Welcome to

Penetration testing III
Wireless sikkerhed

Henrik Kramselund he/him han/ham hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Codeberg

pentest-III-foredrag.tex in the repo security-courses

Plan

Subjects

- Introduce pentest in wireless applications and related technologies
- Basic wi-fi security concepts
- Applying basic security assessment skills
- Point towards some of the most important resources in this subject
- Introduce scanning with aircrak-ng suite of programs and others
- Make it possible to get started hacking on wi-fi networks

Demos and recommendations for exercises

- Running various tools

Whenever it say exercise, it will be a demo!

Goals

Don't Panic!

Inspire you to implement wireless networks securely

by showing insecurities in the previous versions

and listing alternatives for long term wireless security

Goals for today, continued

> It is not clear that the link layer is the right one for security. In a coffeeshop, the security association is terminated by the store: is there any reason you should trust the shopkeeper? Perhaps link-layer security makes some sense in a home, where you control both the access point and the wireless machines. However, we prefer end-to-end security at the network layer or in the applications.

Source: Cheswick-chap2.pdf Firewalls and Internet Security: Repelling the Wily Hacker , Second Edition, 2003, William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin

Todays goals:

- Introduce wireless networks and **security in them**
- Present the common security standards, and some tools used
- Discuss how to secure wireless best, infrastructure and/or encryption
- Wi-Fi security is more than just encryption

Agreements for testing networks

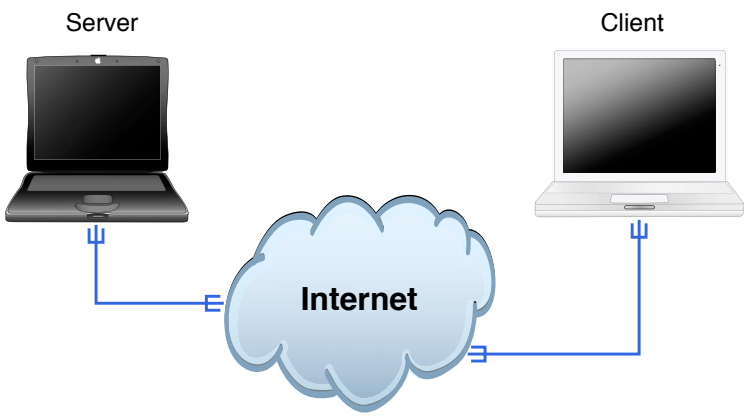
Danish Criminal Code
Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, der uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem.
Husk også brevhemmeligheden

Hacking can result in:

- Getting your devices confiscated by the police
- Paying damages to persons or businesses
- If older getting a fine and a record – even jail perhaps
- Getting a criminal record, making it hard to travel to some countries and working in security
- Fear of terror has increased the focus – so dont step over bounds!

Asking for permission and getting an OK before doing invasive tests!

Internet today



Clients and servers

Rooted in academia

Protocols that are from 1983 and some older

Originally very little encryption, now mostly on HTTPS/TLS

Why talk about hacking wi-fi networks

wireless 802.11

- Everything is wireless today
- Even though HTTPS/TLS used for data transport in most applications
- Core protocols like DNS are NOT encrypted, standards are coming
- Gaining access to a LAN with wireless can open up the whole network to attacks
- We need to deploy wireless technologies securely, even in the face of vulnerabilities found in protocols, algorithms, devices etc.

TL;DR Use segmented networks with updated devices and strong encryption

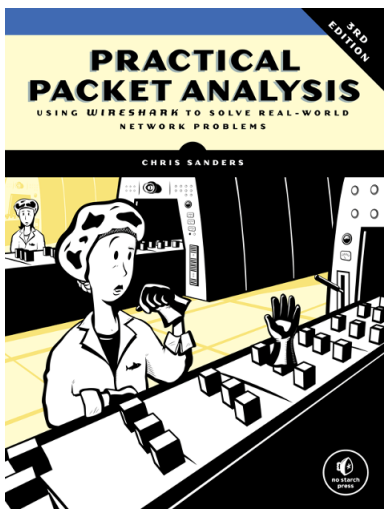
Materials – where to start

- This presentation – slides for today, start here:
  https://github.com/kramse/security-courses/tree/master/presentations/pentest/pentest-II-foredrag
- Setup instructions for creating a Kali virtual machine:
  https://github.com/kramse/kramse-labs
- Communication and Network Security course

  https://github.com/kramse/security-courses/tree/master/courses/networking/communication-and-network-security

  Especially 6-Wifi-Security.pdf
- Download the *exercise booklet* for the Pentest courses:
  https://github.com/kramse/security-courses/tree/master/presentations/pentest/pentest-II-foredrag
  Using Nmap can show access afterwards and point out insecure devices

Books and Educational Materials



Practical Packet Analysis, Using Wireshark to Solve Real-World Network Problems by Chris Sanders, 3rd Edition April 2017, 368 pp. ISBN-13: 978-1-59327-802-1 https://nostarch.com/packetanalysis3

Anything you know about technology will help you hack it, so learn basic functionality first

Reading Summary, continued

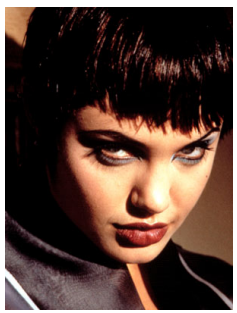
PPA chapter 12: Packet Analysis for Security

- Reconnaissance An attacker's first step
- SYN Scan and fingerprinting
- Traffic Manipulation ARP Cache Poisoning / spoofing
- Analyzing traffic from malware, exploit kits and ransomware

PPA chapter 13: Wireless Packet Analysis

- Sniffing channels
- Wireless card modes, Managed, Ad-hoc and Monitor mode
- 802.11 packet structure
- Wireless security

Hacker tools



- Everyone use similar tools, scanning in monitor mode etc.
- I recommend Aircrack-ng as it has excellent documentation https://www.aircrack-ng.org/
- These tools are low-level and functionality is often automated in other apps, even mobile apps
- Afterwards we again use common pentesting tools:
- Portscanning Nmap, Nping – test ports and services, Nping is great for firewall admins https://nmap.org
- Wireshark avanceret netværkssniffer - http://http://www.wireshark.org/

Picture: Acid Burn / Angelina Jolie Hackers 1995

What happens now?

Think like a hacker

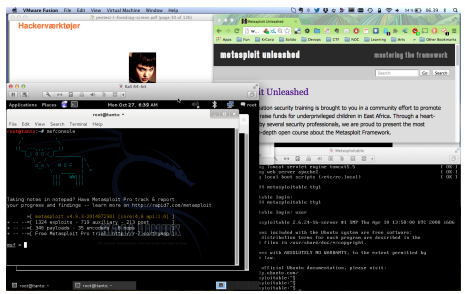
Reconnaissance

- ping sweep, port scan
- OS detection – TCP/IP or banner grabbing
- Service scan – rpcinfo, netbios, ...
- telnet/netcat interact with services

Exploit/test: Metasploit, Nikto, exploit programs

Try to limit to wireless today

Hacker lab setup



- Hardware: modern laptop CPU with virtualisation
  Dont forget to enable hardware virtualisation in the BIOS
- Virtualisation software: VMware, Virtual box, HyperV pick your poison
- Linux server system: Debian amd64 64-bit https://www.debian.org/
- Setup instructions can be found at https://github.com/kramse/kramse-labs
- Target: Wireless networks!
- Bought some *shitty routers*

Hacking is magic

Hacking looks like magic – especially buffer overflows

Hacking is not magic

Hacking only demands ninja training and knowledge others don't have

It is like a puzzle, we need this, this and that. Make it happen in a repeatable way.

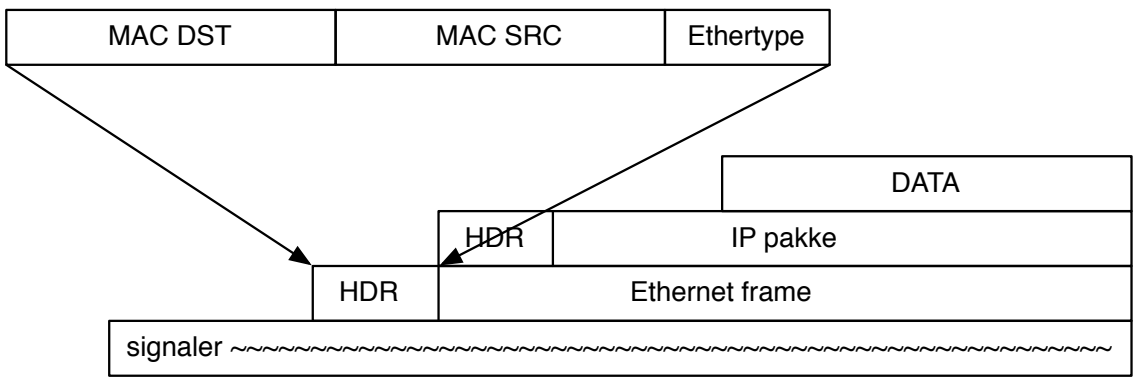
Hacking example not magic MAC addresses

A MAC address (short for medium access control address) is a **unique identifier** assigned to a **network interface controller (NIC)** for use as a network address in communications within a network segment.
This use is common in most IEEE 802 networking technologies, including **Ethernet, Wi-Fi, and Bluetooth**.
Within the Open Systems Interconnection (OSI) network model, MAC addresses are used in the medium access control protocol sublayer of the data link layer. As typically represented, MAC addresses are **recognizable as six groups of two hexadecimal digits**, separated by hyphens, colons, or without a separator.
MAC addresses are primarily **assigned by device manufacturers**, and are therefore often referred to as the **burned-in address**, or as an Ethernet hardware address, hardware address, or physical address. Each address can be stored in the interface hardware, such as its read-only memory, or by a firmware mechanism. **Many network interfaces, however, support changing their MAC addresses**.

Source: https://en.wikipedia.org/wiki/MAC_address

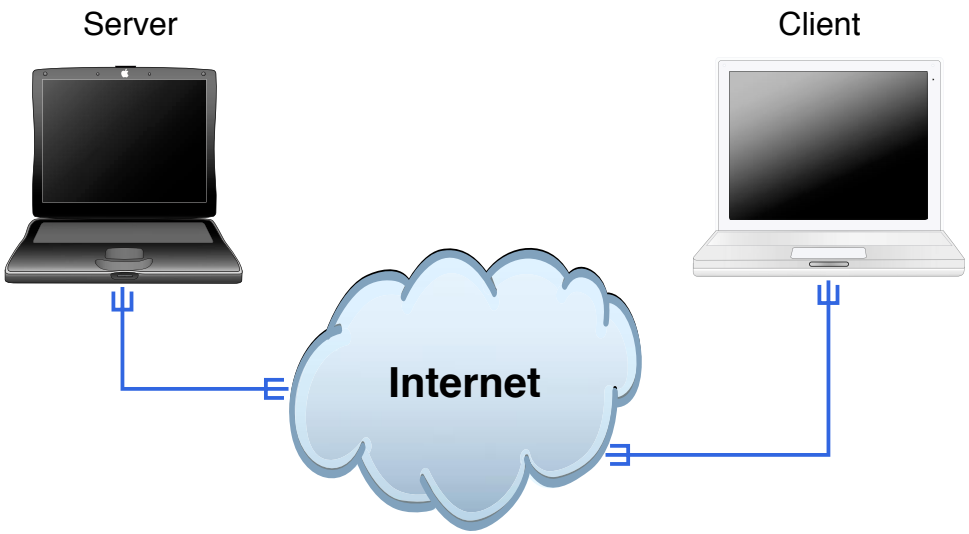
- Great a unique address, we can use that for security!!!1111

MAC filtering



- Filtering on the *unique* address sounds great
- Allow only a list of permitted addresses, cards – systems to join!
- Wait, anyone can change their address on their cards?! Can they guess an allowed one of the 48 bits?

