



Wireless Security 101

- Introduction to wireless security -

Ruxandra F. Olimid

University of Bucharest, Romania and NTNU - Norwegian University of Science and Technology
(ruxandra.olimid@fmi.unibuc.ro)

Seminar at University Rey Juan Carlos
Madrid – November, 19th 2019

Questions to answer

1. *Where do we need/use wireless security?*
2. *Why makes wireless security special?*
3. *What can go wrong with wireless security?*
4. *How can we improve wireless security?*

Where do we need/use wireless security?



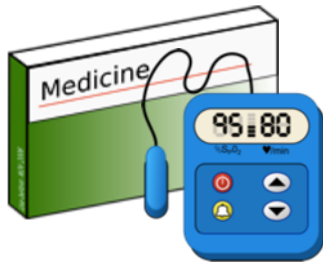
home



business



transport



healthcare



telecommunications

Things are getting "smart" 😊

Use-case: Spain

Spain

Spain has a competitive and well-developed telecommunication market, with high penetration rates for fixed and mobile services. The telecommunication market has undergone a process of mergers and acquisitions in recent years, leading to a concentration of almost 80 per cent of the revenues in three transnational operators: Telefonica, Vodafone and Orange (CNMC, 2016). The market experienced some changes as MasMovil, a former MVNO, bought MNO Yoigo and other operators, and thus became the new fourth national convergent player.

Mobile services: Spain is home to Telefonica, the incumbent operator and one of the largest telecommunication companies, with operations throughout the globe. Competition was first introduced in 1994, when a second licence was granted to a consortium led by Airtel (now Vodafone). A third operator started to provide services in 1999 and its licence was bought by France Telecom (now Orange) in 2005. The following year, a fourth mobile network operator – Yoigo (now MásMóvil) – launched services, further increasing the level of competition in

Key indicators for Spain (2017)	Europe	World
Fixed-telephone sub. per 100 inhab.	42.5	35.8 13.0
Mobile-cellular sub. per 100 inhab.	113.2	120.4 103.6
Active mobile-broadband sub. per 100 inhab.	95.5	85.9 61.9
3G coverage (% of population)	99.6	98.3 87.9
LTE/WiMAX coverage (% of population)	97.0	89.6 76.3
Individuals using the Internet (%)	84.6	77.2 48.6
Households with a computer (%)	78.4	78.6 47.1
Households with Internet access (%)	83.5	80.6 54.7
International bandwidth per Internet user (kbit/s)	27.0	117.5 76.6
Fixed-broadband sub. per 100 inhab.	31.2	30.4 13.6
Fixed-broadband sub. by speed tiers, % distribution		
<256 kbit/s to 2 Mbit/s	0.3	0.6 4.2
>2 to 10 Mbit/s	5.3	12.4 13.2
=equal to or above 10 Mbit/s	94.4	87.0 82.6

Note: Data in italics are ITU estimates. Source: ITU (as of June 2018).

and 1998, respectively, the market opened to competition. At present, Telefónica, Vodafone and Orange compete in the fixed-line market with MásMóvil and regional facilities-based cable operators. All of them are deploying NGA networks, mostly based on FTTH technology.

Government policy: The Government is taking a market-based approach to ICT development and aims to put in place the best conditions for

What makes wireless security special?

Direct access to the medium

(e.g., sniffing, jamming)



Dynamicity / mobility

(e.g., new / old members, handover)



Restricted devices

(e.g., low comp. power, battery life)

What makes wireless security special?

*“GSM should be as secure as the wired network (PSTN) ...
...but, security mechanisms should not have a negative impact on the
usability of the system”*



Trade-off between security and efficiency

What can go wrong with wireless security?



SMART HOUSE – ENGLISH VERSION – REMA 1000

[Source: <https://www.youtube.com/watch?v=nwPtcqcqz00&t=2s>]

But... is this a *wireless security* problem?



The adversary...

