Manolis (Emmanouil Vasilomanolakis)

network security: wireless security

Course plan

- Lecture 1: Intro (**Manolis**, **Carsten**) 30.01
- Lecture 2: **Crypto** essentials (**Carsten**) 06.02
- Lecture 3: **Authentication** (**Manolis**), lab bootcamp (TAs) 13.02
- Lecture 4: **TLS** (**Manolis**) 20.02
- Lecture 5: **Threat detection** (**Manolis**) 27.02
- Lecture 6: Hacking Lab day (**TAs**) – blue team 05.03
- Lecture 7: **IoT security** (**Manolis**) 12.03
- Lecture 8: **WIFI security** (**Manolis**) 19.03
- Lecture 9: **Private communication** (**Carsten**) 02.04
- Lecture 10: **When everything fails** (**Manolis**) 09.04
- Lecture 11: Hacking Lab day (**TAs**) – red team 16.04
- Lecture 12: Guest lecture (OT security, **Ludwig**) 23.04
- Lecture 13: **Exam preps** (**Carsten, Manolis**) 30.04

Outline

- **Introduction**
- **Wireless threats**
- **WIFI security**
  - Open Wi-Fi
  - Obscurity
  - WEP/WPA
  - WPA2
  - WPA3
- **Intro to NFC/RFID security**
- **Conclusion**
- **Lab exercises**

Introduction

- In the good old days:
  - Ethernet only
  - Physical access needed

- Now:
  - Wireless networks are everywhere
  - No physical access needed
  - Wi-Fi can be used both for:
    - Attacking
    - But also: exfiltration!

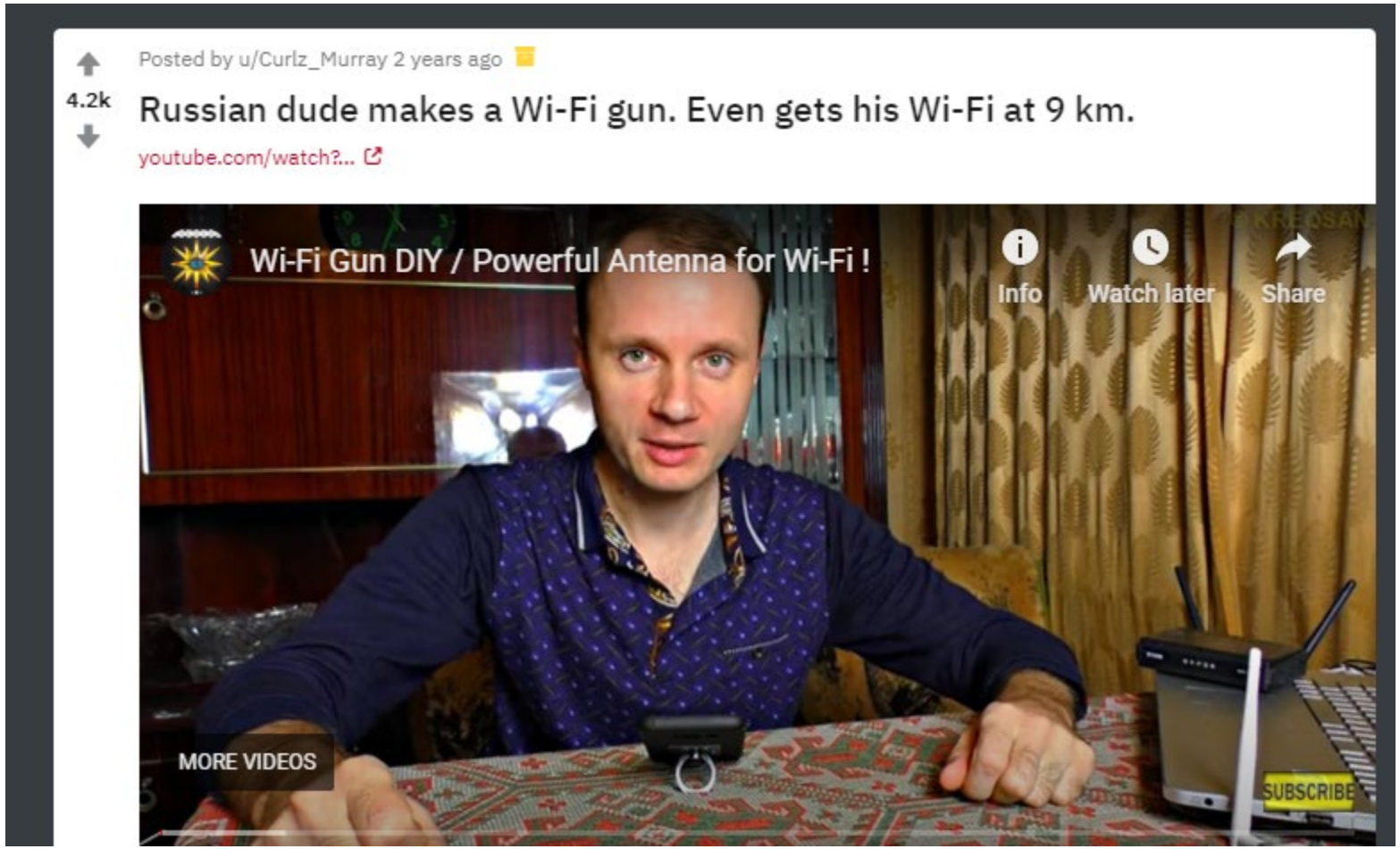
Wireless threats

- Rogue Access Points/Ad-Hoc Networks
  - **Evil twin**
- Denial of Service
- Configuration Problems (Mis-Configurations/Incomplete Configurations)
- **Passive Capturing**

Wireless threats

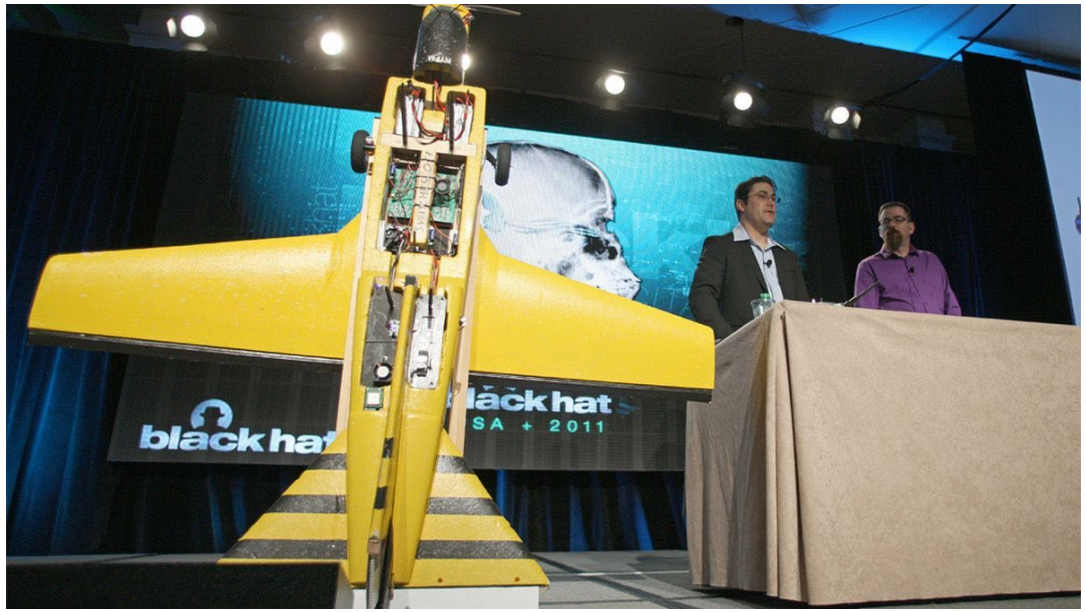
- Jamming
- Sniffing
  - –Usually you have to be close
  - –But…

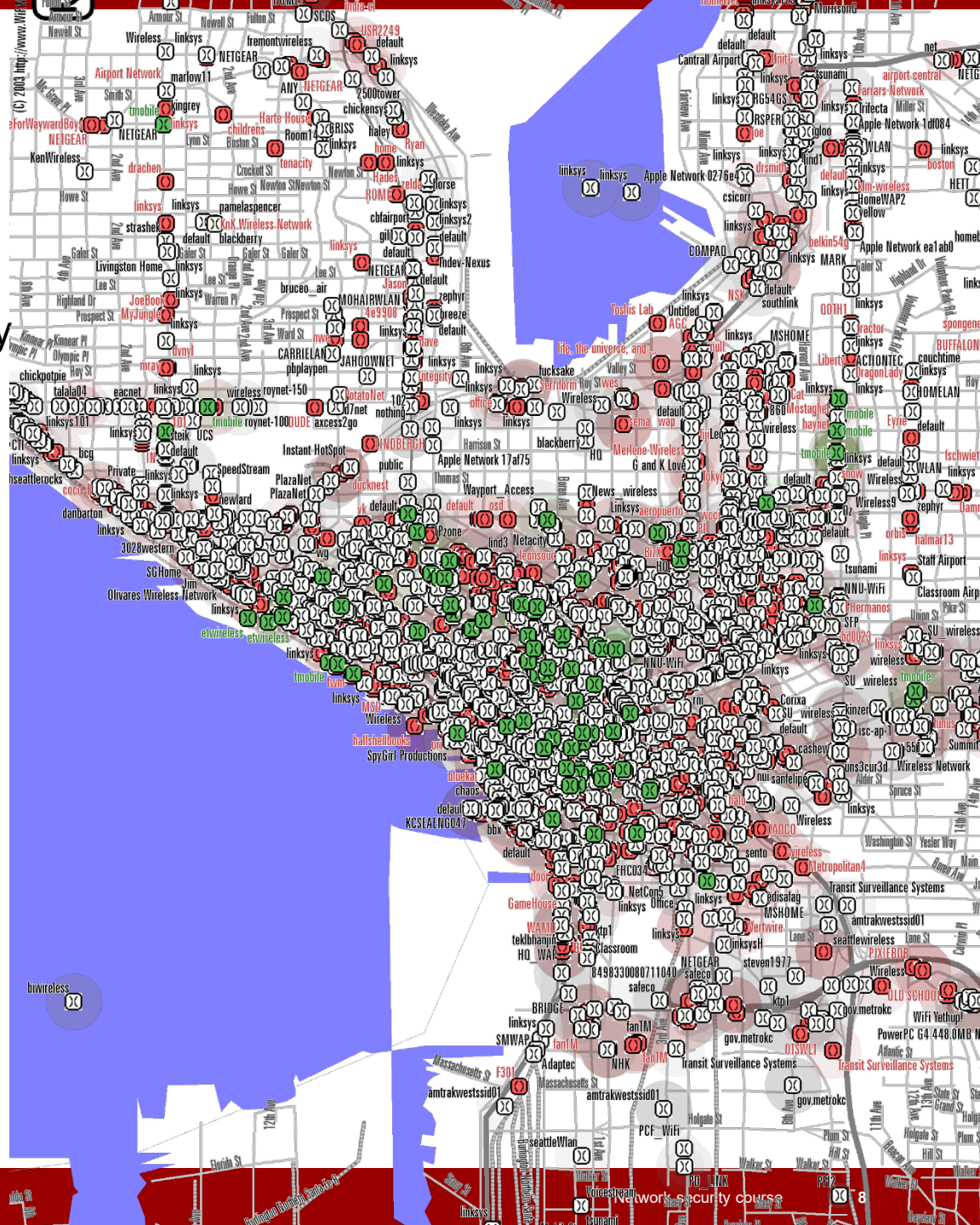
Wi-Fi guns


Posted by u/Curlz_Murray 2 years ago
4.2k
Russian dude makes a Wi-Fi gun. Even gets his Wi-Fi at 9 km.
youtube.com/watch?...
Wi-Fi Gun DIY / Powerful Antenna for Wi-Fi !
Info
Watch later
Share
MORE VIDEOS
SUBSCRIBE

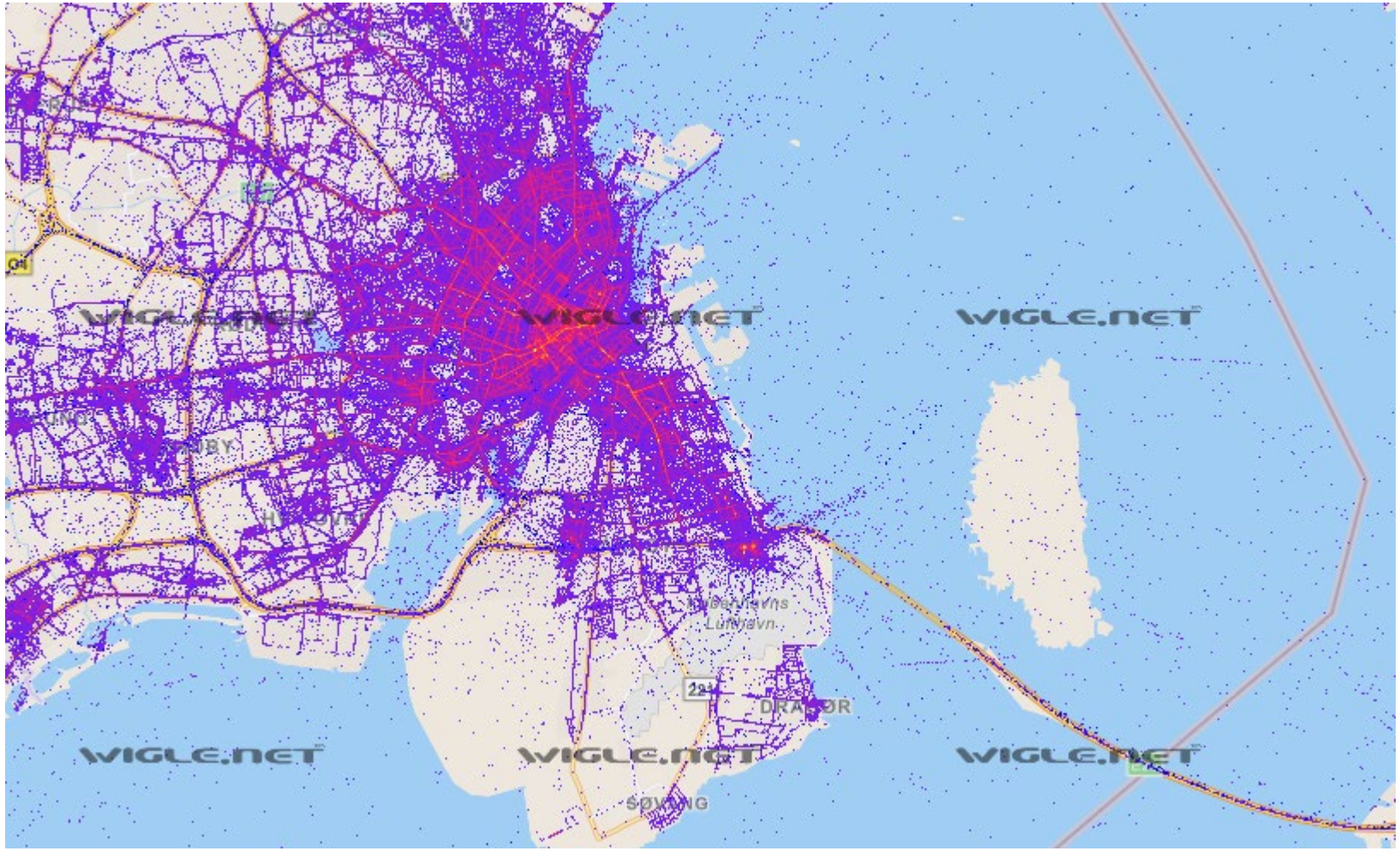
Wardriving

- Act of searching for Wi-Fi wireless networks by a person usually in a moving vehicle
  - Synonyms: Warbiking, warcycling, warwalking