Demo

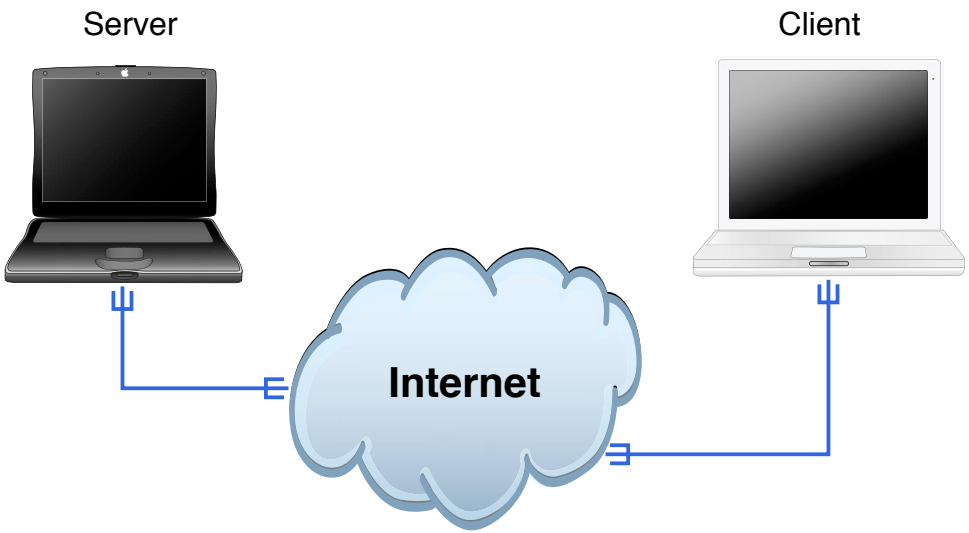


Now lets see the demo

⚠ Wardriving Up to 60min

which is number **3** in the exercise PDF.

Demo



Now lets see the demo

⚠ Aircrack-ng 30 min

which is number **4** in the exercise PDF.

Myths about MAC filtering

This example of MAC filtering is one of many security myths

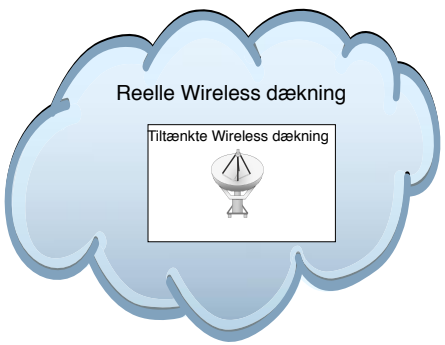
Why does it happen?

- Marketing - vendors keep selling producs listing MAC filtering as a security measure
- Consumers has no knowledge about this – choose the product with the longest list/the most features
- Very few people actually look into this – thanks for being here today!

Help spread knowledge about insecure and secure methods for data and systems

MAC filtering illustrated

Consequences and Impact



- Can be worse than attacks across the internet – anonymous
- Does not require physical access inside building – antennna and 100m
- If broken then it will allow access to LAN and systems inside the organisation, and/or attacks on client systems

More structured walk-through

Introduction – terms and technologies we cover

Basics in Wireless IEEE 802.11 – as seen in wardriving

Hacking wireless networks

Security technologies in IEEE 802.11 short history lesson

Security technologies in **IEEE 802.11i** – Robust Security Networks

Tools airodump og aircrack-ng in a little more detail

Packet injection tools – maybe not swown in detail

Recommendations for deploying wireless networks – guest networks, firewalls and segmentation

Note: wireless security is definitely not only the encryption methods

Tools

- Aircrack-ng is a suite of tools
- Wirelessscanner - Kali and Airodump
- Wireless Injection - aireplay-ng

Wireless hardware

Varenummer: 2225730

TP-Link TL-WN722N

Hi-Speed USB - 802.11b, 802.11g, 802.11n

På lager, 1-2 dages levering
(Billigste fragt: 0 kr.)
Ret land

Køb

120,00 kr.
(96,00 kr.)

4 stk på lager i Århus
0 stk på lager i Viborg
0 stk på lager i København

Laptop or Netbook, I typically use USB wireless cards, not the built-in!

Access Points - get a small selection for testing

Author of aircrack-ng recommended these: TP-Link MR3020 or TP-Link WR902AC Access Point. USB cards AIfa AWUS036AXML, AWUS036AXM, AWUS036ACM or AWUS036NHA

It can be hard to find the right card with the right chipset, versions change

Wifi Pineapple

Source: https://shop.hak5.org/products/wifi-pineapple

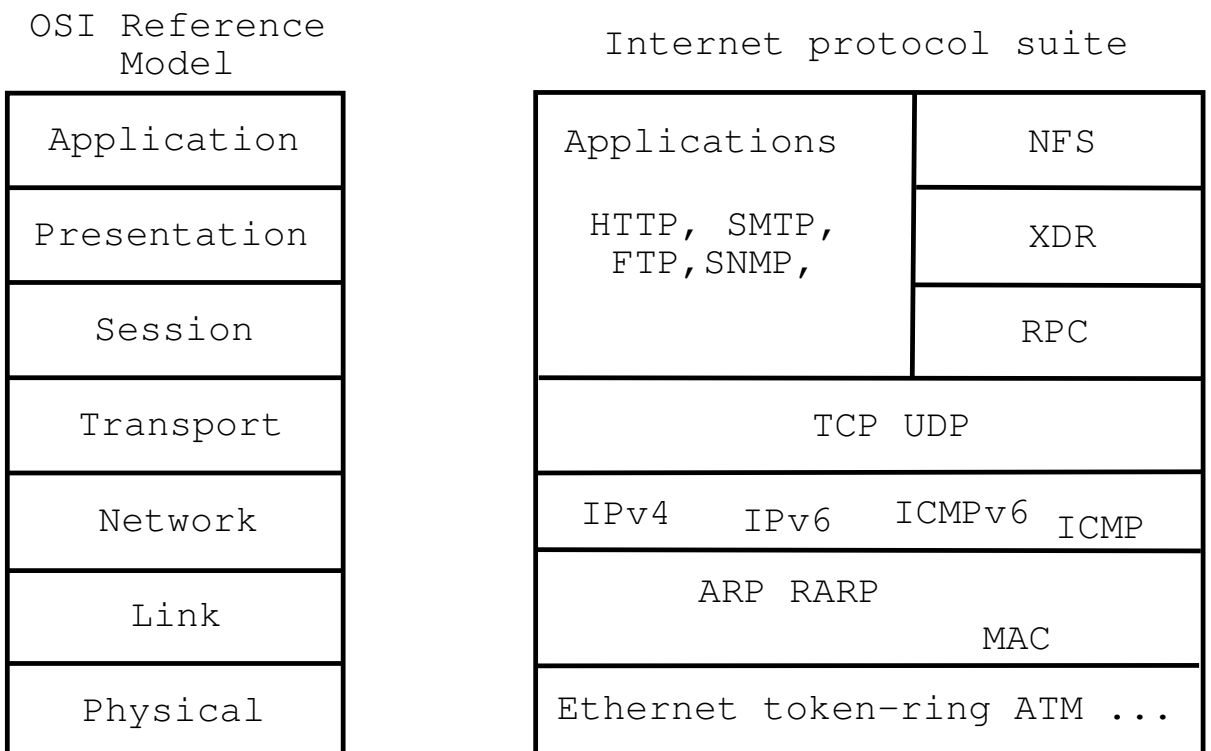
- Various wi-fi platforms exist. They can be nice, and typically have a web interface or GUI
- I have tried multiple versions of the wifi pineapple
- I haven't bought any and prefer the details of the low-level tools myself

Kali Nethunter

- **802.11 Wireless Injection** and **AP mode** support with multiple supported USB wifi cards.
- Capable of running **USB HID Keyboard attacks**, much like the **Teensy** device is able to do.
- **Supports BadUSB MITM attacks**. Plug in your Nethunter to a victim PC, and have your traffic relayed though it.
- Contains a **full Kali Linux toolset**, with many tools available via a simple menu system.
- **USB Y-cable support** in the Nethunter kernel – use your OTG cable while still charging your Nexus device!
- **Software Defined Radio support**. Use **Kali Nethunter** with your HackRF to explore the wireless radio space.

Source: https://www.kali.org/kali-linux-nethunter/

OSI and Internet Protocols



Recommended technologies to learn

So to accomplish the goal of performing wireless attacks efficiently you need some basics

Networking: Basic Protocols from the Internet Protocols suite IP/TCP, or TCP/IP

- Basic Protocols from TCP/IP, Wi-Fi: IPv4 and IPv6 – addresses and ports/services
- Transport Layer: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)
- Common upper layer: Domain Name System (DNS)
- Encrypted/secure versions like (HTTPS) which uses Transport Layer Security (TLS)
- Basic encryption as used and broken WEP, WPA(1) PSK
- Basic encryption and still used WPA2 PSK and Enterprise
- Later add WPS, WPA3 and SAE
- Practice using your home network – you control it, and have the passwords

This will *probably* keep you busy for a while ☺

Wireless technologies IEEE 802.11

- Since its introduction in 1997, the ongoing evolution of IEEE 802.11 Wi-Fi standards has led to much faster data transmission rates, longer ranges, and more reliable and secure connections.
- IEEE 802.11ax™, or Wi-Fi 6, is the most recent standard in the IEEE 802.11 series published in 2021. It supports the increasing use of Wi-Fi in data-heavy and new applications such as video and cloud access.
- IEEE P802.11be™, or Wi-Fi 7, is under development with an estimated completion in 2024. This standard represents a major evolutionary milestone with 4x faster data rates and twice the bandwidth.
- The IEEE 802.11 Working Group has formed special-interest groups to support many next-generation Wi-Fi applications, such as AI, AR/VR, and battery-free IoT.