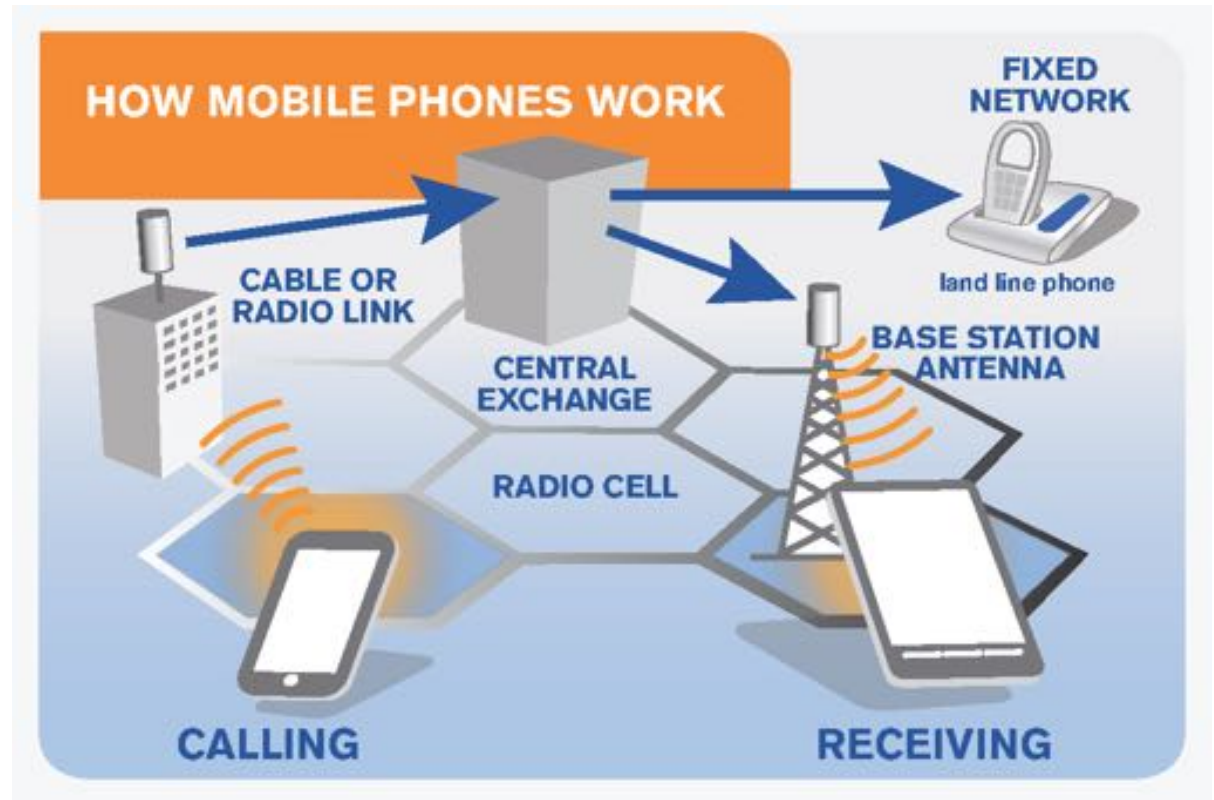
- Acts intentionally, aims to harm the system in some way ...

Adversaries can be:

- *Passive*: can only listen / eavesdrop (sniffing)
- *Active*: can actively interfere, send / stop / modify messages, etc.

Use-case: mobile networks

- User Equipment (UE) / Mobile Station (MS)
- Access Network
- Core Network



[Source: <http://emfguide.itu.int/emfguide.html>]

Use-case: mobile networks

Adversaries can be:

- *Passive*: can sniff the radio communication
- *Semi-passive*: can sniff the radio communication and can trigger active actions that are legitimate for a user (e.g., send messages, initiate calls, etc.)
- *Active*: can set and operate rogue base stations (active IMSI Catchers)



What can go wrong with wireless security?



home



business



transport



healthcare



telecommunications

What can go wrong with wireless security?

How is your home AP configured?



1. With default admin user name and password 😊

D-Link Blog Home
Helps you to solve D-Link network problems.

Categories

- ASUS Products (14)
- D-Link Apps (20)
- D-Link Camera (95)
- D-Link News (75)
- D-Link Reviews (40)
- D-Link Router (255)
- D-Link Storage (21)
- D-Link Switch (67)
- D-Link Videos (7)
- D-Link Wireless (140)
- Drivers and firmware (30)
- Knowledgebase (43)
- Others (151)

Recent Posts

- How do I configure D-Link DSR Series router for a Static IP Internet Connection?
- Why can't I see my D-Link camera video in D-View Cam?
- How do I install my D-Link DSL...

Home

Feb 10

D-Link wireless AP default IP address, default username and password

D-Link Wireless [Add comments](#)

Access Point	IP Address	Default Username	Default Password
DWL-700AP	192.168.0.50	admin	blank
DWL-810	192.168.0.30	admin	blank
DWL-800AP+	192.168.0.30	admin	blank
DWL-900AP	192.168.0.20	N/A	public
DWL-900AP+	192.168.0.50	admin	blank
DWL-1700AP	192.168.0.50.2000	admin	root
DWL-1750	192.168.0.50.2000	admin	root
DWL-2000AP	192.168.0.50	admin	blank
DWL-2100AP	192.168.0.50	admin	blank
DWL-2200AP	192.168.0.50	admin	blank
DWL-2210AP	192.168.0.50	admin	admin