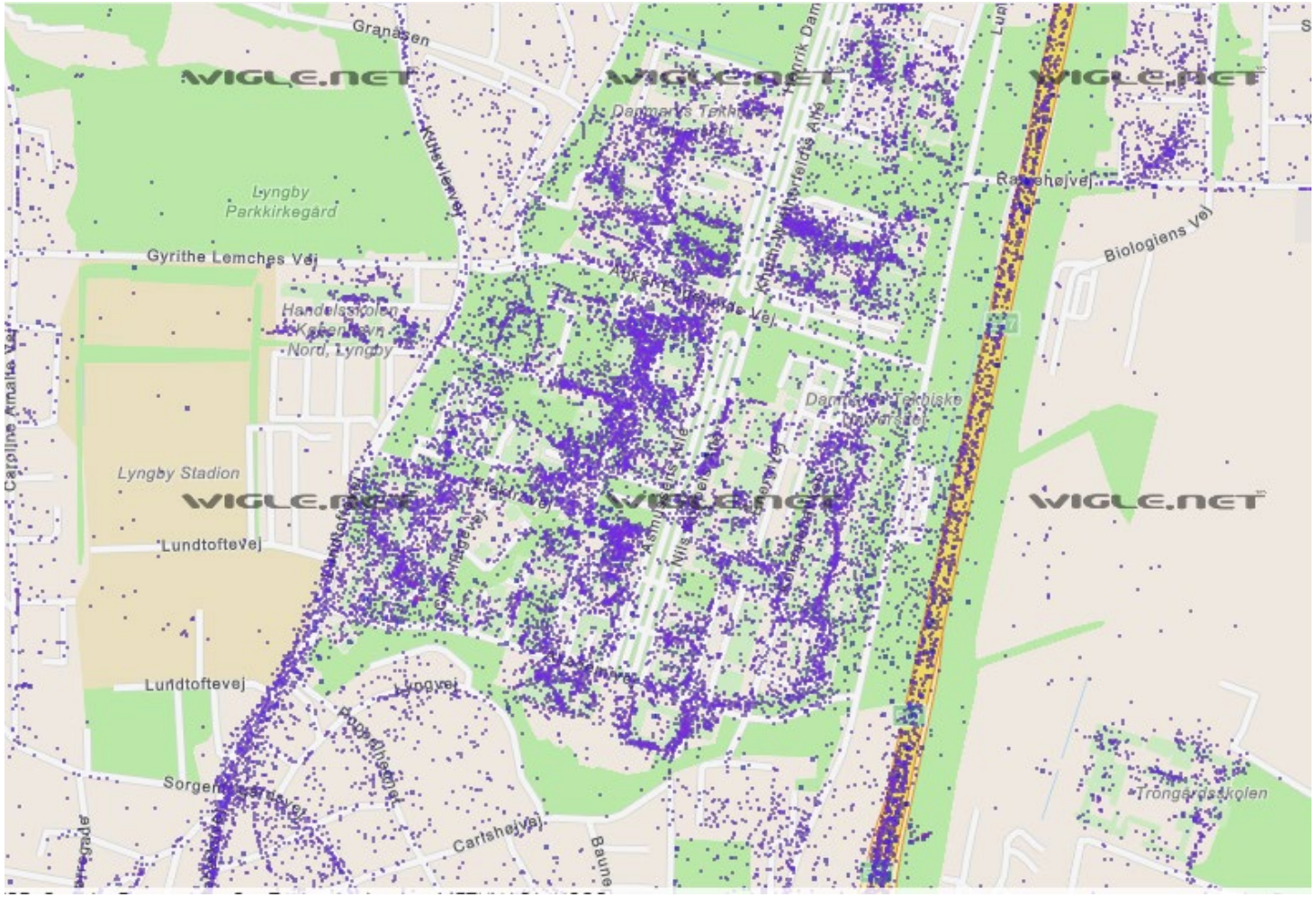




Wigle demo


WIGLE.NET
WIGLE.NET
WIGLE.NET
WIGLE.NET
WIGLE.NET
WIGLE.NET
SØVANG

Wigle demo: DTU campus



Outline

- Introduction
- Wireless threats
- **WIFI security**
  - Open Wi-Fi
  - Obscurity
  - WEP/WPA
  - WPA2
  - WPA3
- **Intro to NFC/RFID security**
- **Conclusion**
- **Lab exercises**

IEEE 802.11 Wireless LAN

- 802.11: 1997, 2mbit/sec, 2.4GHz
- 802.11b: 1999, 11mbit/sec, 2.4GHz
- 802.11a: 1999, 54mbit/sec, 5GHz
- 802.11g: 2003, 54mbit/sec, 5GHz
- 802.11n: 2009, 72-300mbit/sec, 2.4/5GHz
- 802.11ac: 2013, 100-1300mbit/sec, 5GHz

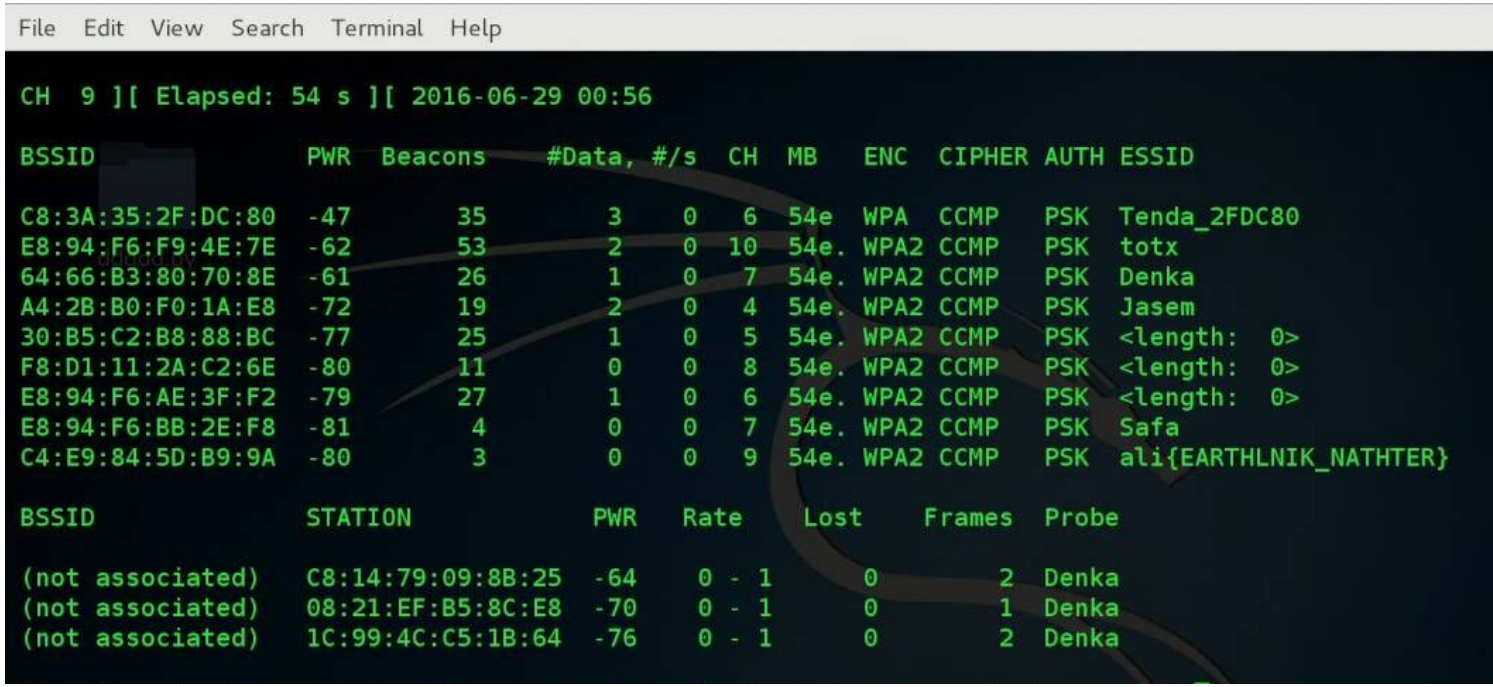
- **802.11i encryption standards for many of the above**

Terminology

- Extended Service Set Identifier (**ESSID**)
  - **Name** of a network
- Basic service set identifiers (**BSSID**)
  - **MAC** address of a network

- **STA** (work station)
  - Client

- **AP** (access point)
- **Ch**: channel



Outline

- Introduction
- Wireless threats
- WIFI security
  - Open Wi-Fi
  - Obscurity
  - WEP/WPA
  - WPA2
  - WPA3
- **Intro to NFC/RFID security**
- **Conclusion**
- **Lab exercises**

Open Wi-Fi network

- Common(?) for cafes, airports, etc.
- The worst option of all
- No encryption whatsoever
- Everyone can see everything

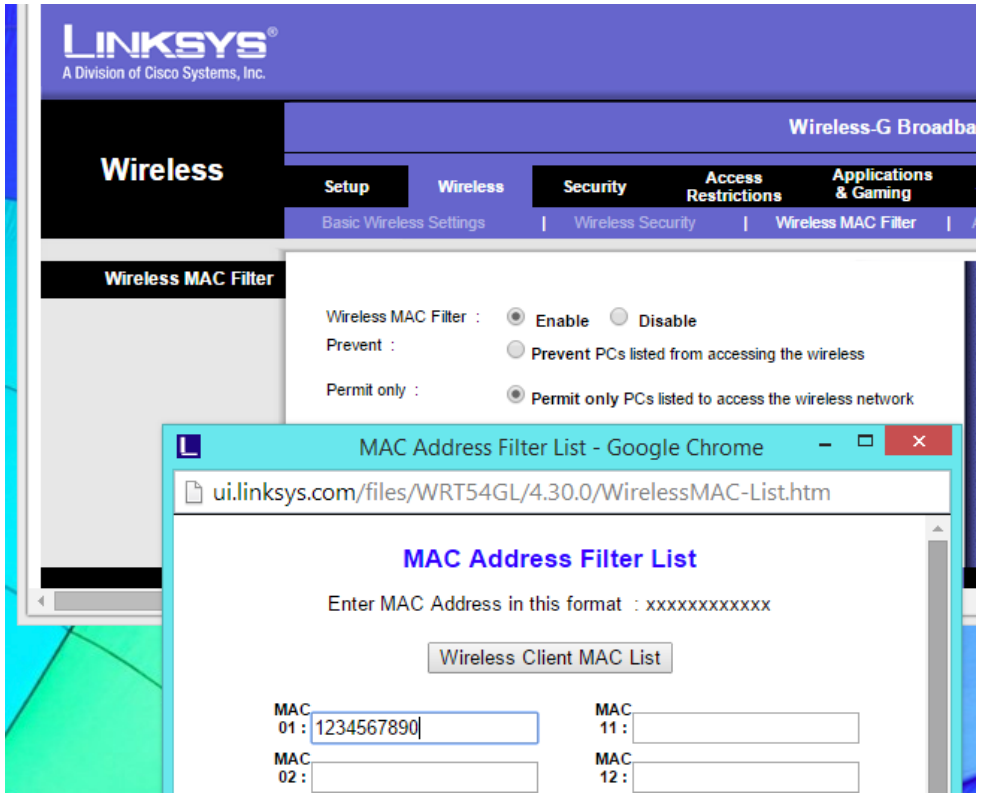
- HTTPS helps
- VPN helps too

Outline

- Introduction
- Wireless threats
- WIFI security
  - Open Wi-Fi
  - Obscurity
  - WEP/WPA
  - WPA2
  - WPA3
- **Intro to NFC/RFID security**
- **Conclusion**
- **Lab exercises**

Other (weird) Wi-Fi security/obscurity techniques

- MAC filtering (e.g. whitelisting)
  - Does not make sense
  - Anyone can see who is connected to a wireless network
  - ***macchanger -m b2:aa:0e:56:ed:f7 eth0***
- Hidden Wi-Fi SSID (-.-)
- No WiFi
  - Many organizations have such a policy
- Lower your router's signal power
- Anti-WiFi paint (!)
  - Blocks WiFi signals
  - (Faraday cage paradigm)
  - Similar to NFC/RFID wallets

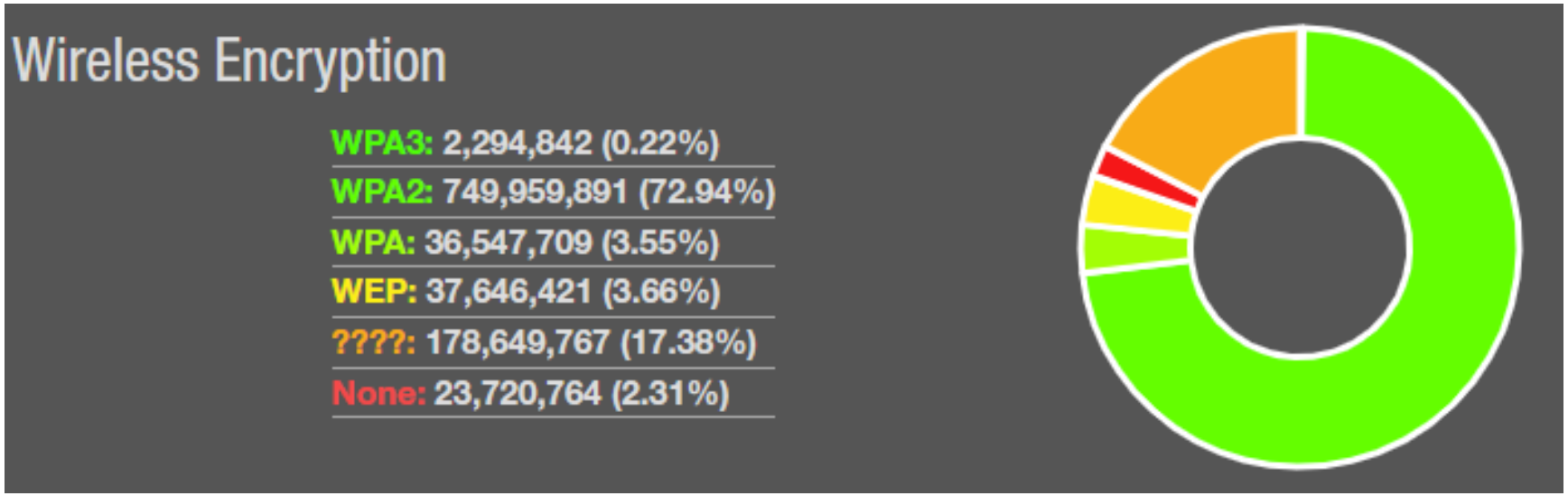


Outline

- Introduction
- Wireless threats
- WIFI security
  - Open Wi-Fi
  - Obscurity
  - WEP/WPA
  - WPA2
  - WPA3
- Intro to NFC/RFID security
- Conclusion
- Lab exercises

