Attacking WiFi networks with traffic injection

Why open and WEP 802.11 networks really suck

Cédric BLANCHER

cedric.blancher@eads.net
EADS Corporate Research Center
EADS/CCR/DCR/SSI

sid@rstack.org
Rstack Team
http://sid.rstack.org/

RECON - Montréal - Canada
17-19 June 2005
http://recon.cx/

Agenda

EADS CCR

Spam...

<commercial>
I work for EADS Corporate Research Center, IT Security dpt

If you happen to need a A380 or Tigre helicopter, see me after my talk :)
</commercial>

Plan

EADS CCR

Introduction

We already know 802.11 networks are weak

- Open networks are prone to any well-known LAN perimeter attack
- WEP is vulnerable

So why this talk ?

Introduction

This talk is "people never learn" story

Goals

- Understand that WiFi open networks are unsecure for users
- Understand that WEP really sucks and should not be used anymore
- Understand that there's no salvation outside WPA/WPA2

Maybe make people learn something, at least (in case they don't know yet)

EADS CCR

Introduction

Traffic injection has changed things

- Increase DoS capabilities
- Dramaticly decreased WEP cracking achievement time
- Allows station traffic attacking
- Allows station attacking

But still...

- Most ISPs selling wireless/router/modem based access only provide WEP support
- Most commercial hotspots are still open networks...

EADS CCR

Plan

EADS CCR

802.11 basics

802.11 is a wireless communication IEEE standard commercialy known as WiFi

- CSMA/CA based
- Infrastructure vs. Ad-hoc
- Association concept
- Management vs. data traffic

802.11 "early" security

WiFi protection scheme is WEP (Wired Equivalent Privacy)

- Authentication through challenge/response
- Confidentiality with RC4 cipher using 24bits IV plus fixed key
- Integrity with CRC32 on cleartext payload

EADS CCR

EADS CCR

Arbitrary frames injection

Quite old but non common functionnality

- Needs appropriate firmware
- Needs appropriate driver
- Needs appropriate library/software

Some tools exist[1], but mainly focus on management traffic
Hostap[2] based stuff, but Prism2 firmwares are somehow reluctant

[1] e.g. `http://sourceforge.net/projects/airjack/`
[2] `http://hostap.epitest.fi/`

EADS CCR

Toolkit

Proper adapter and driver

- Hostap, but limited to some kind of frames
- Atheros/Madwifi[3], patched for traffic injection
- Intersil Prism54[4], development SVN snapshot

Atheros remains the most popular chipset due to a documented HAL

[3] http://madwifi.sf.net/
[4] http://prism54.org/

Traffic injection 101

To inject traffic

1. Load driver and activate adapter
2. Put adapter into monitor mode (real 802.11 mode)
3. Set appropriate channel
4. Open RAW socket on interface
5. Use your socket

Still, you need to implement a 802.11/MAC/IP stack over your socket and/or good libs and tools so you can communicate

EADS CCR

Plan

EADS CCR

EADS CCR

Management traffic

Suppose to control DSS state, such as associations...

Management traffic is a regulation traffic that is completly unprotected
Management traffic is extremely prone to spoofing

Tampering management traffic

You alter DSS current state by tampering management traffic

- Reject association requests
- Inject disassociation frame
- Inject fake associations
- Wake up devices in sleep mode
- Etc.

Mainly DoSes...

EADS CCR

Management traffic generation

Management traffic is easy to generate and inject
See Scapy[5] packets classes

- Dot11
- Dot11Disas
- Dot11AssoResp
- Dot11ReassoResp
- Dot11Deauth
- etc.

See Scapy in action :
`http://www.secdev.org/conf/scapy_csw05.pdf`

[5] `http://www.secdev.org/projects/scapy/`

EADS CCR

Building AP from scratch

For AP mode, you need to inject

- Beacon frames
- Associations requests answers
- Management traffic
- Data frames acking

Rogue APs

If you can be an AP, you can also be a fake one...

- Cheap solution for traffic redirection
- Cheap attack against automatic "WiFi network managers"[a]

Rogue AP is the poor man attack that works so well

[a] `http://theta44.org/main.html`

EADS CCR

WEP breaking basics

WEP is RC4 based, which is XOR based

- Cleartext attacks (e.g. authentication challenge)
- PRGA/IV couple table construction
- Fluhrer, Mantin and Shamir attack based on first bytes of key being weak (weak IVs)
- Korek optimization of FMS attack based on solved cases

Last attacks need traffic gathering

Modified packet injection

Let C be our cleartext message and Mod a C slight modification
Let $C' = C \oplus Mod$

Some maths

$$\begin{aligned} P &= WEP(C + ICV(C)) \\ &= (C + ICV(C)) \oplus RC4(IV + K) \\ P' &= (C' + ICV(C')) \oplus RC4(IV + K) \\ &= (C + ICV(C)) \oplus RC4(IV + K) \oplus (Mod + ICV(Mod)) \\ &= P \oplus (Mod + ICV(Mod)) \end{aligned}$$

This means you can inject arbitrary WEP frames and have them decrypted...

Consequences

We can inject arbitrary traffic through WEP without key knowledge

- Launch oracle based attacks
- Stimulate network in order to create traffic (e.g. aireplay)

Full WEP cracking is no more relying on passive listening

Korek Chopchop attack

Korek published[6] a one packet decrypting attack based on oracle

1. Grab a packet
2. Modify one byte
3. Reinject
4. Deduce byte value

Easy isn't it ?