Source: https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/ Older ones 802.11b 11Mbps, 802.11g 54Mbps, 802.11n endnu hurtigere

Typical use of wireless radios

Wireless Access Point

netværket - typisk Ethernet

An access point is basically a radio with Ethernet interfaces, a bridge, but can also be a whole router

Wireless networking security in IEEE 802.11

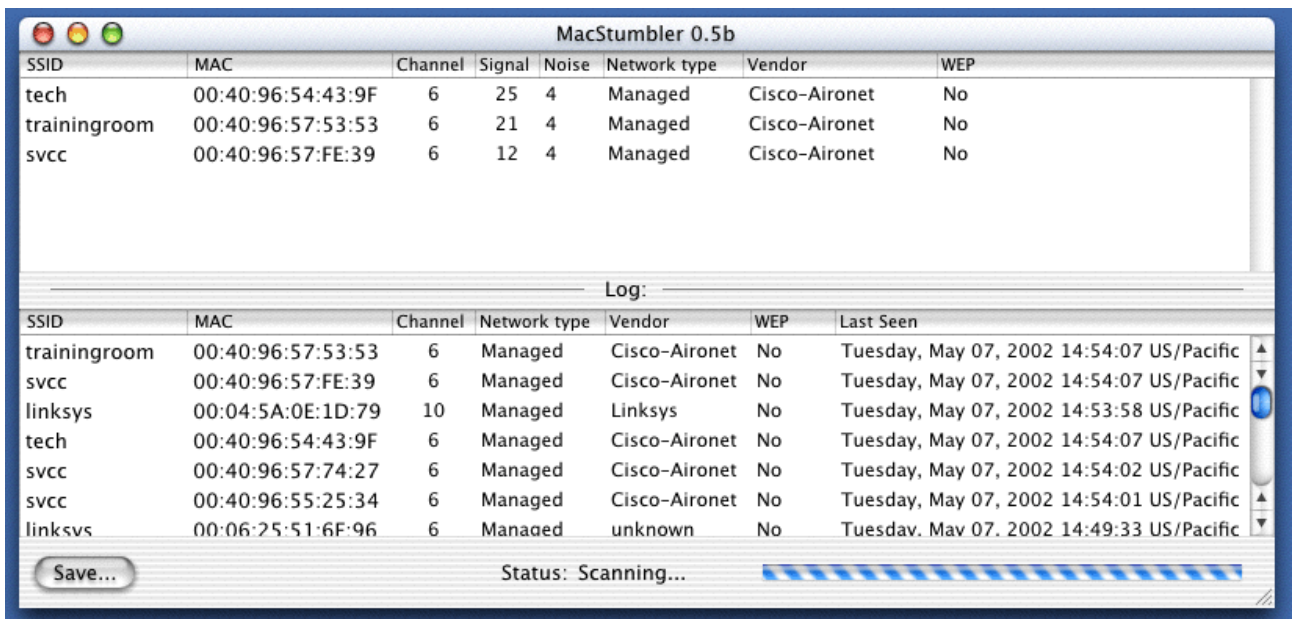
Based on a few prerequisites

- SSID – network name, network id
- Cryptography - Wi-Fi Protected Access
- Maybe MAC filtering – no need to bother with this

Watch out

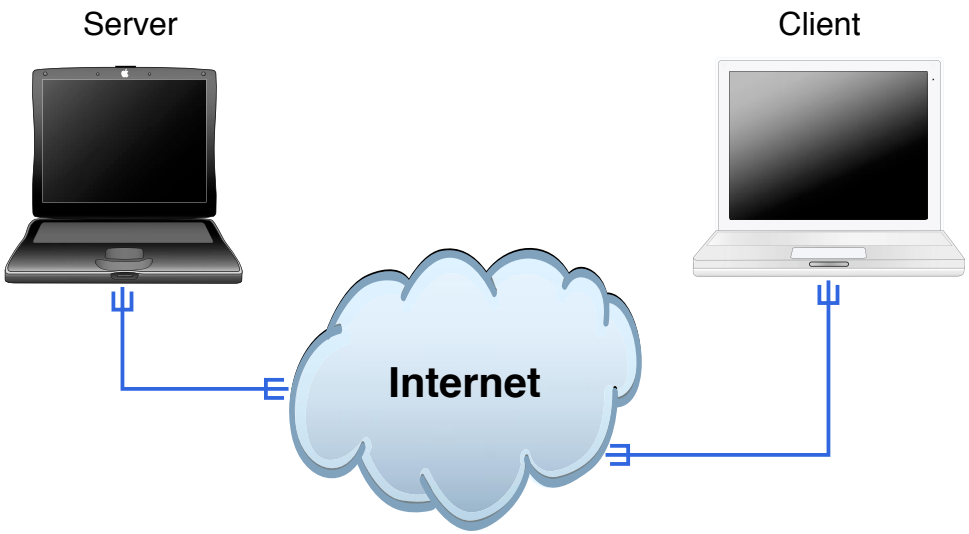
- WPA Pre-shared key (PSK) is based on a single shared key, does not scale well, hard to change
- WPA Enterprise is better and based on individual authentication – each user has a username and password (or certificate)

Demo: wardriving med airodump-ng



Screenshot from MacStumbler – I use airodump-ng from Aircrack-ng.org with Kali

Demo



Now lets see the demo

⚠ Wardriving Up to 60min

which is number 3 in the exercise PDF.

IEEE 802.11 Security fast forward

In 2001, a group from the University of California, Berkeley presented a paper describing weaknesses in the 802.11 Wired Equivalent Privacy (WEP) security mechanism defined in the original standard; they were followed by **Fluhrer, Mantin, and Shamir's** paper titled "Weaknesses in the Key Scheduling Algorithm of RC4". Not long after, Adam Stubblefield and AT&T publicly announced the first **verification of the attack**. In the attack, they were able to intercept transmissions and gain unauthorized access to wireless networks.

Source: http://en.wikipedia.org/wiki/IEEE_802.11

IEEE 802.11 Security fast forward

The IEEE set up a dedicated task group to create a replacement security solution, **802.11i** (previously this work was handled as part of a broader 802.11e effort to enhance the MAC layer). The Wi-Fi Alliance announced an **interim specification called Wi-Fi Protected Access (WPA)** based on a subset of the then current IEEE 802.11i draft. These started to appear in products in **mid-2003**. **IEEE 802.11i (also known as WPA2)** itself was ratified in **June 2004**, and uses government strength encryption in the **Advanced Encryption Standard AES,** instead of RC4, which was used in WEP. The modern recommended encryption for the home/consumer space is **WPA2 (AES Pre-Shared Key) and for the Enterprise space is WPA2 along with a RADIUS authentication server** (or another type of authentication server) and a strong authentication method such as EAP-TLS.

Source: http://en.wikipedia.org/wiki/IEEE_802.11

IEEE 802.11 Security fast forward

In January 2005, the IEEE set up yet another task group "w"to protect management and broadcast frames, which previously were sent unsecured. Its standard was published in 2009.[24]

In **December 2011**, a security flaw was revealed that affects wireless routers with the **optional Wi-Fi Protected Setup (WPS)** feature. While WPS is not a part of 802.11, **the flaw allows a remote attacker to recover the WPS PIN and, with it, the router's 802.11i password in a few hours**.

WPS is bad!

Source: http://en.wikipedia.org/wiki/IEEE_802.11

IEEE 802.11i

IEEE 802.11i-2004, or 802.11i for short, is an amendment to the original IEEE 802.11, implemented as Wi-Fi Protected Access II (WPA2). The draft standard was ratified on 24 June 2004. This standard specifies security mechanisms for wireless networks, replacing the short Authentication and privacy clause of the original standard with a detailed Security clause. In the process, the amendment **deprecated broken Wired Equivalent Privacy (WEP)**, while it was later incorporated into the published IEEE 802.11-2007 standard.

Replacement of WEP

802.11i supersedes the previous security specification, Wired Equivalent Privacy (WEP), which was shown to have security vulnerabilities. Wi-Fi Protected Access (WPA) had previously been introduced by the Wi-Fi Alliance as an intermediate solution to WEP insecurities. WPA implemented a subset of a draft of 802.11i. The Wi-Fi Alliance refers to their approved, interoperable implementation of the **full 802.11i as WPA2**, also called **RSN (Robust Security Network)**. 802.11i makes use of the **Advanced Encryption Standard (AES) block cipher**, whereas WEP and WPA use the RC4 stream cipher.[1]

Source: https://en.wikipedia.org/wiki/IEEE_802.11i-2004

WEP kryptering

WEP *kryptering* - med nøgler der specificeres som tekst eller hexadecimale cifre

typisk 40-bit, svarende til 5 ASCII tegn eller 10 hexadecimale cifre eller 104-bit 13 ASCII tegn eller 26 hexadecimale cifre

WEP er baseret på RC4 algoritmen der er en *stream cipher* lavet af Ron Rivest for RSA Data Security

De første fejl ved WEP

Oprindeligt en dårlig implementation i mange Access Points

Fejl i krypteringen - rettet i nyere firmware

WEP er baseret på en DELT hemmelighed som alle stationer kender

Nøglen ændres sjældent, og det er svært at distribuere en ny

Cryptography

Cryptography or cryptology is the practice and study of techniques for secure communication

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key, to ensure confidentiality, example algorithm AES

Public-key cryptography (like RSA) uses two related keys, a key pair of a public key and a private key. This allows for easier key exchanges, and can provide confidentiality, and methods for signatures and other services

Source: https://en.wikipedia.org/wiki/Cryptography

Kryptografiske principper

Algoritmerne er kendte

Nøglerne er hemmelige

Nøgler har en vis levetid - de skal skiftes ofte

Et successfuldt angreb på en krypto-algoritme er enhver genvej som kræver mindre arbejde end en gennemgang af alle nøglerne

Nye algoritmer, programmer, protokoller m.v. skal gennemgås nøje!

Se evt. Snake Oil Warning Signs: Encryption Software to Avoid
http://www.interhack.net/people/cmcurtin/snake-oil-faq.html

DES, Triple DES og AES

AES

Advanced Encryption Standard

DES kryptering baseret på den IBM udviklede Lucifer algoritme har været benyttet gennem mange år

Der blev i 2001 vedtaget en ny standard algoritme Advanced Encryption Standard (AES) som afløser Data Encryption Standard (DES)

Algoritmen hedder Rijndael og er udviklet af Joan Daemen og Vincent Rijmen.

Se også https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Formålet med kryptering

kryptering er den eneste måde at sikre:

fortrolighed

autenticitet / integritet

WEP sikkerhed

AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.

802.11b, using the Wired Equivalent Protocol (WEP), is crippled with numerous security flaws. Most damning of these is the weakness described in "Weaknesses in the Key Scheduling Algorithm of RC4 "by Scott Fluhrer, Itsik Mantin and Adi Shamir. Adam Stubblefield was the first to implement this attack, but he has not made his software public. AirSnort, along with WEPCrack, which was released about the same time as AirSnort, are the first publicly available implementaions of this attack. http://airsnort.shmoo.com/

major cryptographic errors

weak keying - 24 bit er allerede kendt - 128-bit = 104 bit i praksis

small IV - med kun 24 bit vil hver IV blive genbrugt oftere

CRC-32 som integritetscheck er ikke *stærkt* nok kryptografisk set

Authentication gives pad - giver fuld adgang - hvis der bare opdages *encryption pad* for en bestemt IV. Denne IV kan så bruges til al fremtidig kommunikation

Source: *Secure Coding: Principles and Practices*, Mark G. Graff og Kenneth R. van Wyk, O'Reilly, 2003

Konklusion: Kryptografi er svært

Åbent kursus på Stanford
http://crypto-class.org/

WEP cracking - airodump og aircrack

airodump - opsamling af krypterede pakker

aircrack - statistisk analyse og forsøg på at finde WEP nøglen

Med disse værktøjer er det muligt at knække *128-bit nøgler*!