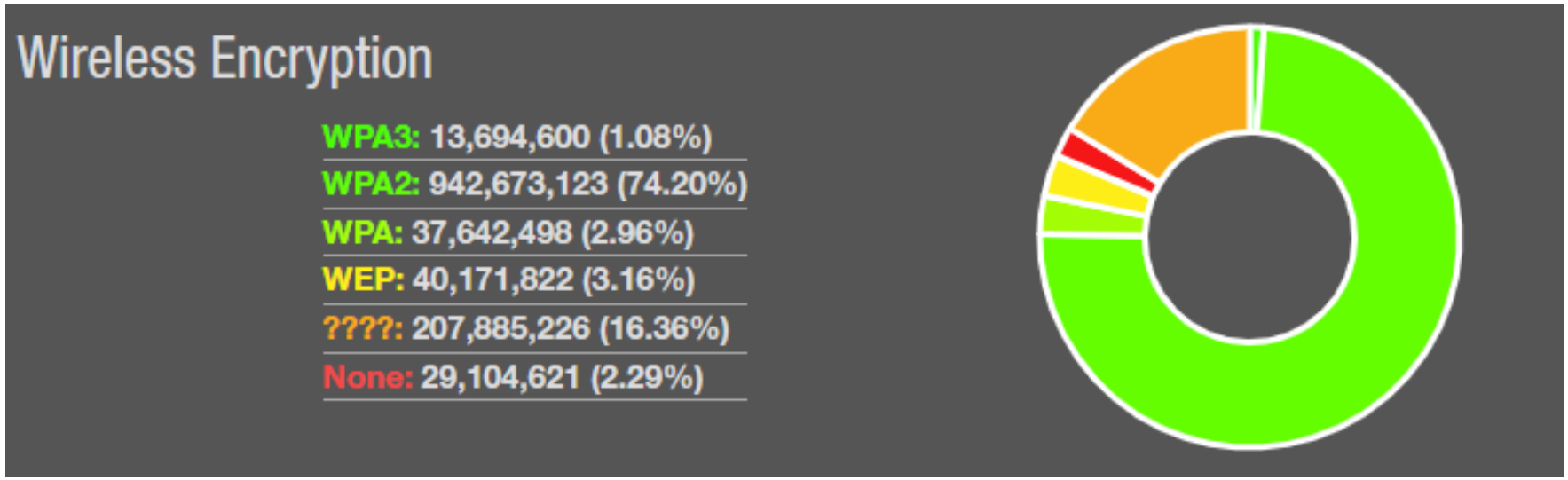
WEP, WPA, WPA2 and open networks

- **Statistics from 2023**
  - https://wigle.net/stats
- **WEP and WPA are dying ☺**
- **Open networks still here ☹**
- **(no stats for WPS)**

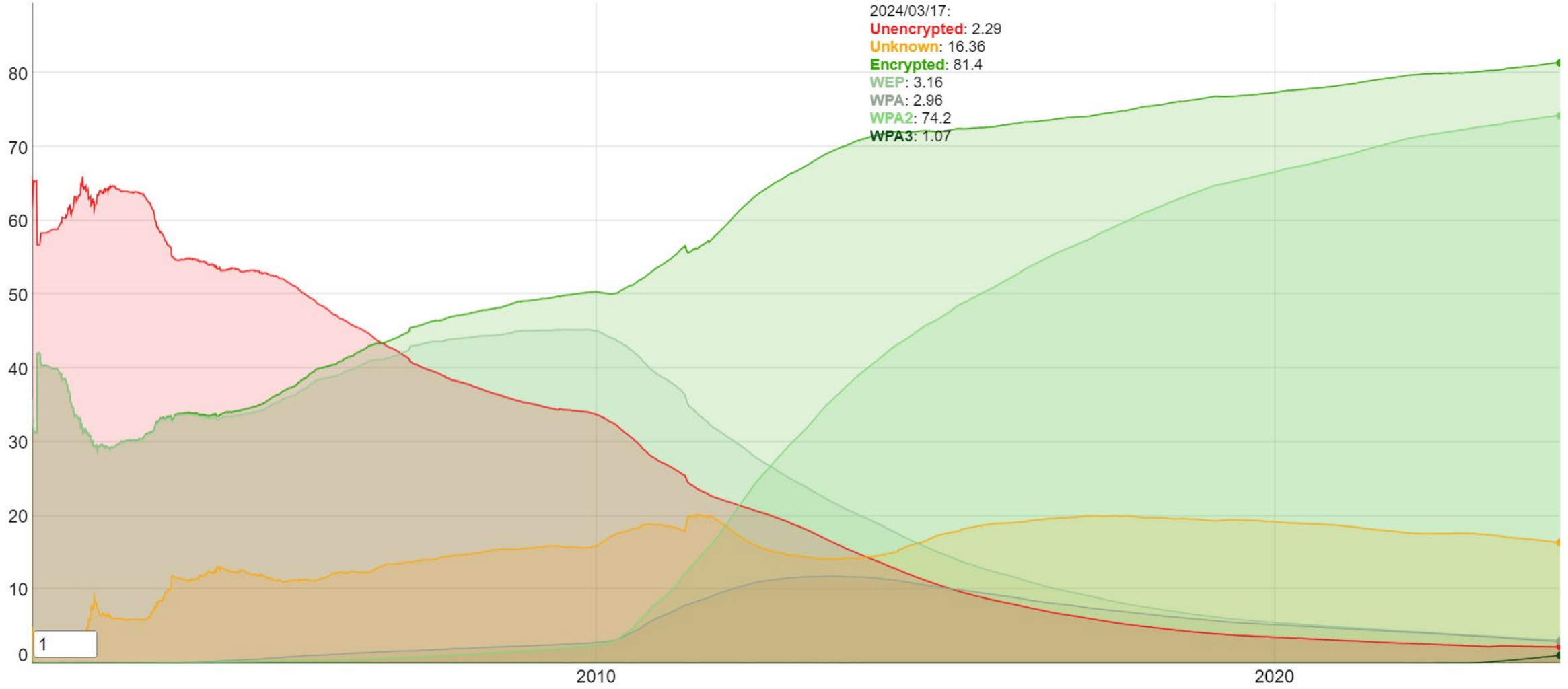


WEP, WPA, WPA2 and open networks

- **Statistics from 2024**
  - https://wigle.net/stats
- **WEP and WPA are dying ☺**
- **Open networks still here ☹**
- **(no stats for WPS)**



WEP, WPA, WPA2 and open networks

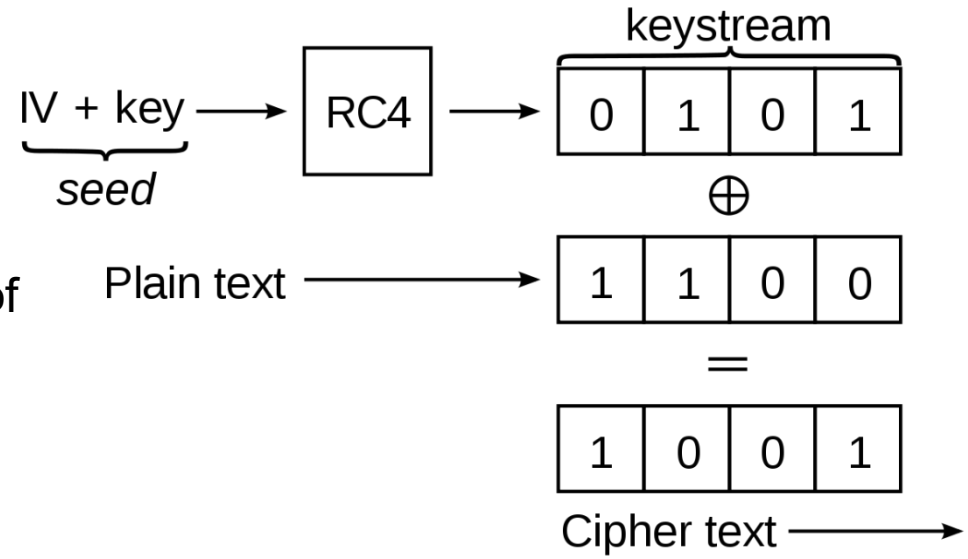


WEP

- “Wired Equivalent Privacy”
- 64/128-bit seed (24-bit IV + 40/104-bit shared key)
- RC4 stream cipher
- CRC32 integrity check
- Open or handshake authentication
- “Weaknesses in the Key Scheduling Algorithm of RC4”, Fluhrer, Mantin and Shamir, 2001
  - Related key attack, exploits small IV keyspace (16.7M)
  - Key recovery in a short time (minutes on a busy network)

WEP attacks

- RC4 is weak (and remember it's a stream cipher)
- IVs must not repeat
- However, IV is only 24bit
- With certain IVs, an attacker knowing the first byte of the keystream and the first m bytes of the key can derive the (m + 1)th byte of the key due to a weakness in the PRNG used to generate the keystream



WEP attacks

- Attack is trivial and fast.
- Just don’t use it.

WPA-1

- WPA stands for “Wifi Protected Access”
  - Temporal fix for WEP
  - **Implements a subset of 802.11i**
- Uses Temporal Key Integrity Protocol (TKIP)
  - Key mixing instead of straight concatenation
    - Dynamic session key
    - Session key + IV -> RC4
  - Sequence numbering
  - 64-bit message integrity check
    - 2 invalid MICs in 60 seconds triggers session key rotation
    - Rotation requires a 60-second timeout (DoS anyone?)
- Message Integrity Checks (MIC)
  - Replaces CRC (no strong data integrity guarantees)
  - Attack exists for WPA-1 (on the MIC hash function Michael)

Outline

- Introduction
- Wireless threats
- WIFI security
  - Open Wi-Fi
  - Obscurity
  - WEP/WPA
  - WPA2
  - WPA3
- Intro to NFC/RFID security
- Conclusion
- Lab exercises

WPA-2 (IEEE 802.11i-2004)

- What is WPA2?
  - Wi-Fi Protected Access 2
  - Introduced September 2004
  - **Two Versions**
    - **Personal** (PSK) – AES Pre-Shared Key
    - **Enterprise** – Server Authentication 802.1x
  - Full implementation of 802.11i

WPA-2 Personal (aka pre-shared key (PSK))

- Commonly used everywhere
- At your house, cafes, small companies, etc.
- Password between 8 (minimum) and 63 characters long

- Okaysh security, as long as:
  - **All** devices are trusted
  - Password **super strong**
  - **Physical** security okay
  - **SSID** name is unique/random
  - ISP and/or router are not providing **weak passwords** by default
  - **WPS** is disabled
  - Your OS is patched against the KRACK attack
  - (that's **a lot of assumptions**)

Okay, so we have a few keys and terms

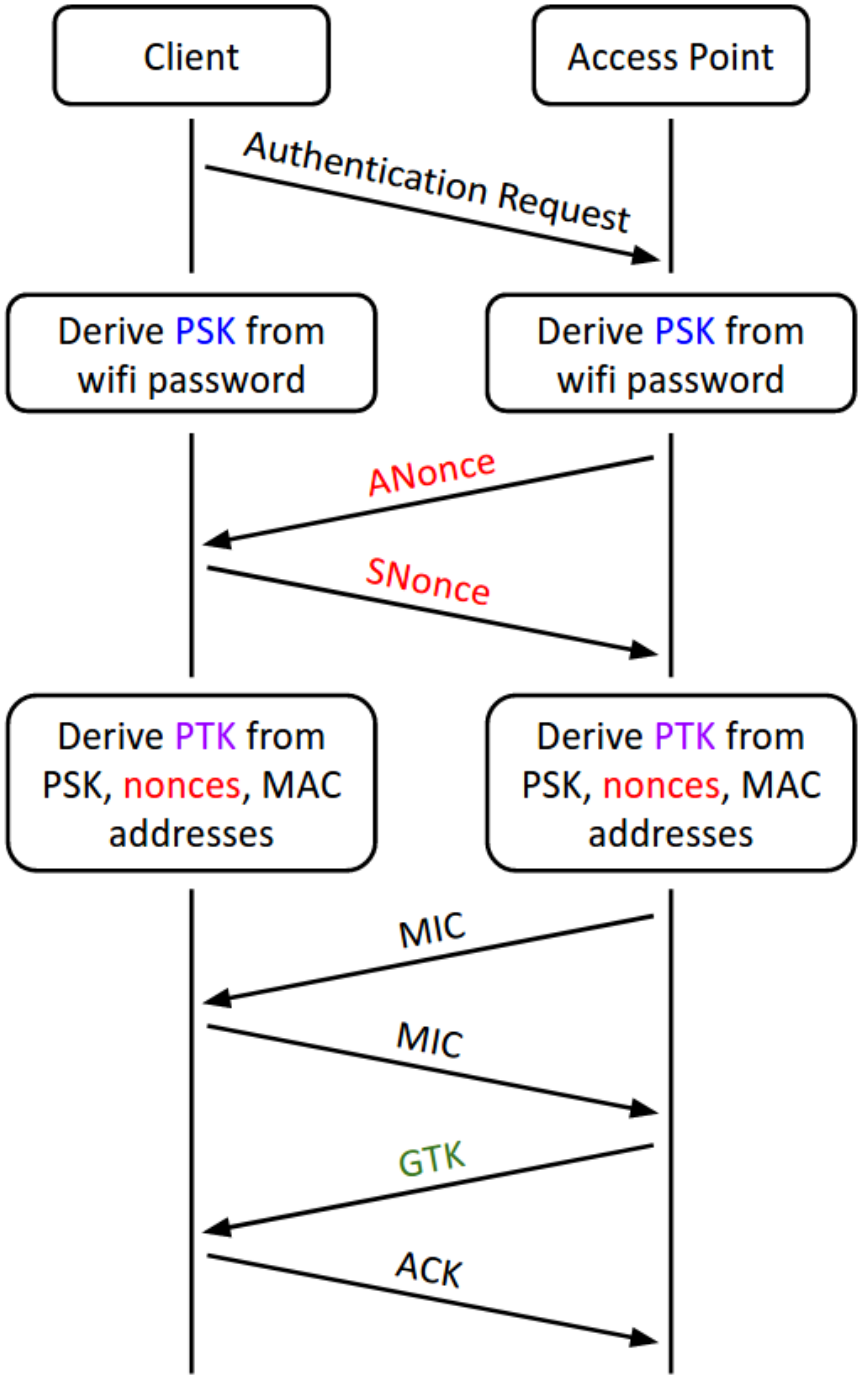
- **PSK** (Pre-shared Key)
- **PTK** (Pairwise Transit Key)
  - **PTK = PBKDF2-SHA1 (PSK + ANonce + SNonce + Mac (AA)+ Mac (SA))**
- ANonce (AP nonce)
- SNonce (STA nonce)
- MIC (message integrity code)
- MAC (media access control) address

Okay, so we have a few keys and terms

- **PMK** (Pairwise Master Key)
  - In WPA2 personal PMK = PSK
- **GMK** (Group Master Key)
  - Used to create GTK
  - Same for all STAs connecting to a specific AP
  - for multicast and broadcast
- **GTK** (Group Temporal Key)
  - used to decrypt multicast and broadcast traffic
  - Changes every time a device leaves a network
  - Distributed securely via pairwise keys that are already established