AD

Hot Tags

- mydlink
- D-Link
- Reviews
- Firmware
- camera
- wireless router
- Access Point
- D-Link Router
- DIR-655
- Firewall
- router
- Cloud Router
- ShareCenter
- IP address
- storage
- DNS-320
- DI-624
- Wi-Fi
- DCS-825L
- Baku Camera

[Source: <http://www.dlink.cc/d-link-wireless/d-link-wireless-ap-default-ip-address.html>]

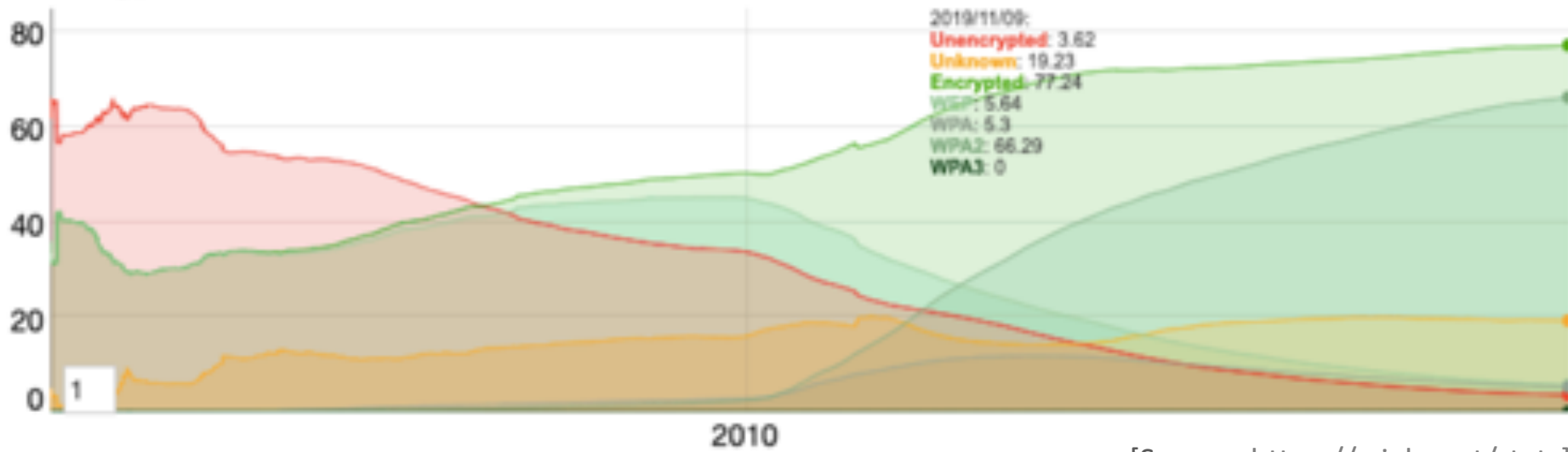
What can go wrong with wireless security?

How is your home AP configured?




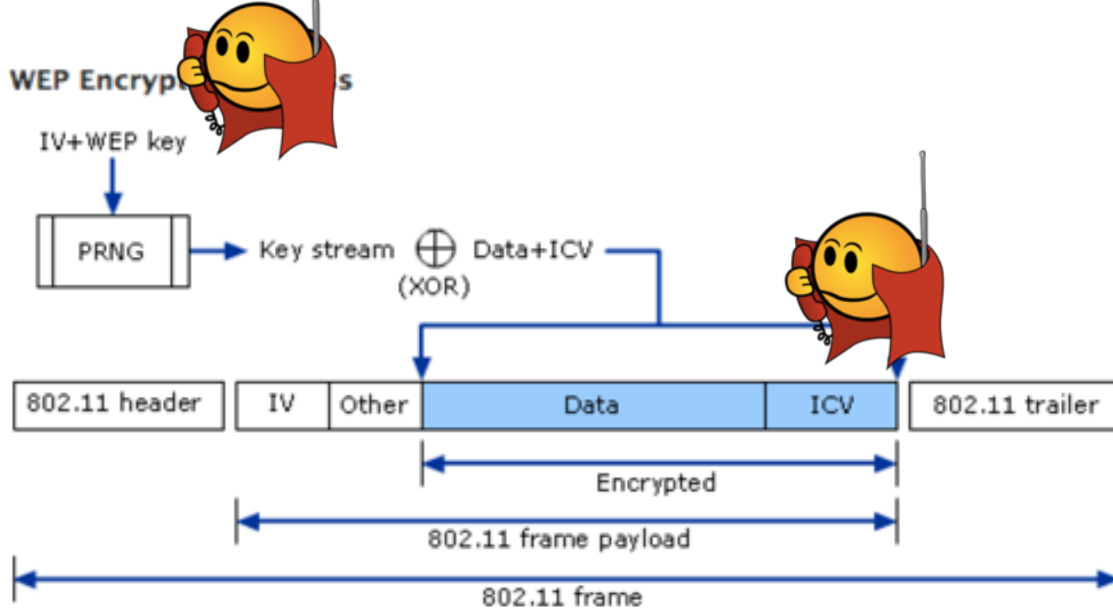
2. Uses WEP (Wired Equivalence Privacy) 😊