[6] http://www.netstumbler.org/showthread.php?t=12489

Korek-Devine WEP cracking

Using Chopchop and some FMS optimizations from Korek, Christophe Devine released Aircrack[7]

1. Use Chopchop to spot an answered ARP request
2. Inject ARP request again and again
3. Stimulate traffic and unique IV collection
4. Terminate WEP key cracking within few seconds

Full WEP cracking is now question of minutes or so

And aircrack still can be optimized...

[7] http://www.cr0.net:8040/code/network/aircrack/

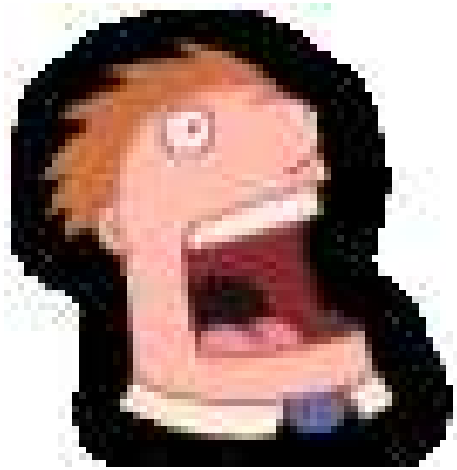
EADS CCR

Commercial WiFi hospots

Commercial public Internet access

- Captive portal based system
- Authentication to billing system through web portal
- Authorization for Internet access
- Authorization tracking

It would be nice to be free... For free !



EADS CCR

MAC based authorization tracking

Authorized 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

Recipe : spoof an authorized MAC address, get an IP and surf

IP based authorization tracking

Authorized 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

Recipe : ARP poison gateway for authorized IP, spoof and surf

MAC+IP addresses based authorization tracking

The smart way fo tracking people ?

- Previous technic won't help because of MAC address checking
- Hint : IP layer does not care about MAC layer
- ARP cache poisoning and IP spoofing
- Send traffic with spoofed MAC address

Recipe : Same as before, plus MAC spoofing, then surf

EADS CCR

Configuration based tricks

Some gateways are misconfigured

- HTTP proxy left open on gateway
- ESTABLISHED,RELATED -j ACCEPT prevents connections drop when authorization expires on Linux based systems
- Administration network on the same VLAN, accessible through WiFi
- Etc.

Misconfigurations tend to be unusual

EADS CCR

What about associated stations ?

Associated stations are almost naked

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

Manufacturers provides so called "solutions", mainly station to station communication prevention systems (e.g. C***o PSPF)

EADS CCR

Traffic tampering

WiFi communication are just opened on the air

- Listen to WiFi traffic
- Identify given requests
- Inject your own answers
- Clap clap, you've done airpwn[8] like tool

Think of just injecting nasty things in HTTP traffic just in case someone would dare use MSIE

[8] http://www.evilscheme.org/defcon/

Communication injection

Send traffic directly to station without AP authorization

- Allows PSPF bypass
- Allows communicating while AP out of reach
- Allows communication while AP refuses association

A smart of for reaching stations without being associated

Proof of concept : Wifitap

Needed a PoC for Cisco PSPF bypass and wrote Wifitap

- Written in Python[9]
- Relies on Scapy[10]
- Uses tuntap device and OS IP stack
- Use WiFi frame injection and sniffing

Wifitap allows communication with station despites AP restrictions

[9] http://www.python.org/
[10] http://www.secdev.org/projects/scapy.html

EADS CCR

Wifitap in short

How Wifitap works

Sending traffic

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

Receiving traffic

- Sniff 802.11 frame
- Remove WEP layer if needed
- Remove 802.11 headers
- Send ethernet through tuntap

Attacker does not need to be associated

EADS CCR

Quick demo...

We Proudly R3wt

Download Wifitap at
`http://sid.rstack.org/code/wifitap.tgz`

EADS CCR

More hotspot bypassing...

Hijacking a guy authorization is not very kind

- Use Wifitap to bypass PSPF
- Now you can send back his traffic to the poor victim

Now your victim and you are able to surf transparently

Plan

EADS CCR

WPA

Transitional recommandation from WiFi Alliance extracted from IEEE work for infrastructure networks

- New authentication scheme based on PSK or 802.1x
- New key generation and scheduling scheme for keys
- New integrity check through Michael MIC with sequencing

Pretty solid solution that can prevent injection/replay

EADS CCR

802.11i

Standard from IEEE for WiFi security
WPA2 is a recommandation from WiFi alliance based on 802.11i

- Authentication using 802.1x
- Ciphering using AES-CCMP
- Integrity check using CCMP MIC

Return to the roots and use of a real adapted ciphering solution

EADS CCR

And then ?

WPA and WPA2 provide strong mechanisms
Some flaws on WPA

- Accelerated attack against PTK key (105bits vs. 128bits)
- WPA PSK bruteforce

Attack counter-measures can be used to trigger DoS

- Wild traffic replay
- Wild dumb traffic injection

Nothing will protect from layer 1 based DoS attackes (bandwidth reservation, jamming)

EADS CCR

Plan

EADS CCR

Conclusion

WiFi environnement are highly insecure and tough to secure
You just can't cope with amateur style protection...

Then...

- Don't use WEP anymore
- Dont' use open network for public access
- Migrate to WPA, then WPA2 as soon as possible

EADS CCR

Rstack powered talk...

Greetings to...

- **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