Handshake

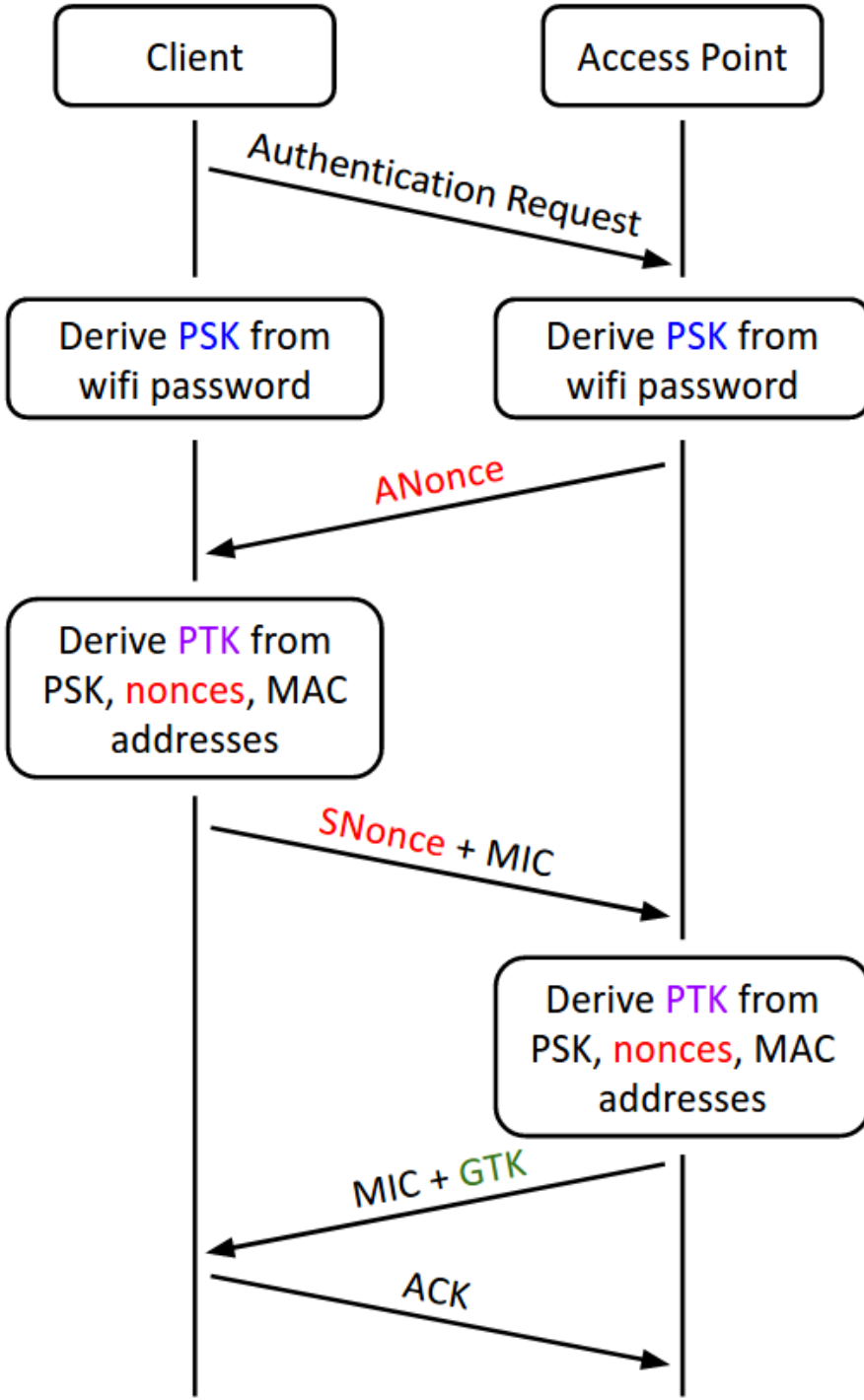
- The client and the access point exchange random nonces, the ANonce and the SNonce.
  - The **nonces ensure that different keys** will be generated during each handshake.
  - The nonces are sent without any encryption.
- The client and access point independently derive the PTK (Pairwise Transport Keys) **as a function of the two nonces, the PSK, and the MAC addresses of both the access point and the client**.
- The client and the access point exchange MICs to check that no one tampered with the nonces, and that both sides correctly derived the PTK.
- The access point encrypts the GTK (Group Temporal Key) and sends it to the client.
- The client sends an ACK (acknowledgement message) to indicate that it successfully received the GTK.
- **All future communication is encrypted with the PTK**
- GTK used for messages broadcast to the entire network



Handshake - simplified

- In practice, the handshake is optimized into a 4-way handshake, requiring only 4 messages to be exchanged between the client and the access point

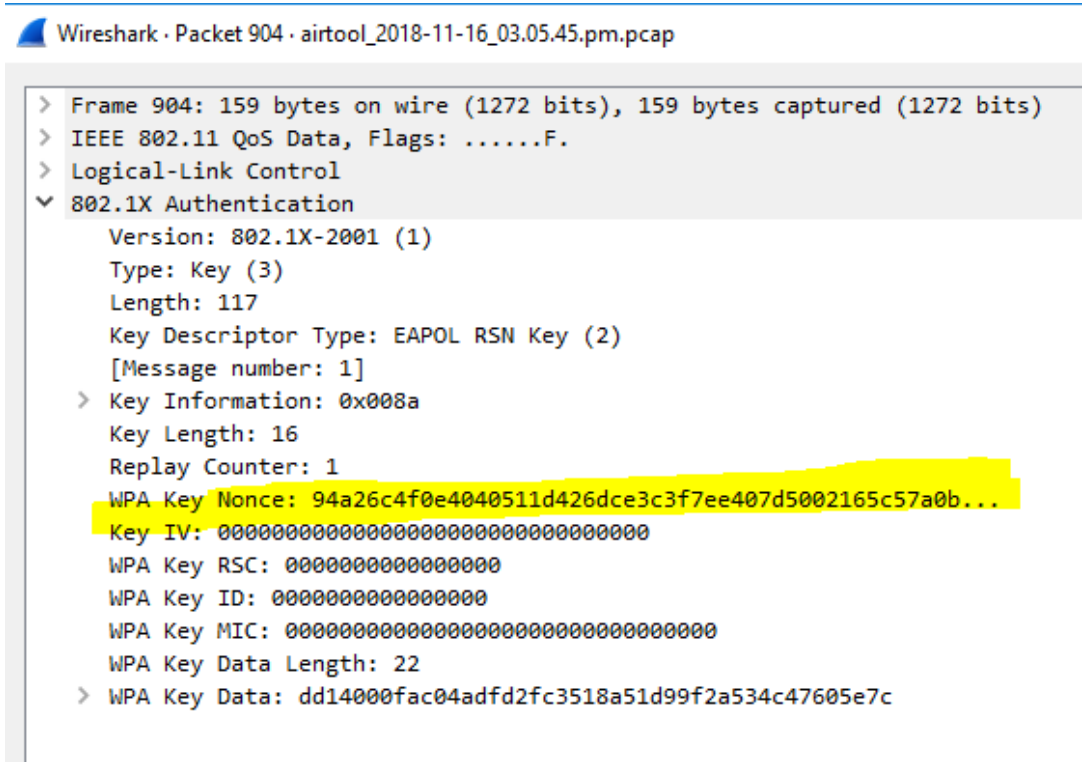
- The access point sends the ANonce, as before.
- Once the client receives the ANonce, it has all the information needed to derive the PTK, so it derives the PTK first. Then it sends the SNonce and the MIC to the access point.
- Once the access point receives the SNonce, it can derive the PTK as well. Then it sends the encrypted GTK and the MIC to the client.
- The client sends an ACK to indicate that it successfully received the GTK, as before.



WPA-2: four-way handshake details – message 1

904 EAPOL	Data frame	9c:5d:12:5e:6c:66	QoS Data	d0:c5:f3:a9:16:c5	Key (Message 1 of 4)
906 EAPOL	Data frame	d0:c5:f3:a9:16:c5	QoS Data	9c:5d:12:5e:6c:66	Key (Message 2 of 4)
908 EAPOL	Data frame	9c:5d:12:5e:6c:66	QoS Data	d0:c5:f3:a9:16:c5	Key (Message 3 of 4)
910 EAPOL	Data frame	d0:c5:f3:a9:16:c5	QoS Data	9c:5d:12:5e:6c:66	Key (Message 4 of 4)

904 EAPOL	Data frame	9c:5d:12:5e:6c:66	QoS Data	d0:c5:f3:a9:16:c5	Key (Message 1 of 4)



WPA-2: four-way handshake details – message 2

Wireshark · Packet 906 · airtool_2018-11-16_03.05.45.pm.pcap

```
> Frame 906: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits)
> IEEE 802.11 QoS Data, Flags: .......T
> Logical-Link Control
v 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 117
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 2]
  v Key Information: 0x010a
      .... .... .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
      .... .... .... 1... = Key Type: Pairwise Key
      .... .... ..00 .... = Key Index: 0
      .... .... .0.. .... = Install: Not set
      .... .... 0... .... = Key ACK: Not set
      .... ...1 .... .... = Key MIC: Set
      .... ..0. .... .... = Secure: Not set
      .... .0.. .... .... = Error: Not set
      .... 0... .... .... = Request: Not set
      ...0 .... .... .... = Encrypted Key Data: Not set
      ..0. .... .... .... = SMK Message: Not set
    Key Length: 16
    Replay Counter: 1
    WPA Key Nonce: b15a752ad4aa52ab4aafaa8155fa57e8bf45fd160ba75d3d...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: d9ca9dcdf198716734767e37a60f7ded
    WPA Key Data Length: 22
  > WPA Key Data: 30140100000fac040100000fac040100000fac010c00
```

WPA-2: four-way handshake details – messages 3 and 4

Wireshark · Packet 908 · airtool_2018-11-16_03.05.45.pm.pcap

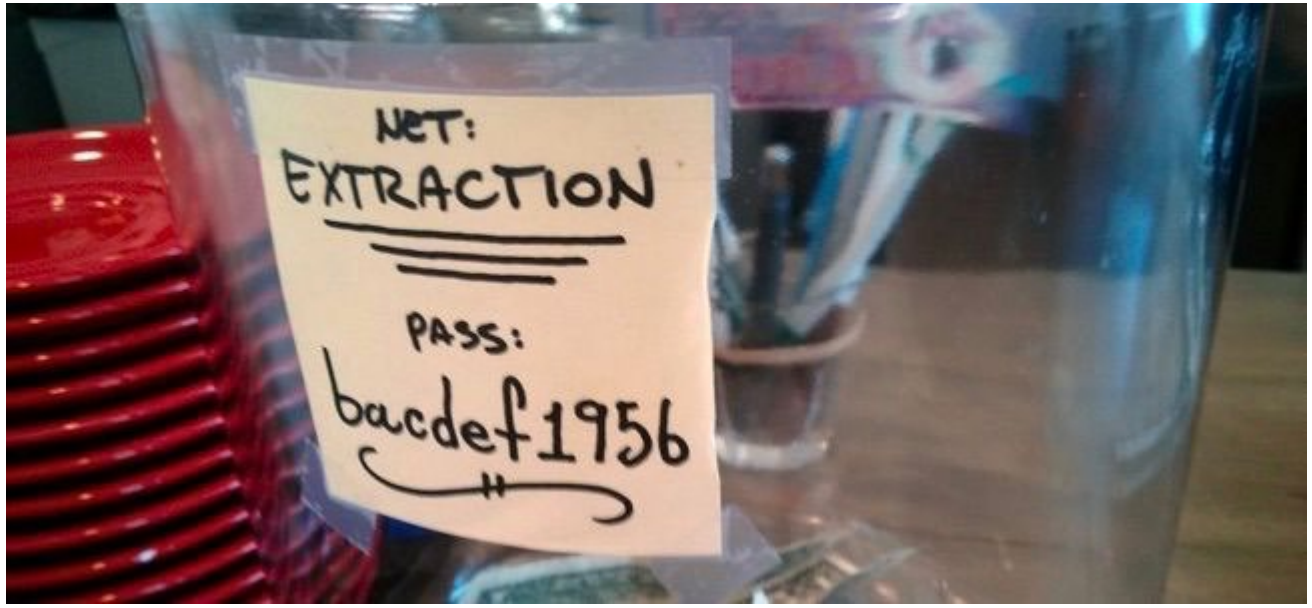
```
> Frame 908: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits)
> IEEE 802.11 QoS Data, Flags: ......F.
> Logical-Link Control
v 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 151
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 3]
  v Key Information: 0x13ca
      .... .... .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
      .... .... .... 1... = Key Type: Pairwise Key
      .... .... ..00 .... = Key Index: 0
      .... .... .1.. .... = Install: Set
      .... .... 1... .... = Key ACK: Set
      .... ...1 .... .... = Key MIC: Set
      .... ..1. .... .... = Secure: Set
      .... .0.. .... .... = Error: Not set
      .... 0... .... .... = Request: Not set
      ...1 .... .... .... = Encrypted Key Data: Set
      ..0. .... .... .... = SMK Message: Not set
    Key Length: 16
    Replay Counter: 2
    WPA Key Nonce: 94a26c4f0e4040511d426dce3c3f7ee407d5002165c57a0b...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: b4c0510000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: b8371c079672d6edc73079cec3b1a9aa
    WPA Key Data Length: 56
    WPA Key Data: eda2301b632e9a24e8654811224ad4c7780b3526e5ca8a00...
```

Overall picture

Management frame	74:3e:2b:23:13:a8	Beacon frame	ff:ff:ff:ff:ff:ff	V-home	Beacon frame, SN=3046, FN=0, Flags=.....
Management frame	74:3e:2b:63:13:a8	Beacon frame	ff:ff:ff:ff:ff:ff	Ruckus	Beacon frame, SN=771, FN=0, Flags=.....
Management frame	74:3e:2b:a3:13:a8	Beacon frame	ff:ff:ff:ff:ff:ff	PRINTERS	Beacon frame, SN=1237, FN=0, Flags=.....
Management frame	74:3e:2b:a3:13:a8	Authentication	cc:08:8d:53:66:1d		Authentication, SN=0, FN=0, Flags=.....
Control frame		Acknowledgement			Acknowledgement, Flags=.....C
Management frame	cc:08:8d:53:66:1d	Association Request	74:3e:2b:a3:13:a8	PRINTERS	Association Request, SN=3992, FN=0, Flags=
Control frame		Acknowledgement			Acknowledgement, Flags=.....C
Management frame	74:3e:2b:a3:13:a8	Association Response	cc:08:8d:53:66:1d		Association Response, SN=1, FN=0, Flags=..
Management frame	74:3e:2b:a3:13:a8	Association Response	cc:08:8d:53:66:1d		Association Response, SN=1, FN=0, Flags=..
Control frame		Acknowledgement			Acknowledgement, Flags=.....C
Data frame	74:3e:2b:a3:13:a8	QoS Data	cc:08:8d:53:66:1d		Key (Message 1 of 4)
Control frame		Acknowledgement			Acknowledgement, Flags=.....C
Data frame	cc:08:8d:53:66:1d	QoS Data	74:3e:2b:a3:13:a8		Key (Message 2 of 4)
Data frame	cc:08:8d:53:66:1d	QoS Data	74:3e:2b:a3:13:a8		Key (Message 2 of 4)
Control frame		Acknowledgement			Acknowledgement, Flags=.....C
Data frame	74:3e:2b:a3:13:a8	QoS Data	cc:08:8d:53:66:1d		Key (Message 3 of 4)
Control frame		Acknowledgement			Acknowledgement, Flags=.....C
Data frame	cc:08:8d:53:66:1d	QoS Data	74:3e:2b:a3:13:a8		Key (Message 4 of 4)
Control frame		Acknowledgement			Acknowledgement, Flags=.....C
Data frame	cc:08:8d:53:66:1d	QoS Data	b4:30:52:cd:f8:94		QoS Data, SN=2193, FN=0, Flags=.p....F.C
Control frame		802.11 Block Ack			802.11 Block Ack, Flags=.....C
Data frame	cc:08:8d:53:66:1d	QoS Data	34:2d:0d:56:88:cd		QoS Data, SN=977, FN=0, Flags=.p....F.C
Control frame		Acknowledgement			Acknowledgement, Flags=.....C
Data frame	cc:08:8d:53:66:1d	QoS Data	54:88:0e:00:1e:ae		QoS Data, SN=3802, FN=0, Flags=.p....F.C

Is WPA-2 (PSK) good for coffee places?