Blandt andet fordi det reelt er 104-bit nøgler ☺

Links:
Tutorial: Simple WEP Crack
http://www.aircrack-ng.org/doku.php?id=simple_wep_crack

airodump opsamling

BSSID	CH	MB	ENC	PWR	Packets	LAN IP / # IVs	ESSID
00:03:93:ED:DD:8D	6	11		209	**801963**	**540180**	wanlan

Når airodump kører opsamles pakkerne

Lås airodump fast til een kanal, -c eller –channel

Startes med airmon og kan skrive til capture filer:

```
airmon-ng start wlan0
airodump-ng --channel 6 --write testfil wlan0mon
```

aircrack - WEP cracker

```
$ aircrack -n 128 -f 2 aftendump-128.cap
                                aircrack 2.1
* Got  540196! unique IVs | fudge factor = 2
* Elapsed time [00:00:22] | tried 12 keys at 32 k/m
KB    depth   votes
 0    0/  1   CE(  45) A1(  20) 7E(  15) 98(  15) 72(  12) 82(  12)
 1    0/  2   62(  43) 1D(  24) 29(  15) 67(  13) 94(  13) F7(  13)
 2    0/  1   B6( 499) E7(  18) 8F(  15) 14(  13) 1D(  12) E5(  10)
 3    0/  1   4E( 157) EE(  40) 29(  39) 15(  30) 7D(  28) 61(  20)
 4    0/  1   93( 136) B1(  28) 0C(  15) 28(  15) 76(  15) D6(  15)
 5    0/  2   E1(  75) CC(  45) 39(  31) 3B(  30) 4F(  16) 49(  13)
 6    0/  2   3B(  65) 51(  42) 2D(  24) 14(  21) 5E(  15) FC(  15)
 7    0/  2   6A( 144) 0C(  96) CF(  34) 14(  33) 16(  33) 18(  27)
 8    0/  1   3A( 152) 73(  41) 97(  35) 57(  28) 5A(  27) 9D(  27)
 9    0/  1   F1(  93) 2D(  45) 51(  29) 57(  27) 59(  27) 16(  26)
10    2/  3   5B(  40) 53(  30) 59(  24) 2D(  15) 67(  15) 71(  12)
11    0/  2   F5(  53) C6(  51) F0(  21) FB(  21) 17(  15) 77(  15)
12    0/  2   E6(  88) F7(  81) D3(  36) E2(  32) E1(  29) D8(  27)
      KEY FOUND! [ CE62B64E93E13B6A3AF15BF5E6 ]
```

Hvor lang tid tager det?

Opsamling a data - ca. en halv time på 802.11b ved optimale forhold

Tiden for kørsel af aircrack fra auditor CD på en Dell CPi 366MHz Pentium II laptop:

```
$ time aircrack -n 128 -f 2 aftendump-128.cap
...
real    5m44.180s   user  0m5.902s     sys  1m42.745s
```

Tiden for kørsel af aircrack på en VIA CL-10000 1GHz CPU med almindelig disk OpenBSD:

```
25.12s real     0.63s user     2.14s system
```

Many years ago, this is instant today – realtime cracking

Erstatning for WEP - WPA

Det anbefales at bruge:

Kendte VPN teknologier eller WPA

baseret på troværdige algoritmer

implementeret i professionelt udstyr

fra troværdige leverandører

udstyr der vedligeholdes og opdateres

Man kan måske endda bruge de eksisterende løsninger - fra hjemmepc adgang, mobil adgang m.v.

RADIUS

RADIUS er en protokol til autentificering af brugere op mod en fælles server

Remote Authentication Dial In User Service (RADIUS)

RADIUS er beskrevet i RFC-2865

RADIUS kan være en fordel i større netværk med

- dial-in
- administration af netværksudstyr
- trådløse netværk
- andre RADIUS kompatible applikationer

Erstatninger for WEP

Der findes idag andre metoder til sikring af trådløse netværk

802.1x Port Based Network Access Control

WPA - Wi-Fi Protected Access)
WPA = 802.1X + EAP + TKIP + MIC

nu WPA2
WPA2 = 802.1X + EAP + CCMP

> WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard and is eligible for FIPS 140-2 compliance.

Source: http://www.wifialliance.org/OpenSection/protected_access.asp

WPA eller WPA2?

WPA2 is based upon the Institute for Electrical and Electronics Engineers (IEEE) 802.11i amendment to the 802.11 standard, which was ratified on July 29, 2004.

Q: How are WPA and WPA2 similar?
A: Both WPA and WPA2 offer a high level of assurance for end-users and network administrators that their data will remain private and access to their network restricted to authorized users. Both utilize 802.1X and Extensible Authentication Protocol (EAP) for authentication. Both have Personal and Enterprise modes of operation that meet the distinct needs of the two different consumer and enterprise market segments.

Q: How are WPA and WPA2 different?
A: WPA2 provides a **stronger encryption mechanism** through **Advanced Encryption Standard (AES)**, which is a requirement for some corporate and government users.

Source: http://www.wifialliance.org WPA2 Q and A

WPA Personal eller Enterprise

Personal - en delt hemmelighed, preshared key

Enterprise - brugere valideres op mod fælles server

Hvorfor er det bedre?

- Flere valgmuligheder - passer til store og små
- WPA skifter den faktiske krypteringsnøgle jævnligt - TKIP
- Initialisationsvektoren (IV) fordobles 24 til 48 bit
- Imødekommer alle kendte problemer med WEP!
- Integrerer godt med andre teknologier - RADIUS

- EAP - Extensible Authentication Protocol - individuel autentifikation
- TKIP - WPA Temporal Key Integrity Protocol - nøgleskift og integritet
- MIC - Message Integrity Code - Michael, ny algoritme til integritet
- CCMP - WPA2 AES / Counter Mode CBC-MAC Protocol

WPA cracking

Nu skifter vi så til WPA og alt er vel så godt?

Desværre ikke!

Du skal vælge en laaaaang passphrase

Hvis koden til wifi er for kort kan man sniffe WPA handshake når en computer går ind på netværket, og knække den!

Med et handshake kan man med aircrack igen lave off-line bruteforce angreb!

WPA cracking demo

Vi konfigurerer AP med Henrik42 som WPA-PSK/passhrase

Vi finder netværk med airodump

Vi starter airodump mod specifik kanal

Vi spoofer deauth og opsamler WPA handshake

Vi knækker WPA :-)

Use the tutorials http://www.aircrack-ng.org/doku.php?id=tutorial

Specielt http://www.aircrack-ng.org/doku.php?id=cracking_wpa

Brug manualsiderne for programmerne i aircrack-ng pakken!

WPA cracking med aircrack - start

```
# aircrack-ng -w dict wlan-test.cap
Opening wlan-test.cap
Read 1082 packets.

#  BSSID              ESSID           Encryption

1  00:11:24:0C:DF:97  wlan            WPA (1 handshake)
2  00:13:5F:26:68:D0  Noea            No data - WEP or WPA
3  00:13:5F:26:64:80  Noea            No data - WEP or WPA
4  00:00:00:00:00:00                  Unknown

Index number of target network ?  1
```

Aircrack-ng er en god måde at checke om der er et handshake i filen

WPA cracking med aircrack - start

```
          [00:00:00] 0 keys tested (0.00 k/s)

                     KEY FOUND! [ Henrik42 ]

Master Key     : 8E 61 AB A2 C5 25 4D 3F 4B 33 E6 AD 2D 55 6F 76
                 6E 88 AC DA EF A3 DE 30 AF D8 99 DB F5 8F 4D BD
Transcient Key : C5 BB 27 DE EA 34 8F E4 81 E7 AA 52 C7 B4 F4 56
                 F2 FC 30 B4 66 99 26 35 08 52 98 26 AE 49 5E D7
                 9F 28 98 AF 02 CA 29 8A 53 11 EB 24 0C B0 1A 0D
                 64 75 72 BF 8D AA 17 8B 9D 94 A9 31 DC FB 0C ED

EAPOL HMAC     : 27 4E 6D 90 55 8F 0C EB E1 AE C8 93 E6 AC A5 1F
```

Min gamle Thinkpad X31 med 1.6GHz Pentium M knækker ca. 150 Keys/sekund

Today a modern GPU (Graphical card) can speed this up to 50.000s per second or more with hashcat

WPA/WPA2 cracking Pyrit 2008

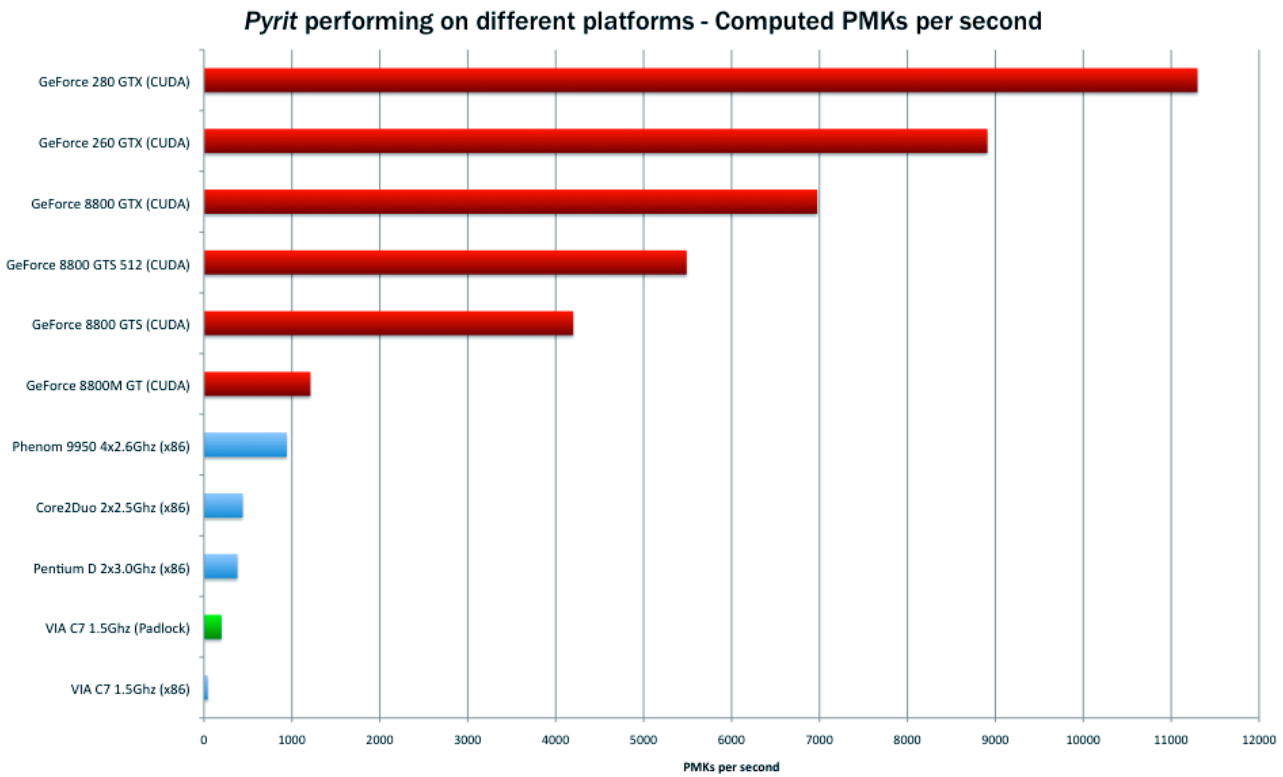
Pyrit takes a step ahead in attacking WPA-PSK and WPA2-PSK, the protocol that today de-facto protects public WIFI-airspace. The project's goal is to estimate the real-world security provided by these protocols. Pyrit does not provide binary files or wordlists and does not encourage anyone to participate or engage in any harmful activity. **This is a research project, not a cracking tool.**

