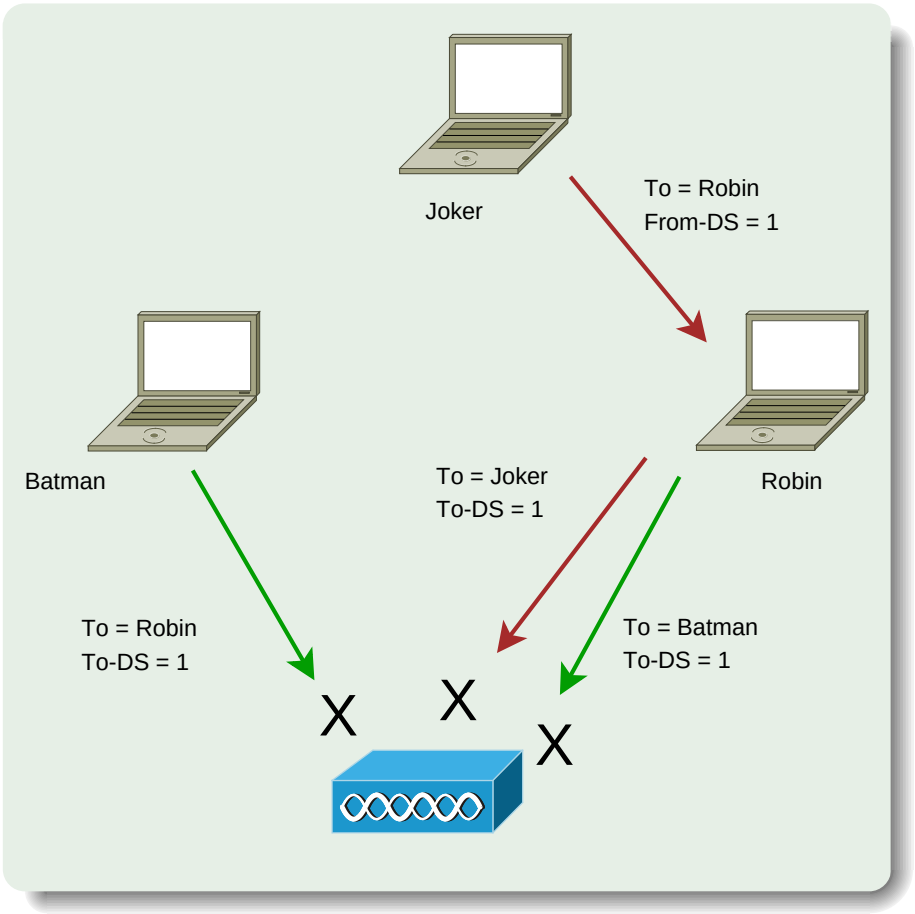
Bidirectionnal communication with injection

Sending packets the ninja way

Sending traffic directly to stations allows direct station to station communication, even if :

- AP applies restrictions
- AP refuses association
- AP is out of reach

Talking to stations the ninja way, without being associated



Attacking stations
Proof of concept : Wifitap

Needed a PoC for Cisco PSPF bypass and wrote Wifitap

- Written in Python[PYTH]
- Relies on Scapy[SCAP]
- Uses tuntap device and OS IP stack
- Use WiFi frame injection and sniffing

Wifitap allows communication with station despite of AP restrictions

Wifitap works for mesh networks as well

EADS CCR

Wifitap usage

```
# ./wifitap.py -h
Usage: wifitap -b <BSSID> [-o <iface>] [-i <iface> [-p]]
               [-s <SMAC>] [-w <WEP key> [-k <key id>]]
               [-d [-v]] [-h]
     -b <BSSID>     specify BSSID for injection
     -o <iface>     specify interface for injection
     -i <iface>     specify interface for listening
     -s <SMAC>      specify source MAC address
     -w <key>       WEP mode and key
     -k <key id>    WEP key id
     -d             activate debug
     -v             verbose debugging
     -h             this so helpful output
```

EADS CCR

Wifitap in short

How does it work ?

Sending traffic

- Read ethernet from tuntap
- Add 802.11 headers
- Set BSSID, From-DS and WEP if needed
- Inject frame over WiFi

Receiving traffic

- Sniff 802.11 frame
- Remove WEP if needed and 802.11
- Build ethernet frame
- Send frame through tuntap

Attacker does not need to be associated (AP or Adhoc)

EADS CCR

Wifitap in short

How does it work ?