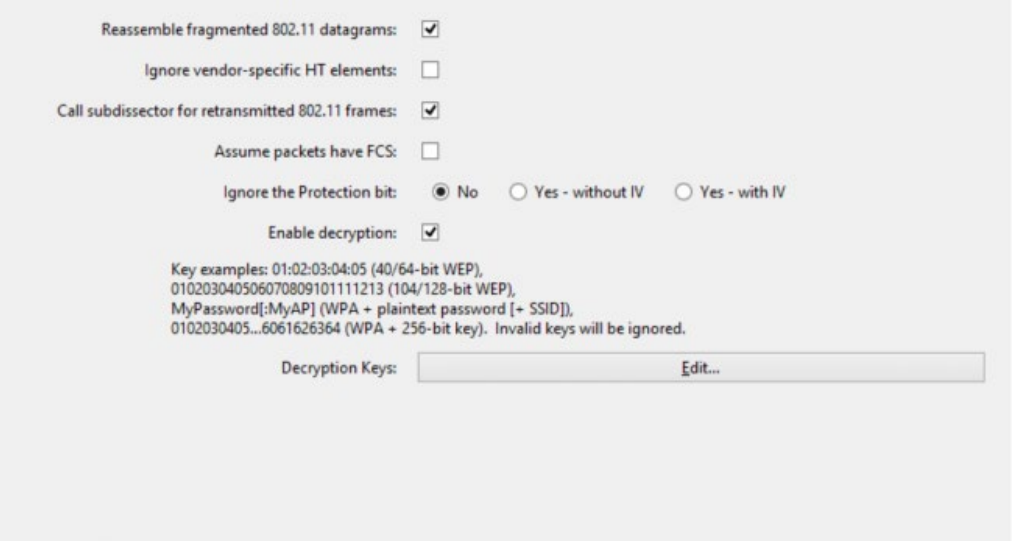
- Is it better than an open network?
- Open discussion



WPA2 PSK: NOT good for coffee places ☹

- If someone knows the **PSK** (i.e. the password of the place)
- And also captures the **association traffic** for a new client (packets sent between the router and a device when it first connects)
  - It's also trivial to get this traffic via "deauth" attacks that forcibly disconnect a device from a Wi-Fi network and force it to reconnect, causing the association process to happen again

- Then:
  - **They can decrypt everything!**



WPA2 PSK: why?????

- Remember the PTK (pairwise transient key)?
  - Each STA has a unique PTK that is used for the encryption
  - Problem: PTK is derived by the PSK
    - **PTK = PBKDF2-SHA1 (PSK + ANonce + SNonce + Mac (AA)+ Mac (SA))**

- Solution (from the coffee manager's perspective):
  - Use WPA2 enterprise (overkill/impossible for small coffee places)
  - Use WPA3 (more and more support for this!)

- Solution (from the users' perspective):
  - Do not use Wi-Fi networks you do not trust (right?)
  - Use VPN

Password Cracking WPA2

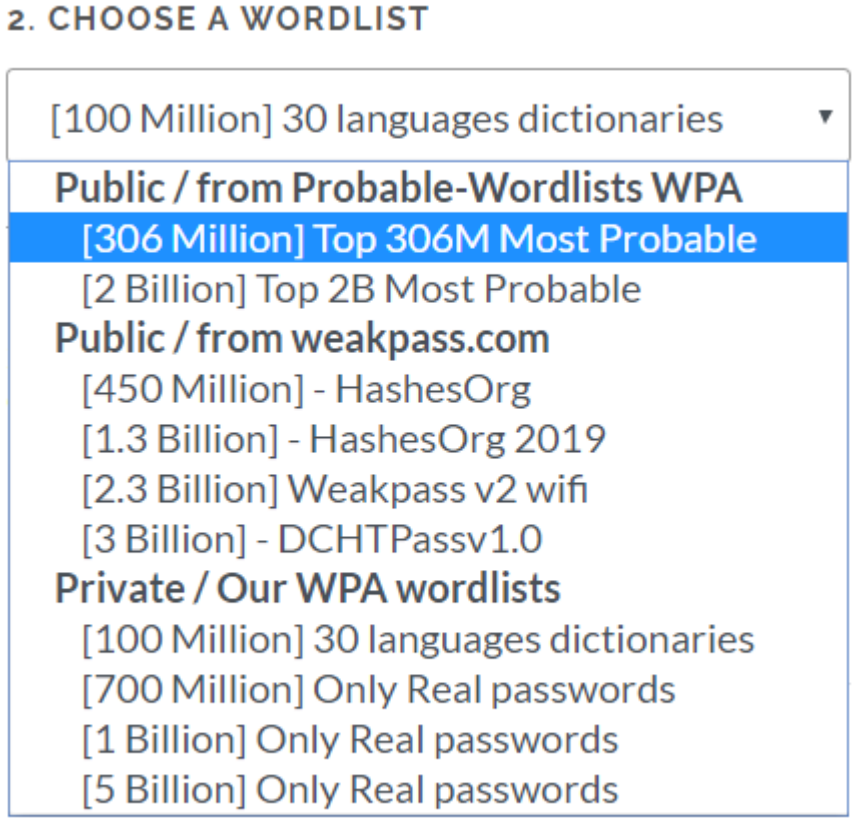
- WPA2 uses PBKDF2
  - Password-Based Key Derivation Function #2
  - From RSA Labs
  - Inputs: Password, Salt, Iteration Count
  - Output: A Key
    - More iterations makes it take longer
    - WPA2 uses 4096 iterations of SHA-1
    - **Salt is the SSID**
    - Password is 8 chars min (63 max)

WPA-2 attacks: deauth and grab the handshake

- PTK is transmitted when a device connects to an AP
  - This might not happen that much, right?
- We can send a deauth packet to a device and it will reconnect
  - A bit more intrusive than just passively sniffing
  - AirCrack-ng can do this for you

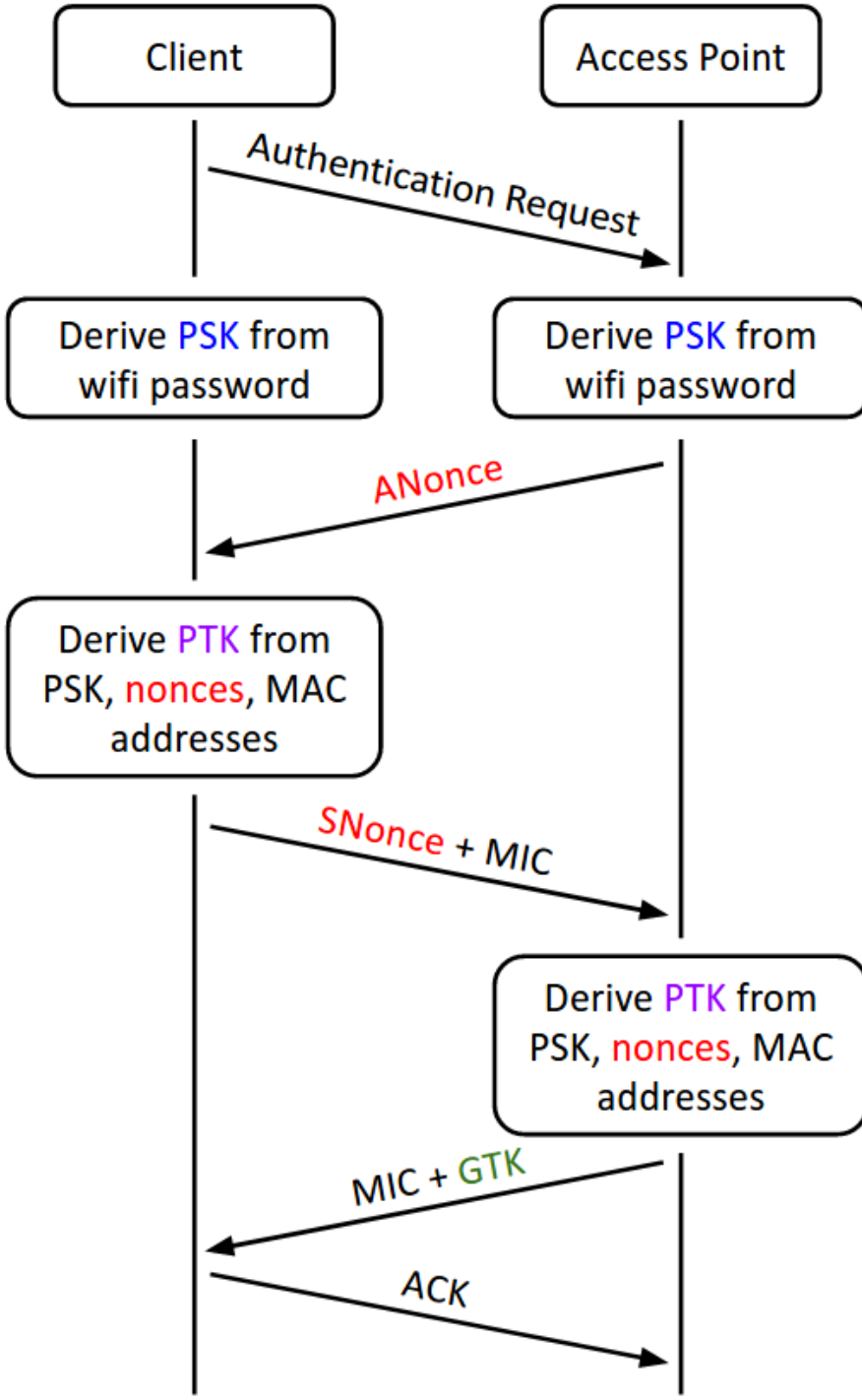
WPA-2 attacks: with handshake -> offline attack

1. Use **rainbow** tables
   - A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes
   - Assuming the target **SSID** is among the top-1000 for which there are rainbow tables
2. Use **dictionaries/password lists**
3. Use **online cracking** services



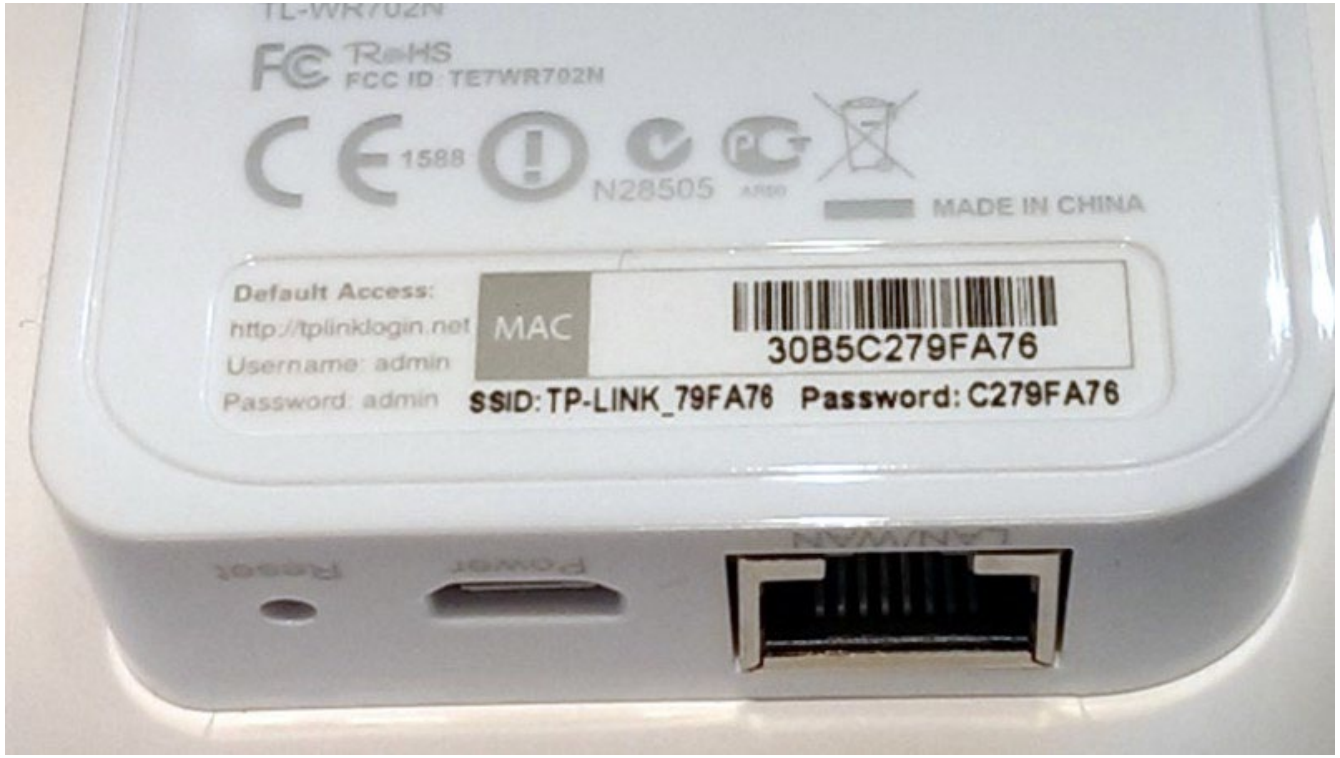
Other WPA-2 attacks

- KRACK (**K**ey **R**einstallation **Atta**c**k**s) attack
- Attacker doesn't learn the password (key) but is able to decrypt traffic
- MitM/evil twin style attack, 2017
- Attacks Messages 3 and 4 of the handshake
- Resets the nonces (msgs 1 and 2)
- Reuses the nonces
- Attack especially targeting Linux/Android
  - Implementation of protocol and reaction to message 3 replaying
  - wpa_supplicant bug installs an all-zero key



Other WPA2 attacks

- and lastly…
- there is always the **vendor/implementation of security**
- **Can you spot the problem(s) here?**



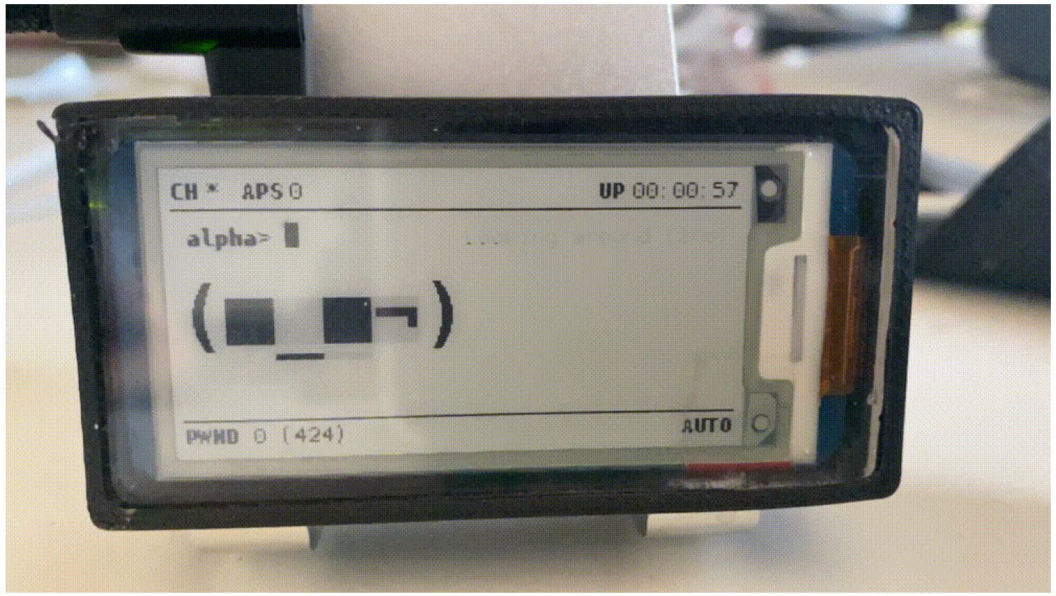
Other WPA2 attacks

- **Many fancy/cute attacks use similar techniques as we have seen before**

PWNAGOTCHI: DEEP REINFORCEMENT LEARNING FOR WIFI PWNING!