Pyrit's implementation allows to create massive databases, pre-computing part of the WPA/WPA2-PSK authentication phase in a space-time-tradeoff. The performance gain for real-world-attacks is in the range of three orders of magnitude which urges for re-consideration of the protocol's security. Exploiting the computational power of GPUs, *Pyrit* is currently by far the most powerful attack against one of the world's most used security-protocols.

Kryptering afhænger af SSID - så skift altid SSID!

http://pyrit.wordpress.com/about/

Tired of WoW?



Source: http://code.google.com/p/pyrit/ Note old data!

Hashcat Cracking passwords and secrets

- Hashcat is the world's fastest CPU-based password recovery tool.
- oclHashcat-plus is a GPGPU-based multi-hash cracker using a brute-force attack (implemented as mask attack), combinator attack, dictionary attack, hybrid attack, mask attack, and rule-based attack.
- oclHashcat-lite is a GPGPU cracker that is optimized for cracking performance. Therefore, it is limited to only doing single-hash cracking using Markov attack, Brute-Force attack and Mask attack.
- John the Ripper password cracker old skool men stadig nyttig

Source:
http://hashcat.net/wiki/
http://www.openwall.com/john/
http://hashcat.net/wiki/doku.php?id=cracking_wpawpa2

New attack on WPA/WPA2 using PMKID

This attack was discovered accidentally while looking for new ways to attack the new WPA3 security standard. WPA3 will be much harder to attack because of its modern key establishment protocol called "Simultaneous Authentication of Equals"(SAE).

The main difference from existing attacks is that in this attack, capture of a full EAPOL 4-way handshake is not required. The new attack is performed on the RSN IE (Robust Security Network Information Element) of a single EAPOL frame.

At this time, we do not know for which vendors or for how many routers this technique will work, but we think it will work against all 802.11i/p/q/r networks with roaming functions enabled (most modern routers).

The main advantages of this attack are as follow: No more regular users required - because the attacker directly communicates with the AP (aka "client-less"attack) No more waiting for a complete 4-way handshake between the regular user and the AP No more eventual retransmissions of EAPOL frames (which can lead to uncrackable results) No more eventual invalid passwords sent by the regular user No more lost EAPOL frames when the regular user or the AP is too far away from the attacker No more fixing of nonce and replaycounter values required (resulting in slightly higher speeds) No more special output format (pcap, hccapx, etc.) - final data will appear as regular hex encoded string

- https://hashcat.net/forum/thread-7717.html New attack on WPA/WPA2 using PMKID
- https://www.evilsocket.net/2019/02/13/Pwning-WiFi-networks-with-bettercap-and-the-PMKID-client-less-attack/

Wi-Fi Protected Setup, WPS hacking - Reaver

Reaver Open Source Reaver implements a brute force attack against Wifi Protected Setup (WPS) registrar PINs in order to recover WPA/WPA2 passphrases, as described in http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf.

Reaver has been designed to be a robust and practical attack against WPS, and has been tested against a wide variety of access points and WPS implementations.

On average Reaver will recover the target AP's plain text WPA/WPA2 passphrase in 4-10 hours, depending on the AP. In practice, it will generally take half this time to guess the correct WPS pin and recover the passphrase.

Hvad betyder ease of use?

Source:
https://code.google.com/p/reaver-wps/

http://lifehacker.com/5873407/how-to-crack-a-wi+fi-networks-wpa-password-with-reaver

WPS Design Flaws used by Reaver

Design Flaw #1

Option / Authentication	Physical Access	Web Interface	PIN
Push-button-connect	X		
PIN – Internal Registrar		X	
PIN – External Registrar			X

WPS Options and which kind of authentication they actually use.

As the External Registrar option does not require any kind of authentication apart from providing the PIN, it is potentially vulnerable to brute force attacks.

Pin only, no other means necessary

Source:
http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

WPS Design Flaws used by Reaver

IEEE 802.11/EAP Expanded Type, Vendor ID: WFA (0x372A), Vendor Type: SimpleConfig (0x01)			
M1	Enrollee → Registrar	N1 || Description || PK_E	Diffie-Hellman Key Exchange
M2	Enrollee ← Registrar	N1 || N2 || Description || PK_R || Authenticator	
M3	Enrollee → Registrar	N2 || E-Hash1 || E-Hash2 || Authenticator	
M4	Enrollee ← Registrar	N1 || R-Hash1 || R-Hash2 || $E_{KeyWrapKey}$(R-S1) || Authenticator	proove posession of 1st half of PIN
M5	Enrollee → Registrar	N2 || $E_{KeyWrapKey}$(E-S1) || Authenticator	proove posession of 1st half of PIN
M6	Enrollee ← Registrar	N1 || $E_{KeyWrapKey}$(R-S2) || Authenticator	proove posession of 2nd half of PIN
M7	Enrollee → Registrar	N2 || $E_{KeyWrapKey}$(E-S2 ||ConfigData) || Authenticator	proove posession of 2nd half of PIN, send AP configuration
M8	Enrollee ← Registrar	N1 || $E_{KeyWrapKey}$(ConfigData) || Authenticator	set AP configuration

Enrollee = AP Registrar = Supplicant = Client/Attacker	PSK1 = first 128 bits of $HMAC_{AuthKey}$(1st half of PIN) PSK2 = first 128 bits of $HMAC_{AuthKey}$(2nd half of PIN)
PK_E = Diffie-Hellman Public Key Enrollee PK_R = Diffie-Hellman Public Key Registrar Authkey and KeyWrapKey are derived from the Diffie-Hellman shared key.	E-S1 = 128 random bits E-S2 = 128 random bits E-Hash1 = $HMAC_{AuthKey}$(E-S1 || PSK1 || PK_E || PK_R) E-Hash2 = $HMAC_{AuthKey}$(E-S2 || PSK2 || PK_E || PK_R)
Authenticator = $HMAC_{Authkey}$(last message || current message) $E_{KeyWrapKey}$ = Stuff encrypted with KeyWrapKey (AES-CBC)	R-S1 = 128 random bits R-S2 = 128 random bits R-Hash1 = $HMAC_{AuthKey}$(R-S1 || PSK1 || PK_E || PK_R) R-Hash2 = $HMAC_{AuthKey}$(R-S2 || PSK2 || PK_E || PK_R)

1	2	3	4	5	6	7	0
1st half of PIN				2nd half of PIN			checksum

Reminds me of NTLM cracking, crack parts independently

Source:
http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

WPS Design Flaws used by Reaver

Design flaw #2

An attacker can derive information about the correctness of parts the PIN from the AP´s responses.

- If the attacker receives an EAP-NACK message after sending M4, he knows that the 1st half of the PIN was incorrect.
- If the attacker receives an EAP-NACK message after sending M6, he knows that the 2nd half of the PIN was incorrect.

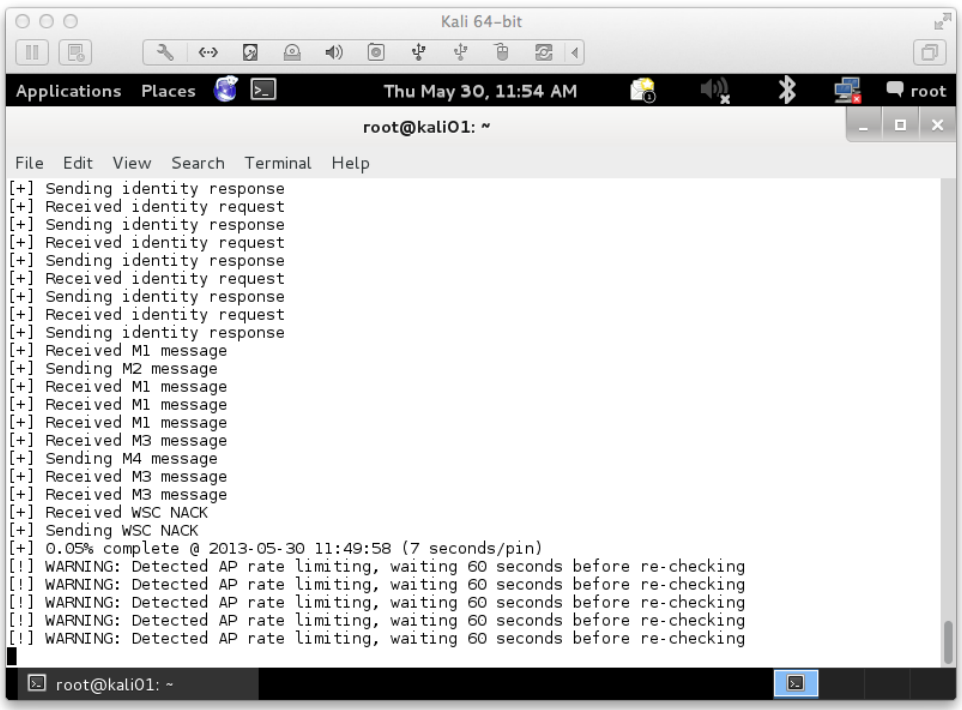
This form of authentication dramatically decreases the maximum possible authentication attempts needed from 10^8 (=100.000.000) to $10^4 + 10^4$ (=20.000).

As the 8th digit of the PIN is always a checksum of digit one to digit seven, there are at most $10^4 + 10^3$ (=11.000) attempts needed to find the correct PIN.

100.000.000 is a lot, 11.000 is not

Source:
http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

Reaver Rate limiting



Make no mistake, it will work!

WPA3 Security

WPA3

In January 2018, the Wi-Fi Alliance announced WPA3 as a replacement to WPA2.[12][13] Certification began in June 2018,[14] and WPA3 support has been mandatory for devices which bear the "Wi-Fi CERTIFIED™"logo since July 2020.[11]

The new standard uses an equivalent 192-bit cryptographic strength in WPA3-Enterprise mode[15] (AES-256 in GCM mode with SHA-384 as HMAC), and still mandates the use of CCMP-128 (AES-128 in CCM mode) as the minimum encryption algorithm in WPA3-Personal mode.