Sending traffic

- Read ethernet from tuntap
- Add 802.11 headers
- Set BSSID, From-DS and WEP if needed
- Inject frame over WiFi

Receiving traffic

- Sniff 802.11 frame
- Remove WEP if needed and 802.11
- Build ethernet frame
- Send frame through tuntap

Attacker does not need to be associated (AP or Adhoc)

EADS CCR

Wifitap in short

How does it work ?

Sending traffic

- Read ethernet from tuntap
- Add 802.11 headers
- Set BSSID, From-DS and WEP if needed
- Inject frame over WiFi

Receiving traffic

- Sniff 802.11 frame
- Remove WEP if needed and 802.11
- Build ethernet frame
- Send frame through tuntap

Attacker does not need to be associated (AP or Adhoc)

EADS CCR

Demo

Demo

- Wifitap in action

Hotspots with isolation

Some hotspots implement isolation to prevent clients from attacking each other

- Does not protect against "session" hijacking
- Attacker must then to take over victim's session
- Victim does not have access anymore, and still pays for it

And among all, it's pretty useless...

More hotspot bypassing...

Hijacking people authorization is not very kind

- Use Wifitap to bypass isolation
- Now you can route back his traffic to your victim

Your victim and you are both able to surf transparently

Now, you "can be a true gentlemanly [h|cr]acker" [ISCD] ;)

EADS CCR

Agenda

EADS CCR

Conclusion

So you thought dropping the wire was that easy ?

- No privacy, no integrity
- Public accesses are just so insecure
- Crackers do know about that

EADS CCR

Conclusion

What do we do to fix that ?

Clients

- Open network services can't be trusted
- Open network traffic neither
- Think authentication, encryption, VPN

Don't forget to tunnel DNS as well :)

Infrastructure

- Considering WEP ? Forget it !
- Consider real stuff : WPA/WPA2 w/EAP
- Now supported on most devices/OS

Conclusion

What do we do to fix that ?

Clients

- Open network services can't be trusted
- Open network traffic neither
- Think authentication, encryption, VPN

Don't forget to tunnel DNS as well :)

Infrastructure

- Considering WEP ? Forget it !
- Consider real stuff : WPA/WPA2 w/EAP
- Now supported on most devices/OS

Conclusion

What do we do to fix that ?

Clients

- Open network services can't be trusted
- Open network traffic neither
- Think authentication, encryption, VPN

Don't forget to tunnel DNS as well :)

Infrastructure

- Considering WEP ? Forget it !
- Consider real stuff : WPA/WPA2 w/EAP
- Now supported on most devices/OS

Thank you for your attention and...

Greetings to...

- **BCS Asia 2006** people, partners and sponsors
- **EADS CRC/DCR/STI/C team**
- **Rstack.org** team
  `http://www.rstack.org/`
- **MISC Magazine**
  `http://www.miscmag.com/`
- **French Honeynet Project**
  `http://www.frenchhoneynet.org/`

Download theses slides from `http://sid.rstack.org/`

EADS CCR

Agenda

EADS CCR

EADS CCR

Demos

- Captive portal bypass
- Traffic tampering
- Bidirectional isolation bypass

We Proudly R3wt

EADS CCR

EADS CCR

Bibliography I


[ABOB] Bernard Aboba, The Unofficial 802.11 Security Web Page, http://www.drizzle.com/~aboba/IEEE/


[BLA02] C. Blancher, Switched environments security, a fairy tale, 2002, http://sid.rstack.org/pres/0207_LSM02_ARP.pdf


[BLA03] C. Blancher, Layer 2 filtering and transparent firewalling, 2003 http://sid.rstack.org/pres/0307_LSM03_L2_Filter.pdf


[BLA06] C. Blancher, WiFi traffic injection based attacks, 2005-2006 http://sid.rstack.org/pres/0602_Securecon_WirelessInject

Bibliography II


[AIRP] Airpwn, http://www.evilscheme.org/defcon/


[ARPS] Arp-sk, http://sid.rstack.org/arp-sk/


[EBT] Ebtables, http://ebtables.sourceforge.net/


[KRM] Karma, http://theta44.org/karma/


[NSTX] Nstx, http://nstx.dereference.de/nstx/


[OZY] OzymanDNS, http://www.doxpara.com/ozymandns_src_0.1.tgz


[PYTH] Python, http://www.python.org/


[SCAP] Scapy, http://www.secdev.org/projects/scapy/

EADS CCR

Bibliography III

 [WTAP] Wifitap, http://sid.rstack.org/index.php/Wifitap_EN

 [ISCD] ISC Handler's Diary, http://isc.sans.org/diary.php?date=2005-06-26