Pwnagotchi is an A2C-based "AI" powered by bettercap and running on a Raspberry Pi Zero W that learns from its surrounding WiFi environment in order to maximize the crackable WPA key material it captures (either through passive sniffing or by performing deauthentication and association attacks). This material is collected on disk as PCAP files containing any form of handshake supported by hashcat, including full and half WPA handshakes as well as PMKIDs.

Learn more about the project and how it started on the author's blog.



WPA-2 Personal: re-cap

- Okaysh security, as long as:
  - **All** devices are trusted
  - Password **super strong**
  - **Physical** security okay
  - **SSID** name is unique/random
  - ISP and/or router are not providing **weak passwords** by default
  - OS patched against the KRACK attack
  - **WPS** is disabled
  - (that's **a lot of assumptions**)

WPS (Wi-Fi Protected Setup)

- “Hey, WPA2 passwords are too complicated, wouldn’t it be nice to have super easy pins with the same security?”
- WPS (Wi-Fi Protected Setup)
  - Wi-Fi-Alliance, 2006
- The WPS protocol consists of a series of EAP message exchanges that are triggered by a user action, relying on an exchange of descriptive information that should precede that user's action
  - The descriptive information is transferred through a new Information Element (IE) that is added to the beacon, probe response, and optionally to the probe request and association request/response messages.
  - Other than purely informative type-length-values, those IEs will also hold the possible and the currently deployed configuration methods of the device

WPS (Wi-Fi Protected Setup)

- After this communication of the device capabilities from both ends, the user initiates the actual protocol session
  - The session consists of eight messages that are followed, in the case of a successful session, by a message to indicate that the protocol is completed.
  - The exact stream of messages may change when configuring different kinds of devices (AP or STA), or when using different physical media (wired or wireless)

WPS modes

- **PIN method:**
  - PIN has to be read from either a sticker or display on the new wireless device. This PIN must then be entered at the "representant" of the network, usually the network's access point. Alt access point may be entered into the new device. This method is the mandatory baseline mode and everything must support it. The Wi-Fi Direct specification supersedes this requirement by stating that all devices with a keypad or display must support the PIN method
- **Push button method:**
  - User has to push a button, either an actual or virtual one, on both the access point and the new wireless client device. On most devices, this discovery mode turns itself off as soon as a connection is established or after a delay (typically 2 minutes or less), whichever comes first, thereby minimizing its vulnerability. Support of this mode is mandatory for access points and optional for connecting devices. The Wi-Fi Direct specification supersedes this requirement by stating that all devices must support the push button method
- **Near-field communication method:**
  - User has to bring the new client close to the access point to allow a near field communication between the devices. NFC Forum–compliant RFID tags can also be used. Support of this mode is optional
- **USB method:**
  - User uses a USB flash drive to transfer data between the new client device and the network's access point. Support of this mode is optional, but deprecated

WPS attacks

Physical security issues

Online brute-force attack

- 2011: reported a design and implementation flaw that makes brute-force attacks against PIN-based WPS
- The vulnerability centers around the acknowledgement messages sent between the registrar and enrollee when attempting to validate a PIN, which is an **eight-digit** number used to add new WPA enrollees to the network
- Eight digit means 10^8 = 100,000,000 possible combinations
- **But**, since the **last digit is a checksum of the previous digits**, there are seven unknown digits in each PIN, yielding 10^7 = 10,000,000 possible combinations.
- When someone tries a PIN, the registrar reports the validity of the first and second halves of the PIN separately. Since the first half of the pin consists of four digits (10,000 possibilities) and the second half has only three active digits (1000 possibilities), at most 11,000 guesses are needed before the PIN is recovered
- This is a **reduction** by **three orders of magnitude**. As a result, an attack can be completed in under four hours. The ease or difficulty of exploiting this flaw is implementation-dependent, as Wi-Fi router manufacturers could defend against such attacks by slowing or disabling the WPS feature after several failed PIN validation attempts
- In some devices, **disabling WPS in the user interface does not result in the feature actually being disabled, and the device remains vulnerable to this attack**. Firmware updates have been released for some of these devices allowing WPS to be disabled completely. Vendors could also patch the vulnerability by adding a lock-down period if the Wi-Fi access point detects a brute-force attack in progress, which disables the PIN method for long enough to make the attack impractical

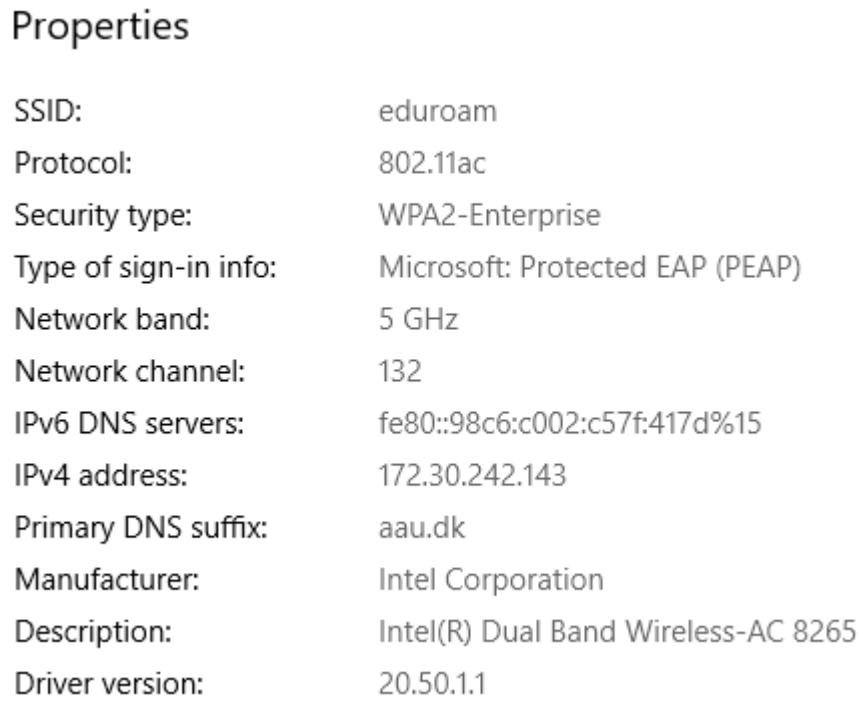
Outline

- Introduction
- Wireless threats
- WIFI security
  - Open Wi-Fi
  - Obscurity
  - WEP/WPA
  - WPA2
  - WPA3
- Intro to NFC/RFID security
- Conclusion
- Lab exercises

WPA-2: Enterprise

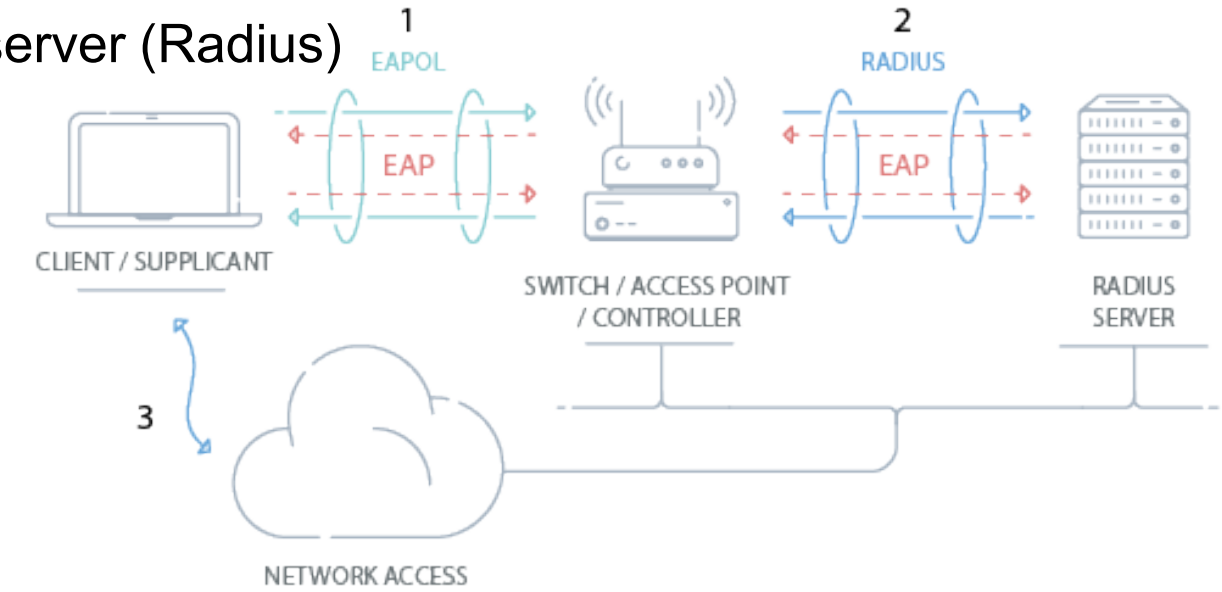
- Intended for large organizations/companies/etc

- The idea is that a single password is not enough
  - What about old/fired employees?
  - Visitors connecting to the Wi-Fi once
  - How can you revoke access with WPA2 PSK?



WPA-2: Enterprise

- Addition of an authentication server (Radius)
  - Checks credentials for validity
- Authentication via
  - PKI
  - Credentials
- Federation possible
  - Eduroam has RADIUS servers work as proxies (such as RADSEC)
  - student visits a neighboring university, the RADIUS server can authenticate their status at their home university and grant them secure network access



WPA-2: Enterprise

- **Authorized users** create a unique username and password
- Before handshake:
  - **Authentication of user over TLS**
- **PMK** (pairwise master key): which in this case is not the same as PSK
  - Truly unique for each user

WPA-2: Enterprise

- Decent security (finally!)

- **But:**
  - **Very complex**
    - **need for Radius servers,**
    - **LDAP server for identity management,**
    - **PKI, certificate generation, distribution, revocation…**
    - **Too much for a home/coffee shop/even small company**

- **Not many attacks for WPA2 enterprise**
  - Evil twin paradigms could be implemented
  - Some downgrade attacks possible

Outline

- Introduction
- Wireless threats
- WIFI security
  - Open Wi-Fi
  - Obscurity
  - WEP/WPA
  - WPA2
  - WPA3
- Intro to NFC/RFID security
- Conclusion
- Lab exercises

WPA3

- WPA2 is quite **old** (15 years old)
- WPA2-personal is **broken** on arrival
  - Off-line attacks had always been possible
- WPA2-Enterprise is good but **complicated**
- Open wireless networks are… open

- **WPA3 plans ahead**
  - Not just with updated crypto

WPA3

- Open networks are now replaced by **Opportunistic Wireless Encryption (OWE)**
  - **Problem:** all Wi-Fi traffic is plaintext
  - **Solution:** all Wi-Fi traffic gets encrypted
- WPA2-PSK mode is replaced by **Simultaneous Authentication of Equals (SAE)**
  - **Problem:** passive offline attacks were possible with PSK
  - **Solution:** protocol is resistant to active, passive and dictionary-type attacks
- WPA3-enterprise now with suite **B/CNSA grade ciphers**
  - **Problem:** mix-and-match nature of WPA2-Enterprise can result to downgrades
  - **Solution:** create a cipher suite and a set of rules to ensure consistency
- Enchantments to **certification testing**
  - **Problem:** too many WPA2-Enterprise certified devices do not properly check certification chains
  - **Solution:** Management frame protection, optional for WPA2, is now mandatory for WPA3

WPA3: Opportunistic Wireless Encryption

- Opportunistic Wireless Encryption (OWE)
  - RFC 8110

- **Unauthenticated Diffie-Hellman** at association time
  - Associate request and response exchange **ephemeral public keys via DH**
  - STA and AP derive a unique PMK (truly pairwise and unknowable by third parties)
  - PMK is used in a 4-way handshake post association to generate traffic encryption keys

- **Unauthenticated**
  - Remember the DH MitM attack
  - Still better than an Open network (and sometimes better than shared/public PSK in coffee shops)

- **Backward compatibility**

WPA3: strong security from weak passwords

- WPA2-PSK: offline dictionary attacks
  - Passive attack: adversary records the 4-way handshake
  - Takes that home (offline) and runs through all possible attacks

- WPA2-PSK replaced by **Simultaneous Authentication of Equals (SAE)**
  - Password-based authentication based on the **dragon fly key exchange**
  - RFC 7664
  - Resistant to active, passive and dictionary attacks

- SAE uses 802.11 authentication frames
  - Authentication generates a PMK, association indicates the PMKID
  - Post-association 4-way handshake generates traffic encryption keys

- SAE provision is identical to WPA2-PSK
  - User simply enters password

Simultaneous Authentication of Equals (SAE)

- Dragonfly key exchange is based on a **zero-knowledge proof**
  - Password indexes into a secret point on an **elliptic curve**
  - Secret point becomes the generator (base) of a unique cryptographic exchange
  - Each side must use the same generator to arrive to the same key (no offline tricks)