The WPA3 standard also replaces the pre-shared key (PSK) exchange with Simultaneous Authentication of Equals (SAE) exchange, a method originally introduced with IEEE 802.11s, resulting in a more secure initial key exchange in personal mode[16][17] and forward secrecy.[18] The Wi-Fi Alliance also says that WPA3 will mitigate security issues posed by weak passwords and simplify the process of setting up devices with no display interface.[2][19]

Protection of management frames as specified in the IEEE 802.11w amendment is also enforced by the WPA3 specifications.

Source: https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

- Does not seem to be used much, in Denmark, yet – but coming

IS WPA3 supported?

> A wireless network adapter that supports Wi-Fi 6. To see if your PC supports it, check the documentation that came with it or check the PC manufacturer's website. Tip: You can also check to see if your router supports Wi-Fi 6 by opening the Command Prompt, and then typing the command netsh wlan show drivers. Look next to Radio types supported and see if it includes 802.11ax.

Source: https://support.microsoft.com/en-us/windows/faster-and-more-secure-wi-fi-in-windows-26177a28-38ed-1a8e-7e

- Your devices must support both WPA3 in both operating system and Wi-Fi drivers!
- Windows 10 and 11 does, so try upgrading drivers
- Android does since Android 10 – pretty new still
- Apple devices have support in recent versions

WPA3 on Apple Devices

- iPhone 7 or later.
- iPad 5th generation or later.
- Apple TV 4K or later.
- Apple Watch series 3 or later.
- Mac computers (late 2013 or later, with 802.11ac or later)

Source: https://support.apple.com/da-dk/guide/security/sec8a67fa93d/web

Wi-Fi CERTIFIED WPA3™

WPA3™ provides cutting-edge security protocols to the market. Building on the widespread success and adoption of Wi-Fi security, WPA3 adds new features to simplify Wi-Fi security, enable more robust authentication, deliver increased cryptographic strength for highly sensitive data markets, and maintain resiliency of mission critical networks. All WPA3 networks:

- Use the latest security methods
- Disallow outdated legacy protocols
- Require use of Protected Management Frames (PMF)

Since Wi-Fi networks differ in usage purpose and security needs, WPA3 includes additional capabilities specifically for personal and enterprise networks. Users of WPA3-Personal receive increased protections from password guessing attempts, while WPA3-Enterprise users can now take advantage of higher-grade security protocols for sensitive data networks.

WPA3 is a mandatory certification for Wi-Fi CERTIFIED™ devices.

Source: https://www.wi-fi.org/discover-wi-fi/security

WPA3 Personal Simultaneous Authentication of Equals (SAE)

WPA3-Personal is based on Simultaneous Authentication of Equals (SAE), defined in Institute of Electrical and Electronics Engineers (IEEE) Std 802.11-2016 and updated in 802.11-2020. The Wi-Fi Alliance WPA3 Specification defines additional requirements for devices operating in SAE modes. **SAE is a key exchange protocol that authenticates two peers using only a password**, resulting in a shared secret between the two peers that can be used for secret communication while exchanging data over a public network. It provides a secure alternative to using certificates when a centralized authority is not available.

In a Wi-Fi infrastructure network, the SAE handshake negotiates a fresh Pairwise Master Key (PMK) per client, which is then used in a traditional Wi-Fi four-way handshake to generate session keys. Neither the PMK nor the password credential used in the SAE exchange can be obtained by a passive attack, active attack, or offline dictionary attack. Password recovery is only possible through repeated active attacks guessing a different password each time. Additionally, forward secrecy is provided because the SAE handshake assures the PMK cannot be recovered if the password becomes known.

Source: Wi-Fi CERTIFIED WPA3™ Technology Overview January 2021
https://www.wi-fi.org/system/files/Wi-Fi_CERTIFIED_WPA3_Technology_Overview_202101.pdf

WPA3-Personal

WPA3-Personal brings better protections to individual users by providing more robust password-based authentication, even when users choose passwords that fall short of typical complexity recommendations. This capability is enabled through Simultaneous Authentication of Equals (SAE). The technology is **resistant to offline dictionary attacks** where an adversary attempts to determine a network password by trying possible passwords without further network interaction.

- **Natural password selection**: Allows users to choose passwords that are easier to remember
- **Ease of use**: Delivers enhanced protections with no change to the way users connect to a network
- **Forward secrecy**: Protects data traffic even if a password is compromised after the data was transmitted

Source: https://www.wi-fi.org/discover-wi-fi/security

Note: Compare this with Diffie-Hellman https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange and Transport Layer Security (TLS) https://en.wikipedia.org/wiki/Transport_Layer_Security

WPA3-Enterprise

WPA3-Enterprise builds upon the foundation of WPA2-Enterprise with the additional requirement of using Protected Management Frames on all WPA3 connections.

- **Authentication**: multiple Extensible Authentication Protocol (EAP) methods
- **Authenticated encryption**: minimum 128-bit Advanced Encryption Standard Counter Mode with Cipher Block Chaining Message Authentication (AES-CCMP 128)
- **Key derivation and confirmation**: minimum 256-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA256)
- **Robust management frame protection**: minimum 128-bit Broadcast/Multicast Integrity Protocol Cipher-based Message Authentication Code (BIP-CMAC-128)

Source: https://www.wi-fi.org/discover-wi-fi/security

WPA3-Enterprise with 192-bit mode

WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to better protect sensitive data.

- **Authentication**: Extensible Authentication Protocol – Transport Layer Security (EAP-TLS) using Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve
- **Authenticated encryption**: 256-bit Galois/Counter Mode Protocol (GCMP-256)
- **Key derivation and confirmation**: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)
- **Robust management frame protection**: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

  The 192-bit security mode offered by WPA3-Enterprise ensures the right combination of cryptographic tools are used and sets a consistent baseline of security within a WPA3 network.

Source: https://www.wi-fi.org/discover-wi-fi/security

WPA3 MiTM and evil twin attacks

WPA3™ includes features that provide Wi-Fi® devices with additional safeguards against a variety of attacks, including man in the middle (MITM) and evil twin attacks.

In this post, we will explore the details of two additional new features: SAE Public Key (SAE-PK) and Transition Disable. SAE-PK provides protection against evil twin attacks on client devices in public networks that use WPA3-Personal, while Transition Disable provides protection against active downgrade attacks on client devices operating in a transition mode with WPA3-Personal, WPA3-Enterprise or Wi-Fi Enhanced Open™.

Source: https://www.wi-fi.org/beacon/thomas-derham-nehru-bhandaru/wi-fi-certified-wpa3-december-2020-update-brings-new-0

2020: Dragonblood

> April 2019 — Modern Wi-Fi networks use WPA2 to protect transmitted data. However, because **WPA2 is more than 14 years old**, the Wi-Fi Alliance recently announced the new and more secure WPA3 protocol. One of the supposed advantages of WPA3 is that, thanks to its underlying **Dragonfly handshake**, it's **near impossible to crack the password** of a network. Unfortunately, we found that even with WPA3, an **attacker within range of a victim can still recover the password**. If the victim uses no extra protection such as HTTPS, this allows an attacker to steal sensitive information such as passwords and emails. We hope our disclosure motivates vendors to mitigate our attacks before WPA3 becomes widespread.
>
> ...
>
> Fortunately, as a result of our research, both the Wi-Fi standard and EAP-pwd are being updated with a more secure protocol. Although this update is not backwards-compatible with current deployments of WPA3, it does prevent most of our attacks.

Source: https://wpa3.mathyvanhoef.com/

- Side-channel leaks
- Full paper Mathy Vanhoef and Eyal Ronen. 2020. *Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd*. In IEEE Symposium on Security & Privacy (SP). IEEE. https://eprint.iacr.org/2019/383