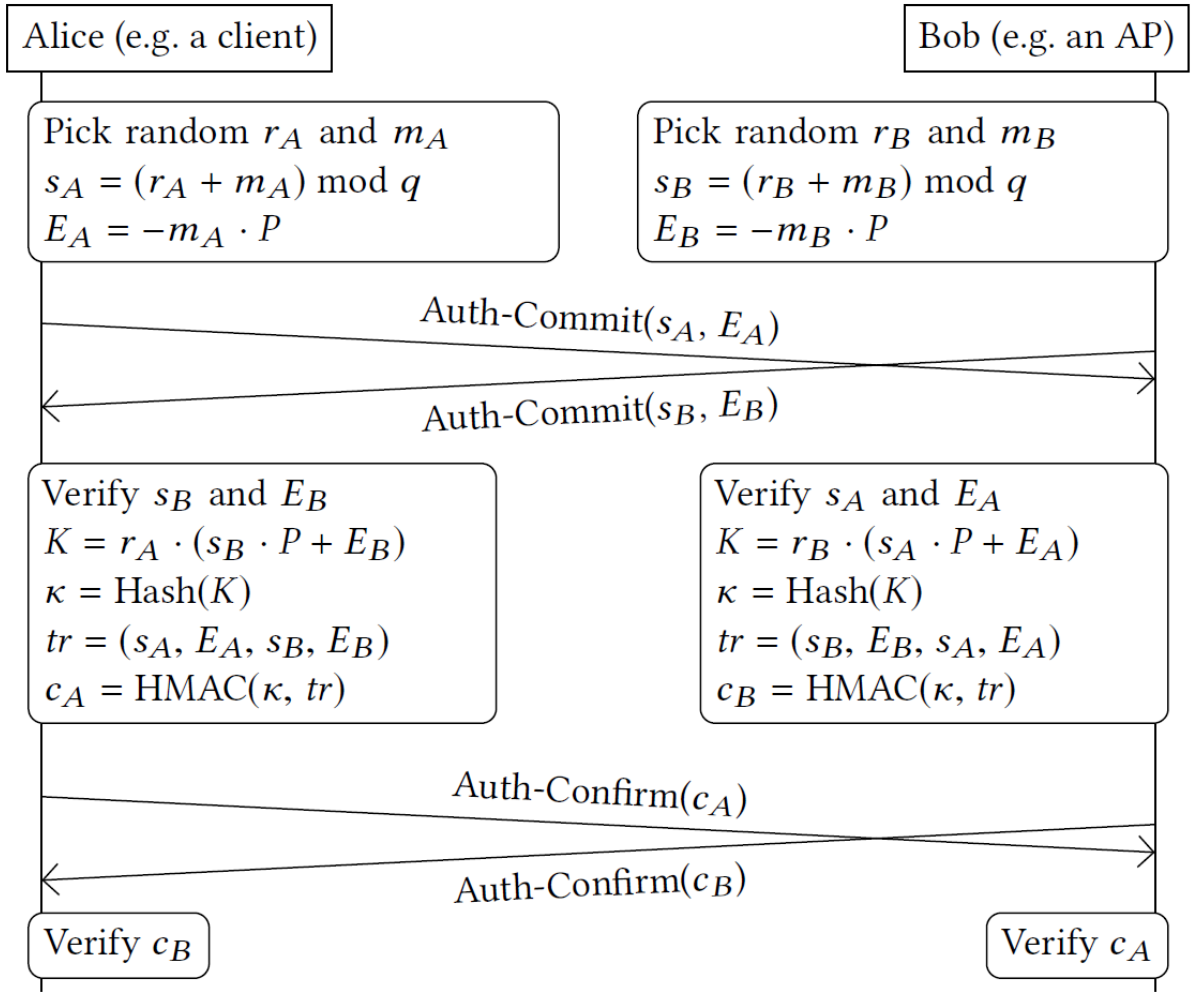
- Passively observing SAE reveals nothing
  - Computational Diffie Hellman assumption

- Active attack reveals whether a single guess of a password was correct or not
  - **Adversarial advantage grows from *interaction* not *computation***
  - Only way to guess the password is from repeated active attacks (detectable)

- Strong protocol allows for “weaker” passwords to be used
  - Probability of guess being correct is n/D, where D is the number of possible passwords with n guesses

Dragonfly protocol

- Each peer picks 2 random numbers (r,m)
- Calculate E
- Send s, E
- Each peer verifies s, E



WPA3-Enterprise: Suite B/CNSA

- WPA2-Enterprise: too many options, especially for EAP authentication
  - DH or RSA, 1024-bit or 2048-bit? TLS1.0? SHA-1?
  - Downgrades and deployments that are less secure
  - Clients may be connecting with really different degrees of security

- Suite B/CNSA provides a consistent level of security for the entire network

- Requires Suite B TLS cipher suites (RFC 6460) to be used in EAP-TLS
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 using p384 or
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 using p384 or
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

- Policy enforced by EAP server based on new RADIUS attributes

- 4-way handshake and KDF use SHA384 with Suite B/CNSA

WPA3 attacks

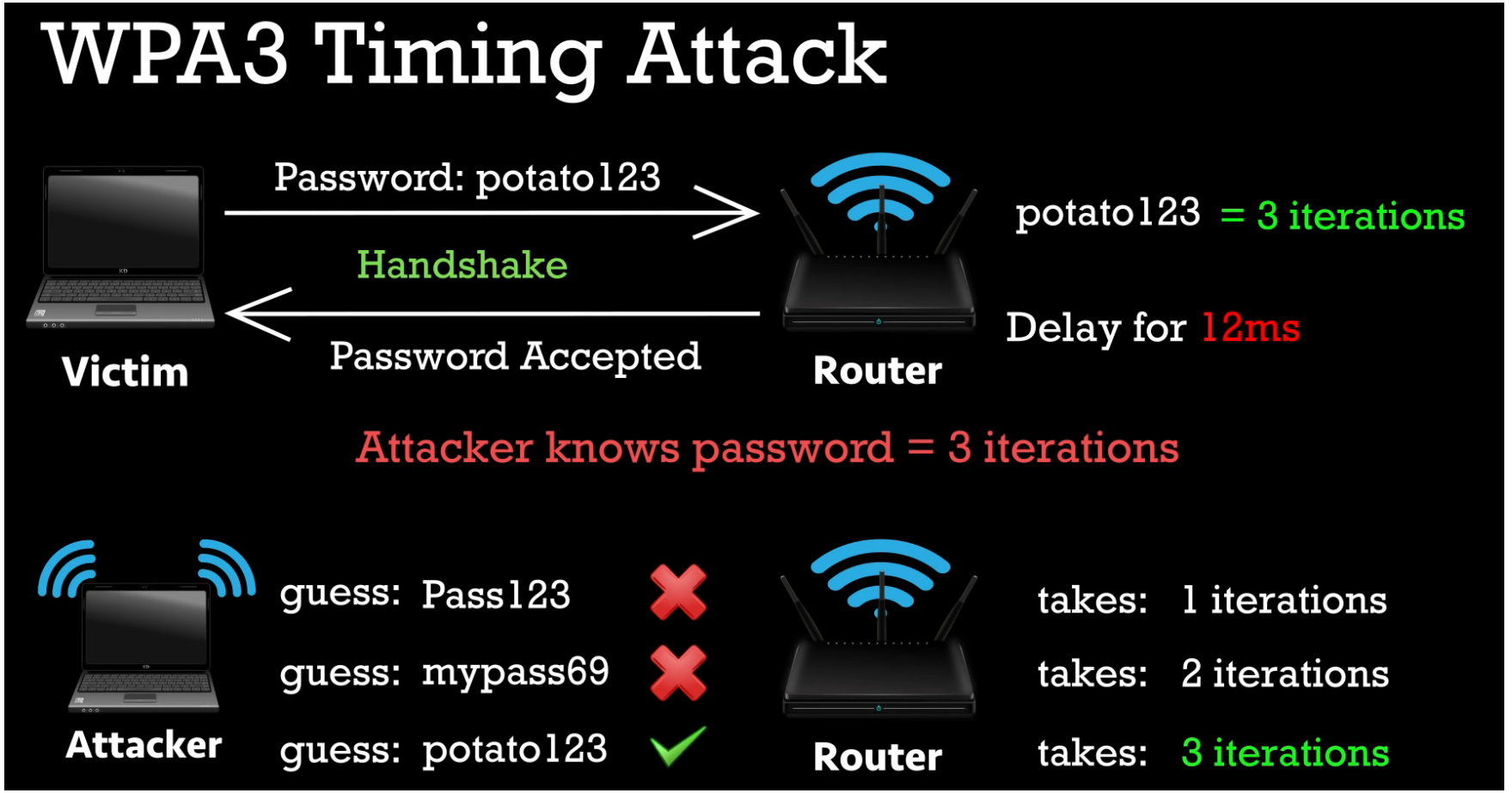
- Criticism to Wi-Fi-alliance:
  - Closed discussions/development of protocol
  - Bad practice / scientific community not happy

- **Dragonblood attacks**
  - **Denial of service** (to the Wi-Fi-router)
  - **Handshake attack** on the dragonfly protocol
    - Fixed by introducing Brainpool curves
      - Introduced new vulnerability… (see next slide)
  - **Side-channel attacks**

- **Downgrade to WPA2 attacks**

- **More info:**
  - https://wpa3.mathyvanhoef.com/

Timing attacks



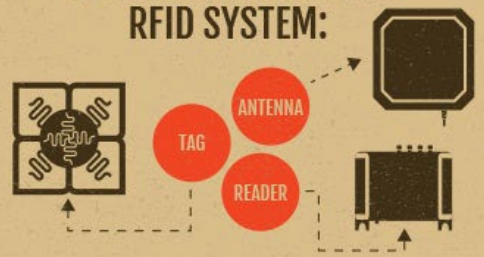
Outline

- Introduction
- Wireless threats
- WIFI security
  - Open Wi-Fi
  - Obscurity
  - WEP/WPA
  - WPA2
  - WPA3
- **Intro to NFC/RFID security**
- **Conclusion**
- **Lab exercises**

A (very) brief intro to nfc/rfid security

RFID & NFC?

3 PARTS OF A TYPICAL RFID SYSTEM:



RFID FREQUENCY RANGES:

Low Frequency (LF):	High Frequency (HF):	Ultra High Frequency (UHF):
125–134 kHz	13.56 MHz	856 MHz to 960 MHz
(LF)	(HF)	(UHF)
Range: Up to 10 cm	Range: Up to 30 cm	Range: Up to 100 m

RFID CAN BE EITHER...

ACTIVE
- Own power source
- Broadcast range up to 100 meters
- Ideal for material location

...or PASSIVE
- No power source
- Powered by a reader
- Read range from near contact up to 25 meters

POPULAR USES:

- Asset Tracking
- Race Timing
- Inventory Management
- Tool Tracking
- Access Control
- Attendee Tracking

- Operate at the same frequency (13.56 MHz) as HF RFID readers and tags
- May act as both a reader and a tag
- Devices must be in close proximity due to the short read range limitations of its radio frequency (usually no more than a few centimeters)

POPULAR USES:

INFORMATION SHARING
Transferring info between smartphones by tapping two devices together

CONTACTLESS PAYMENT
Credit cards, debit cards, key fobs and other devices use NFC to make secure payments

"There are 150 million NFC devices now. By 2014, there will be 300 MILLION."

Reed Peterson, Head of Business & Market Development for the GSMA

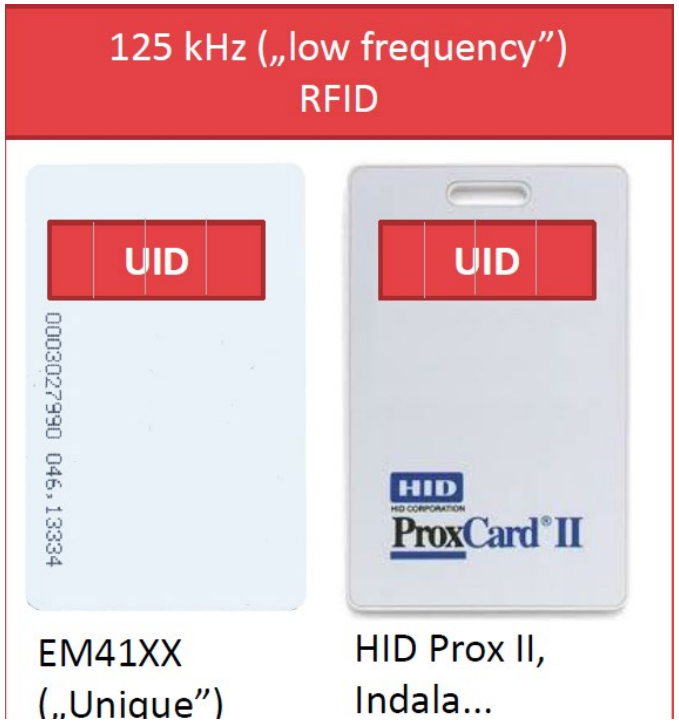
SMART POSTERS
Using an NFC-enabled smartphone, viewers can access exclusive content

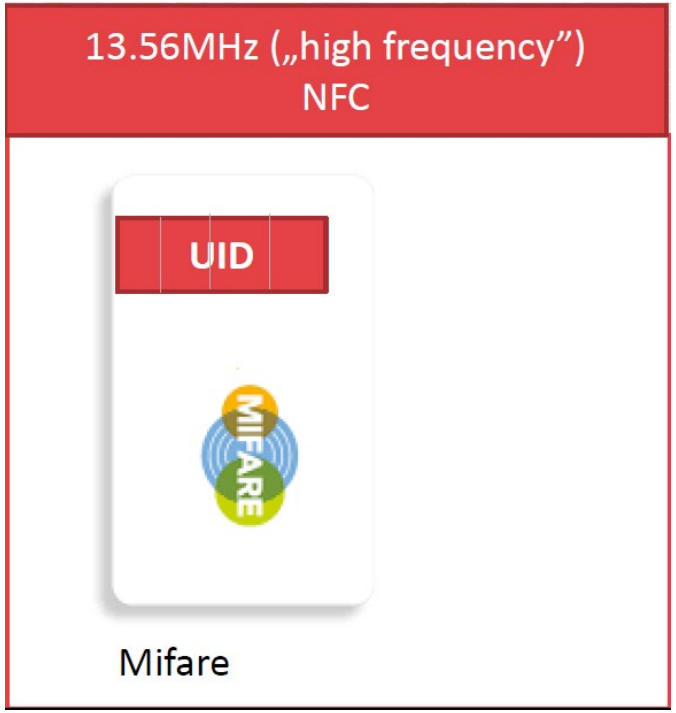
NINE OF THE TOP TEN

HANDSET MAKERS HAVE NFC-ENABLED DEVICES AND BOTH ANDROID & WINDOWS PHONES SUPPORT THE TECHNOLOGY

Are these cards secure?

- RFID
- NFC

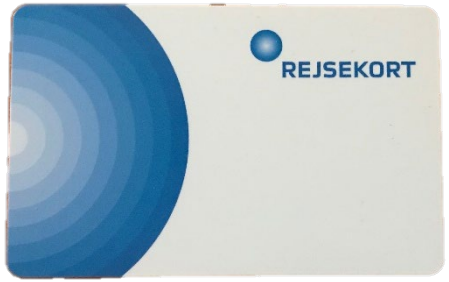




Are these cards secure?

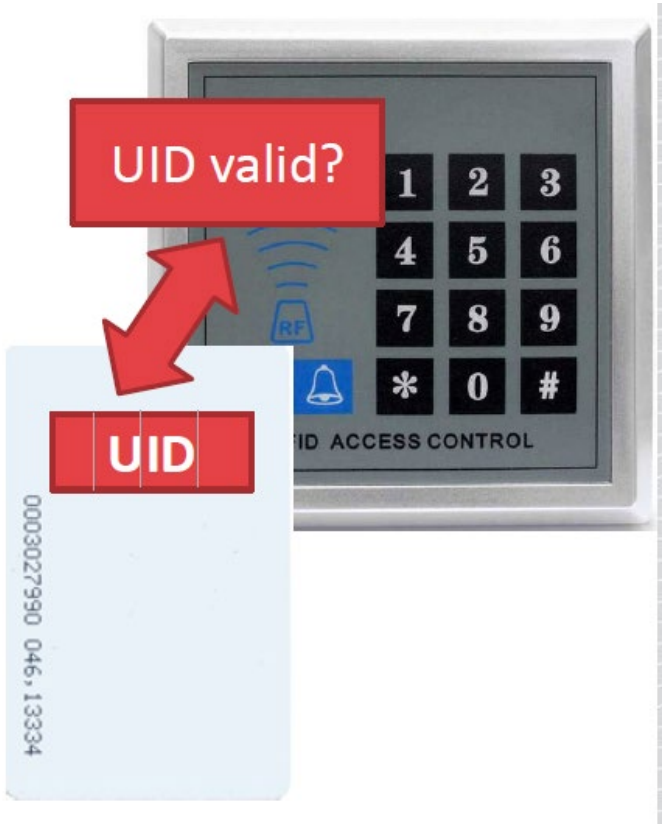
- Quick answer is: **it depends**
  - –Different cards implement different protocols
  - –Example your bank card (secure) vs the DTU student card (not really)

- The majority of cards that is used as a simple authentication mechanism are problematic
  - –Usually a MIFARE classic card



Simplest cards' security

- Store a "unique" id
  - –Called: CSN (Card Serial Number) or UID (Unique IDentifier)
  - –3-10 bytes
  - –Read-only
  - –Anyone can read it
  - –Reader checks for registered CSN/UID



UID/CSN “security”

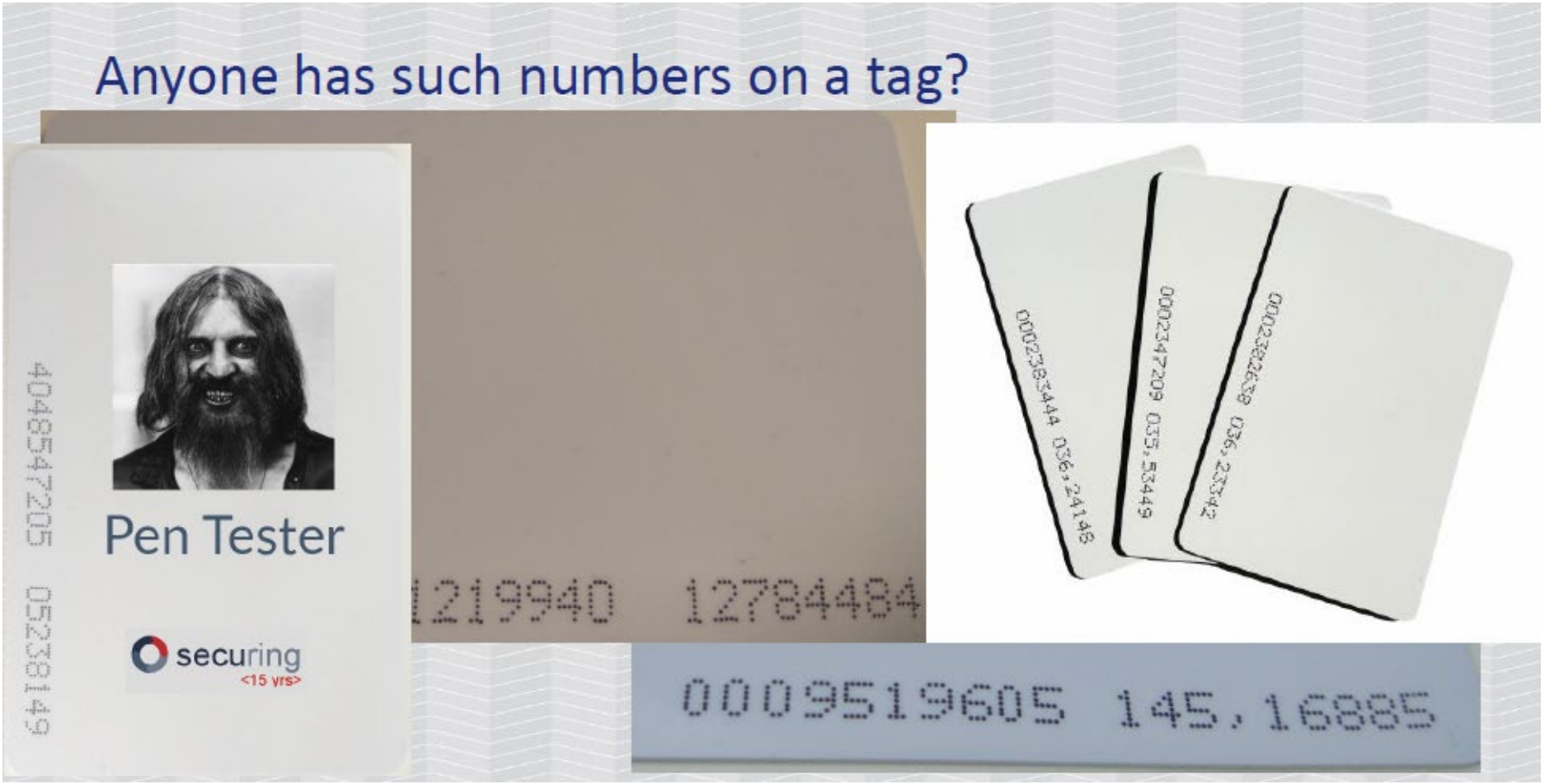
- Value set in factory
- Cannot be altered
- Only vendor knows how to make a tag

- Do you see any problem with this?

Not really secure

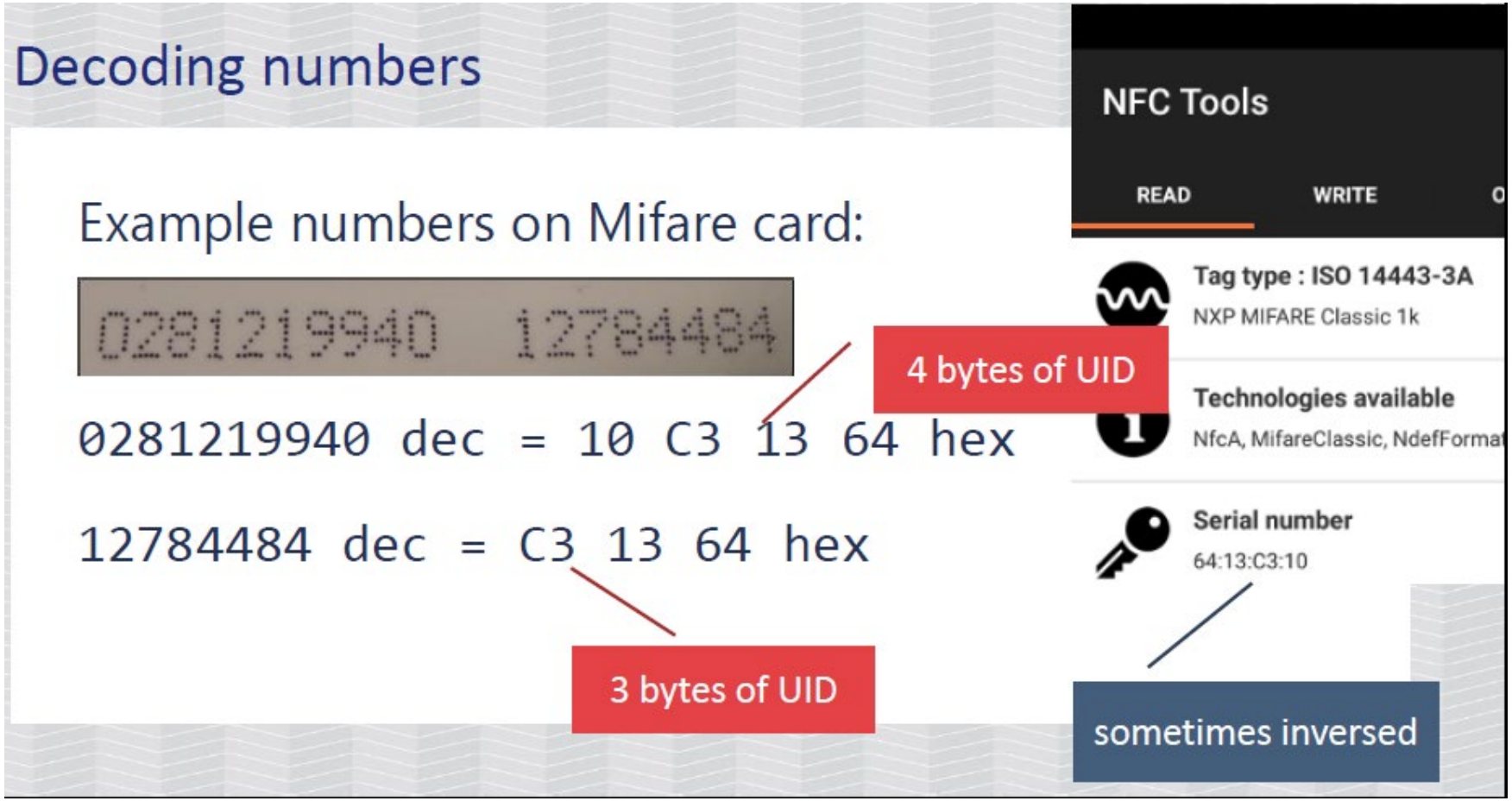
- Anyone who is able to read the card can duplicate it

You can also hack them by simply taking a photo



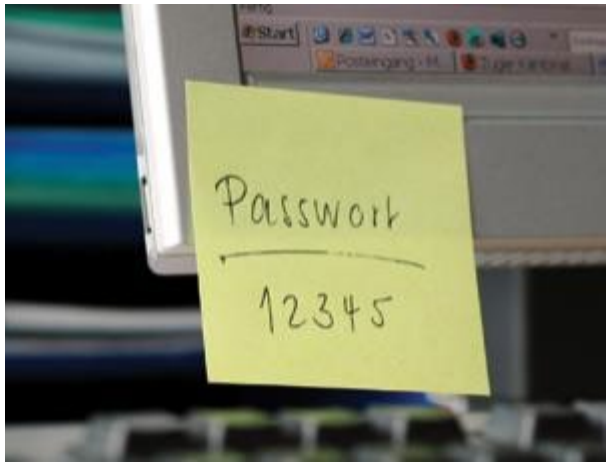
You can also hack them by simply taking a photo

Dec to hex


Decoding numbers
Example numbers on Mifare card:
0281219940 12784484
0281219940 dec = 10 C3 13 64 hex
12784484 dec = C3 13 64 hex
4 bytes of UID
3 bytes of UID
NFC Tools
READ
WRITE
Tag type : ISO 14443-3A
NXP MIFARE Classic 1k
Technologies available
Serial number
64:13:C3:10
sometimes inversed

Btw humans are always the weak link

- At least we use a pin on top of our NFC cards!



Btw humans are always the weak link

- Social engineer attacks…

MIFARE

- MIFARE is a trademark which covers a number of different contactless cards
  - **proprietary** protocols

- MIFARE **Classic**
  - Employs a proprietary protocol compliant to parts 1–3 of ISO/IEC 14443 Type A, with an NXP proprietary security protocol for authentication and ciphering
- MIFARE **Plus**
  - Drop-in replacement for MIFARE Classic with certified security level (AES-128 based) and is fully backwards compatible with MIFARE Classic.
- MIFARE **Ultralight**
  - Low-cost ICs that are useful for high volume applications such as public transport, loyalty cards and event ticketing
- MIFARE **DESFire**
  - Contactless ICs that comply to parts 3 and 4 of ISO/IEC 14443-4 Type A with a mask-ROM operating system from NXP. The DES in the name refers to the use of a DES, two-key 3DES, three-key 3DES and AES encryption; while Fire is an acronym for Fast, innovative, reliable, and enhanced

MIFARE

- Some of the types provide enhanced security (especially when a chip exists on card)

- Examples
  - DTU, and many other companies use: MIFARE Classic 1K
  - Rejsekort: MIFARE Classic 4K
  - (Danish) banks: MIFARE Plus

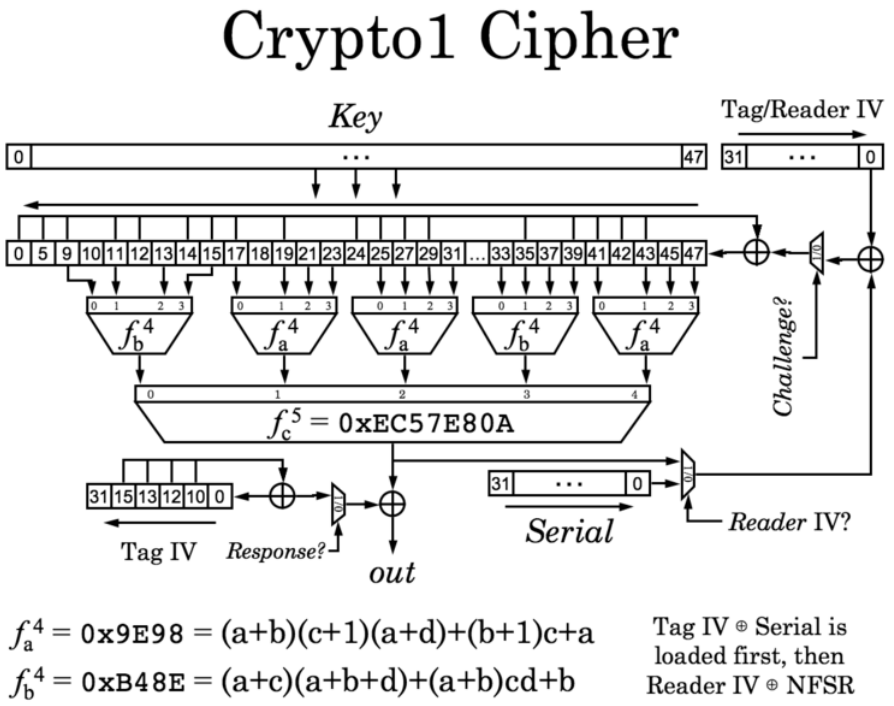
Use case: MIFARE Classic 1K

- Memory storage device
  - Divided into segments and blocks with simple security mechanisms for access control
  - Used heavily as it is cheap

- **1,024 bytes** of data storage, split in to **16 sectors**
  - Each sector protected by **two keys A** and **B**

Can MIFARE Classic be attacked?

- Attack = clone
- Yes, but not trivially (not just a simple scan as with previous attack examples)
- Keys A and B are needed
- Attacks (there are different ones) exploit vulnerabilities on the **proprietary** CRYPTO1 algorithm



Can MIFARE Classic be attacked?

- Attack = clone
- Yes, but not trivially (not just a simple scan as with previous attack examples)
- Keys A and B are needed
- Doable in a few minutes or hours

Outline

- **Introduction**
- **Wireless threats**
- **WIFI security**
  - –Open Wi-Fi
  - –Obscurity
  - –WEP/WPA
  - –WPA2
  - –WPA3
- **Intro to NFC/RFID security**
- **Conclusion**
- **Lab exercises**