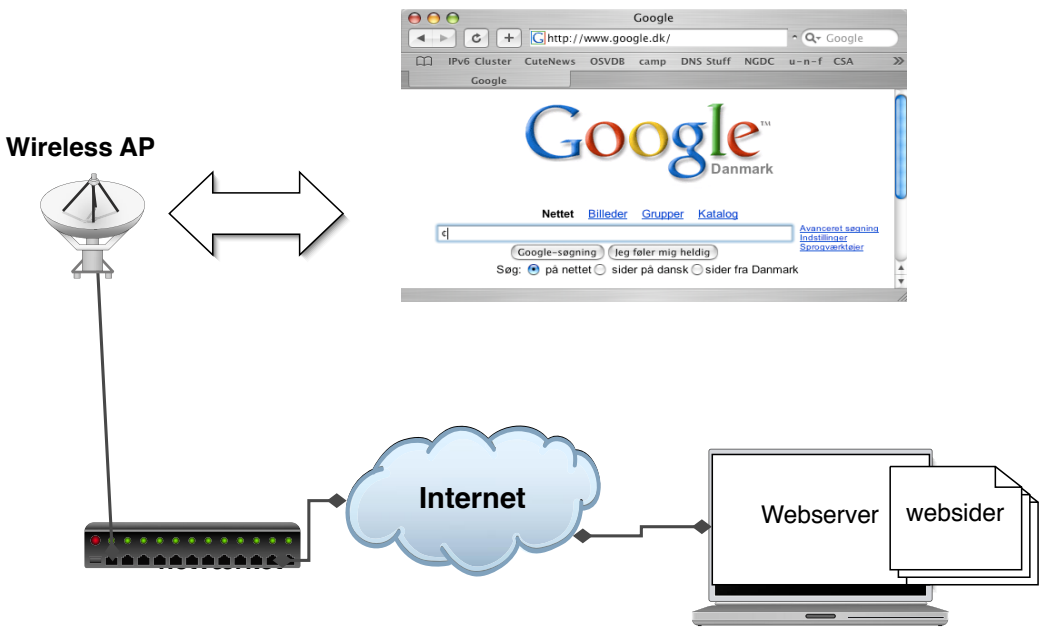
2021: Fragment and Forge

Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation

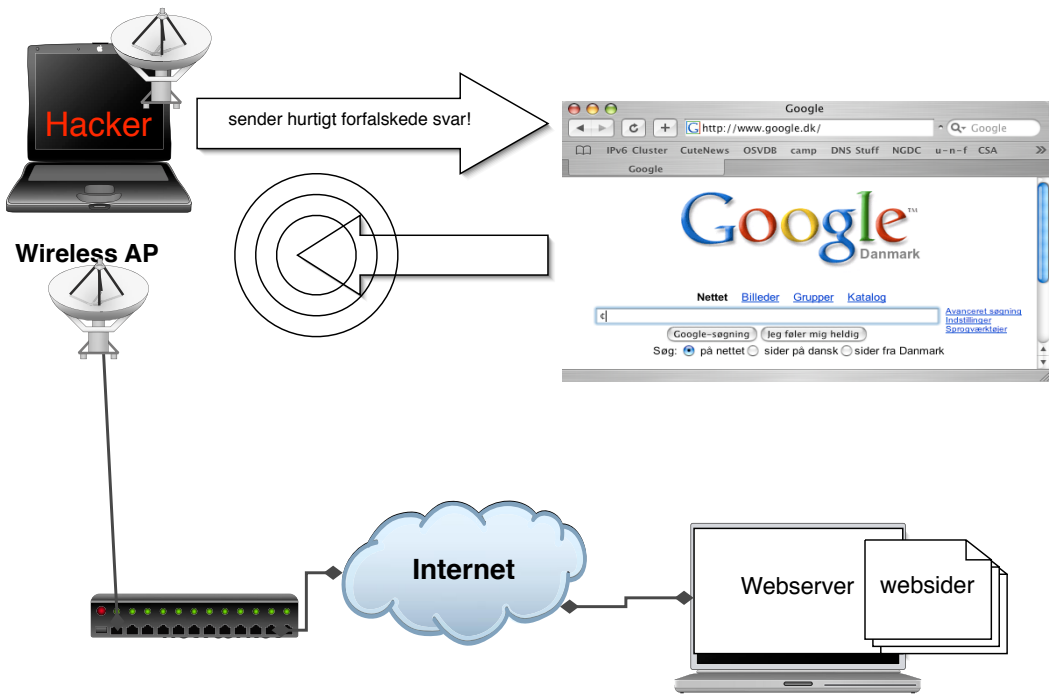
Abstract In this paper, we present three design flaws in the **802.11 standard that underpins Wi-Fi**. One design flaw is in the frame aggregation functionality, and another two are in the frame fragmentation functionality. These design flaws enable an adversary to **forge encrypted frames** in various ways, which in turn enables **exfiltration of sensitive data**. We also discovered common implementation flaws related to aggregation and fragmentation, which further worsen the impact of our attacks. Our results **affect all protected Wi-Fi networks, ranging from WEP all the way to WPA3**, meaning the discovered flaws have been part of Wi-Fi **since its release in 1997**. In our experiments, all devices were vulnerable to one or more of our attacks, confirming that **all Wi-Fi devices are likely affected**. Finally, we present a tool to test whether devices are affected by any of the vulnerabilities, and we discuss countermeasures to prevent our attacks.

Source: Mathy Vanhoef https://eprint.iacr.org/2021/763.pdf (bold by me)

Normal WLAN brug



Packet injection - airpwn 2004



Classic Malicious actor in the middle – intercept and change data

Airpwn teknikker

Klienten sender forespørgsel

Hackerens program airpwn lytter og sender så falske pakker

Hvordan kan det lade sig gøre?

- Normal forespørgsel og svar på Internet tager måske 20-50ms
- Airpwn kan svare på omkring 1ms angives det
- Airpwn har alle informationer til rådighed

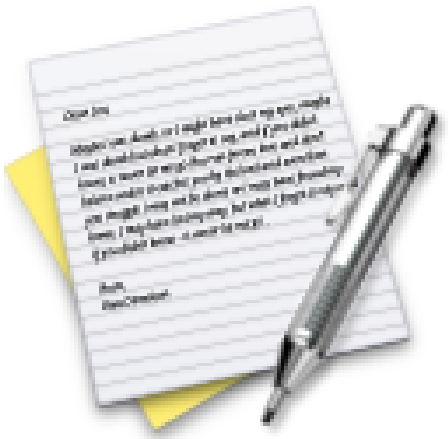
Airpwn source findes på Sourceforge
http://airpwn.sourceforge.net/

NB: Airpwn som demonstreret er begrænset til TCP og ukrypterede forbindelser

Mange Wireless netværk idag er ukrypterede og samme teknikker kan bruges idag

Ja, de **samme metoder** oprindeligt fra **2004** kan bruges idag!

Øvelse: airdecap



Vi afprøver nu airdecap på de opsamlede filer fra før

Brug dele af tutorials fra
http://www.aircrack-ng.org/doku.php?id=airdecap-ng&s[]=airdecap

"... decrypts a WPA/WPA2 encrypted capture using the passphrase"

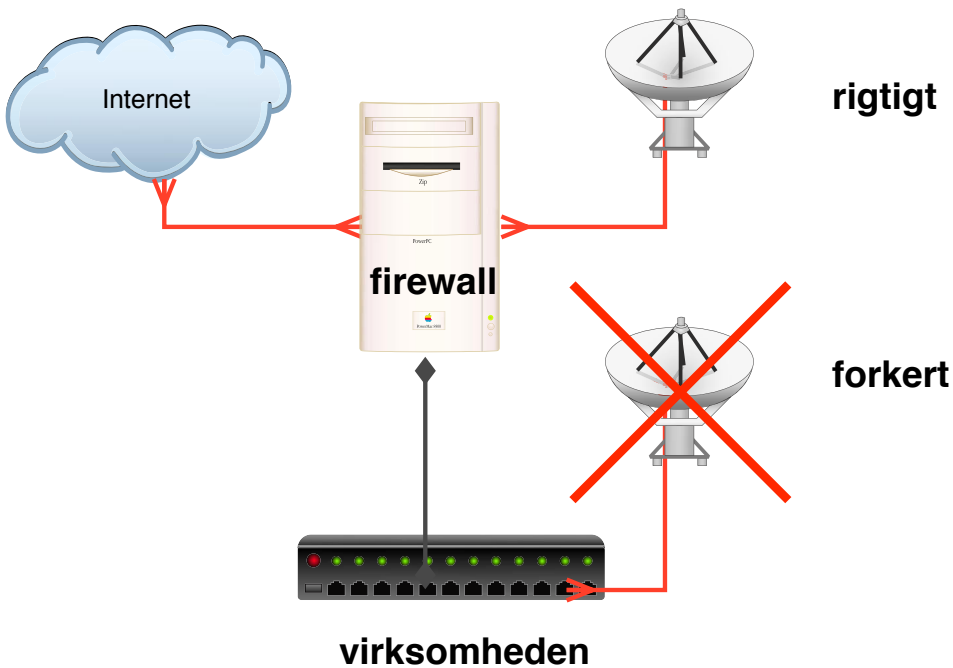
Når adgangen er skabt

Så går man igang med de almindelige værktøjer

SecTools.Org: Top 125 Network Security Tools http://www.sectools.org

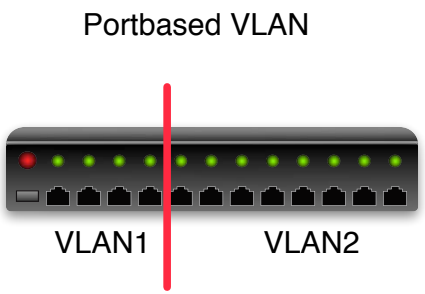
Forsvaret er som altid - flere lag af sikkerhed!

Infrastrukturændringer



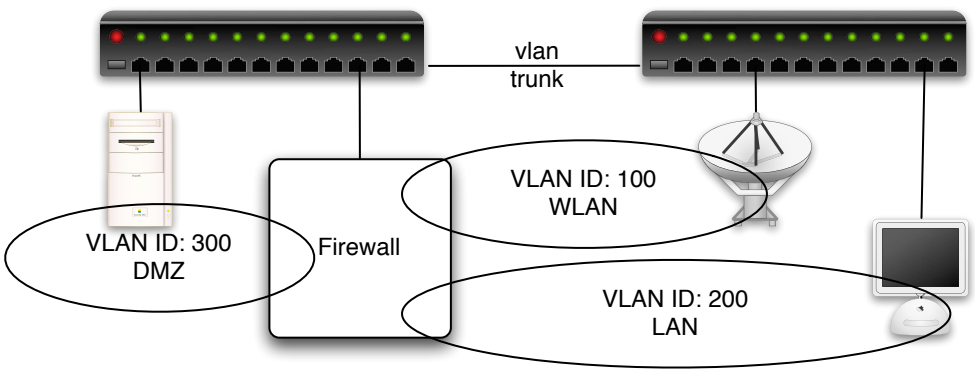
Sådan bør et access point logisk forbindes til netværket

VLAN Virtual LAN



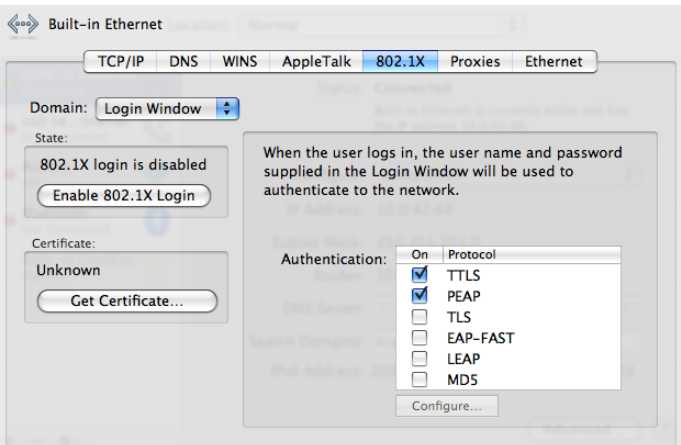
- Nogle switche tillader at man opdeler portene
- Denne opdeling kaldes VLAN og portbaseret er det mest simple
- Port 1-4 er et LAN
- De resterende er et andet LAN
- Data skal omkring en firewall eller en router for at krydse fra VLAN1 til VLAN2

IEEE 802.1q



- Nogle switche tillader at man opdeler portene, men tillige benytter 802.1q
- Med 802.1q tillades VLAN tagging på Ethernet niveau
- Data skal omkring en firewall eller en router for at krydse fra VLAN1 til VLAN2
- VLAN trunking giver mulighed for at dele VLANs ud på flere switches
- Der findes værktøjer der måske kan lette dette arbejde YMMV: OpenNAC FreeNAC, PacketFence

IEEE 802.1x Port Based Network Access Control



- Nogle switche tillader at man benytter 802.1x
- Denne protokol sikrer at man valideres før der gives adgang til porten
- Når systemet skal have adgang til porten afleveres brugernavn og kodeord/certifikat
- Denne protokol indgår også i WPA Enterprise

802.1x og andre teknologier

802.1x i forhold til MAC filtrering giver væsentlige fordele

MAC filtrering kan spoofes, hvor 802.1x kræver det rigtige kodeord

Typisk benyttes RADIUS og 802.1x integrerer således mod både LDAP og Active Directory

Undgå standard indstillinger

når vi scanner efter services går det nemt med at finde dem

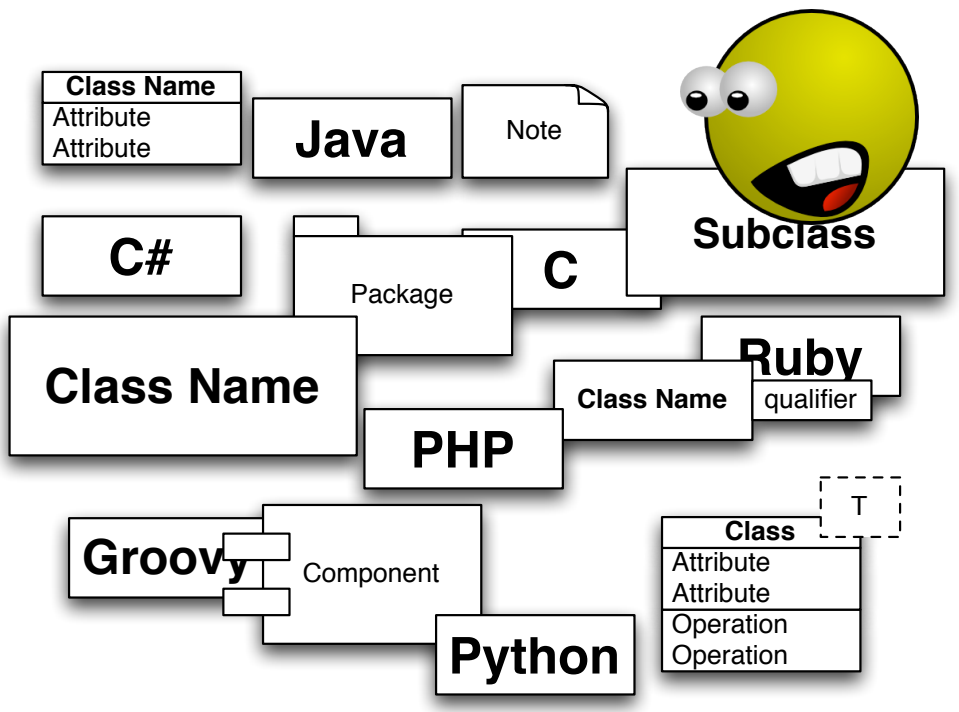
Giv jer selv mere tid til at omkonfigurere og opdatere ved at undgå standardindstillinger

Tiden der går fra en sårbarhed annonceres til den bliver udnyttet er meget kort idag!

Ved at undgå standard indstillinger kan der måske opnås en lidt længere frist - inden ormene kommer

NB: ingen garanti - og det hjælper sjældent mod en dedikeret angriber

Next step, software sikkerhed



Wireless AP implementerer protokoller med hardware+software

Sårbare AP'er - 1

Hvordan bygger man et billigt Access Point?

- En embedded kerne
- En embedded TCP/IP stak
- Noget 802.11 hardware
- Et par Ethernet stik
- eventuelt et modem
- Tape ...

Hvad med efterfølgende opdatering af software?

Sårbare AP'er - 2

Eksempler på access point sårbarheder:

Konfigurationsfilen kan hentes uden autentificering - inkl. WEP nøgler

Konfigurationen sker via SNMP - som sender community string i klar tekst

Wi-Fi Protected Setup,(WPS) kan ikke slås helt fra

...

Konklusionen er klar - hardwaren er i mange tilfælde ikke sikker nok til at anvende på forretnings-kritiske LAN segmenter!

Hvordan finder man buffer overflow, og andre fejl

Black box testing

Closed source reverse engineering

White box testing

Open source betyder man kan læse og analysere koden

Source code review - automatisk eller manuelt

Fejl kan findes ved at prøve sig frem - fuzzing

Exploits virker typisk mod specifikke versioner af software

Forudsætninger

Bemærk: alle angreb har forudsætninger for at virke

Et angreb mod Telnet virker kun hvis du bruger Telnet

Et angreb mod Apache HTTPD virker ikke mod Microsoft IIS

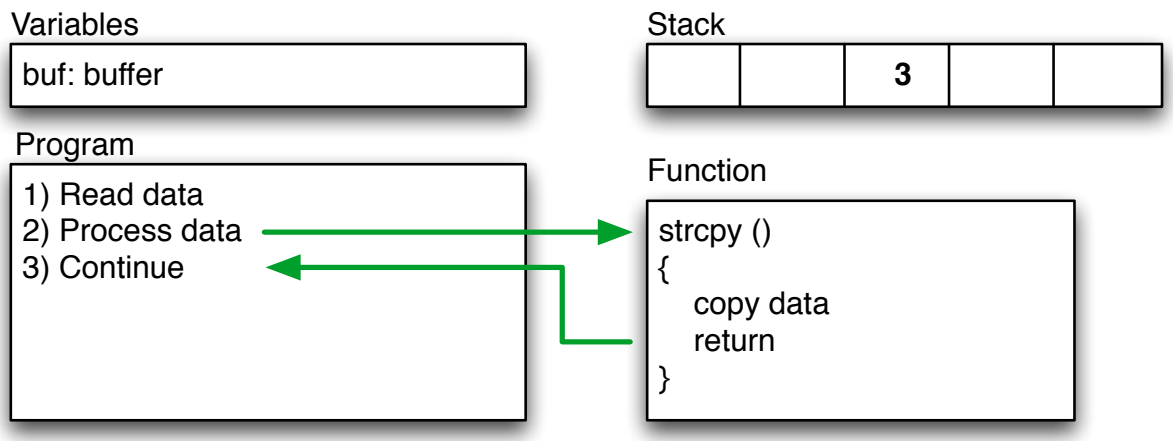
Kan du bryde kæden af forudsætninger har du vundet!

buffer overflows et C problem

Et buffer overflow er det der sker når man skriver flere data end der er afsat plads til i en buffer, et dataområde. Typisk vil programmet gå ned, men i visse tilfælde kan en angriber overskrive returadresser for funktionskald og overtage kontrollen.

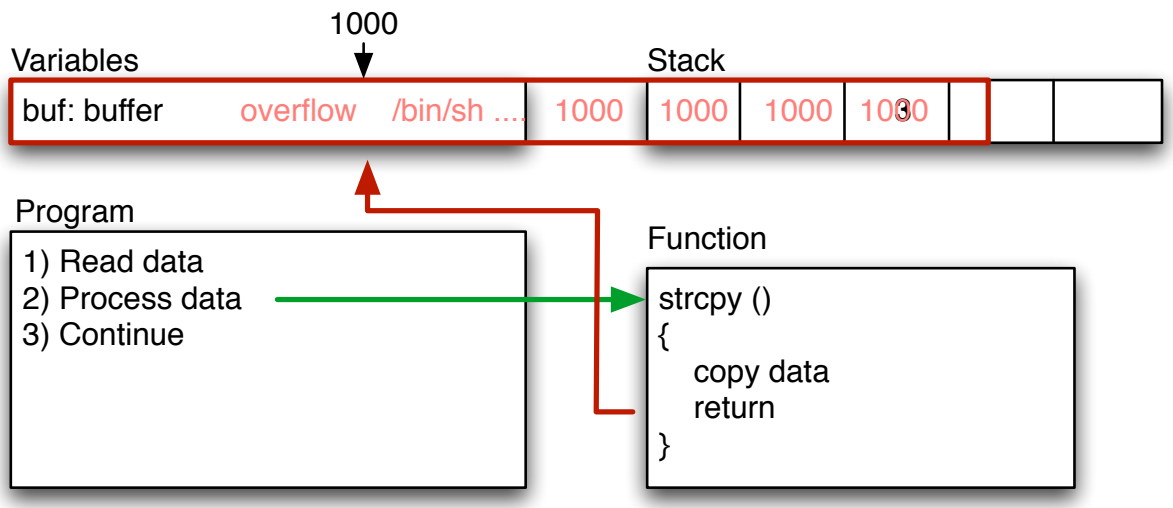
Stack protection er et udtryk for de systemer der ved hjælp af operativsystemer, programbiblioteker og lign. beskytter stakken med returadresser og andre variable mod overskrivning gennem buffer overflows. StackGuard og Propolice er nogle af de mest kendte.

Buffer og stacks




```
main(int argc, char **argv)
{       char buf[200];
         strcpy(buf, argv[1]);
         printf("%s\n",buf);
}
```

Overflow - segmentation fault



Bad function overwrites return value!

Control return address

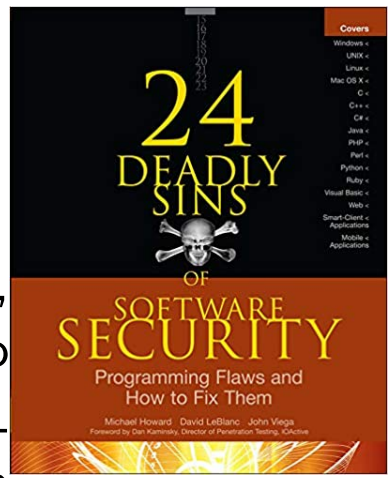
Run shellcode from buffer, or from other place

Wireless buffer overflows beware of the BLOB

AP and driver software has errors, some exploitable

24 Deadly Sins of Software Security

24 Deadly Sins of Software Security af Michael Howard, David Leblanc, John Viega 2009

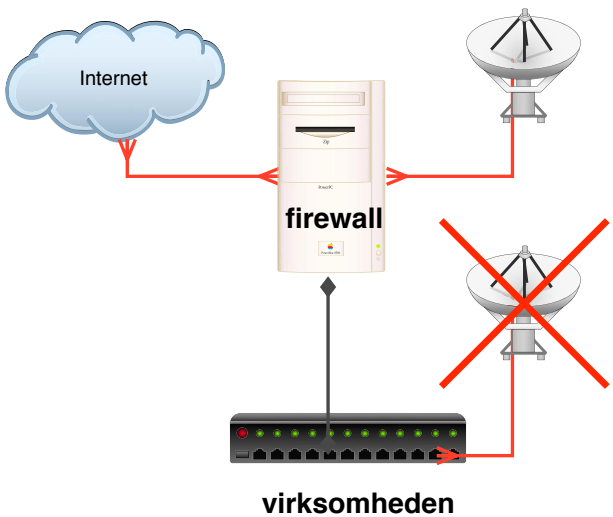


Obligatorisk læsning for alle udviklere

Denne bog er præcis og giver overblik på kun 432 sider

Buffer Overruns, Format String Problems, Integer Overflows, SQL Injection, Command Injection, Failing to Handle Errors, Cross-Site Scripting, Failing to Protect Network Traffic, Magic URLs Hidden Form Fields, Improper Use of SSL and TLS, Weak Password-Based Systems, Failing to Store and Protect Data Securely, Information Leakage, Improper File Access, Trusting Network Name Resolution, Race Conditions, Unauthenticated Key Exchange, Cryptographically Strong Random Numbers, Poor Usability

Recommendations for wireless networks



rigtig

- Use a specific SSID - network name, influences the WPA PSK keying
- Never use WEP
- Use WPA PSK or Enterprise, or at least some VPN with individual user logins
- When using WPA Personal/PSK passphrase must be long, like +40 chars!

forkert

- Place network Access Points on the network where they can be monitored. Separate VLAN, isolated from the cabled LAN
- Have rules for the use of wireless networks, also for persons travelling - "Always use VPN when using insecure wireless in hotels, airports etc."

Questions?

Henrik Kramselund he/him han/ham hlk@zencurity.com @kramse

You are always welcome to send me questions later via email

Mobile: +45 2026 6000

Email: hlk@zencurity.com