WiFi Encryption Over Time



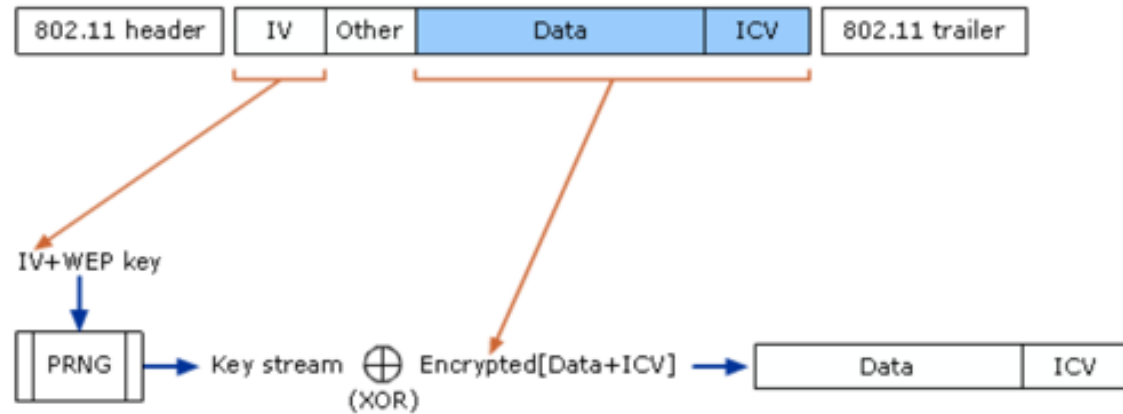
[Source: <https://wile.net/stats>]

Use-case: WEP



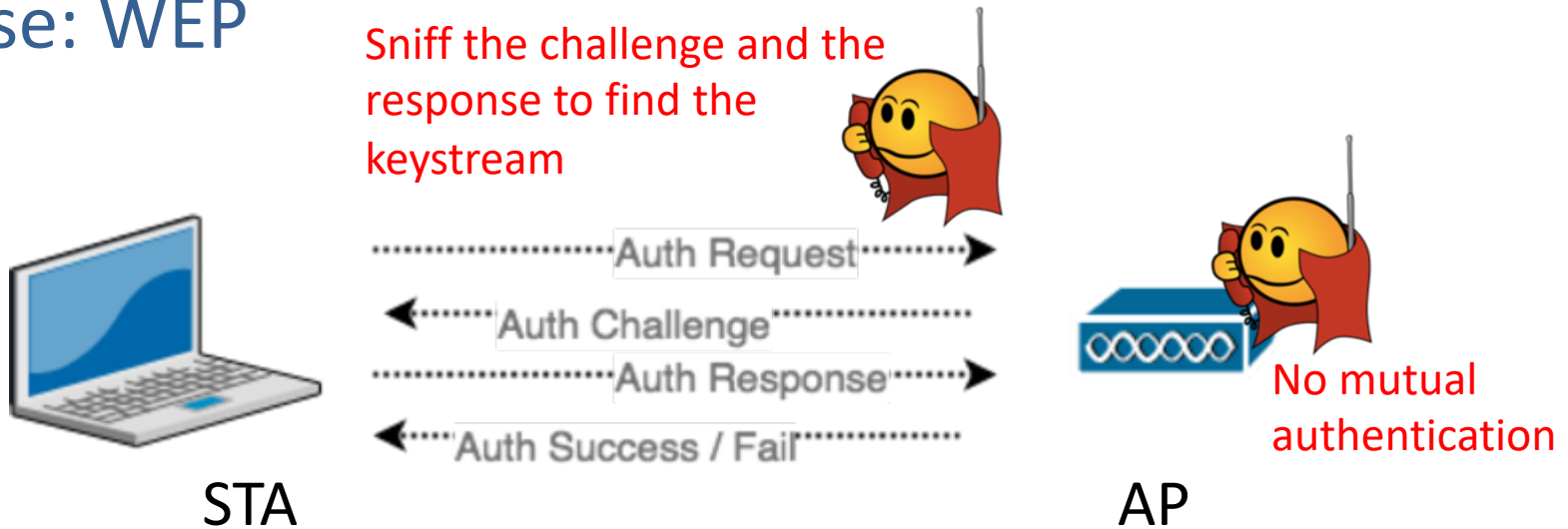
IV: Initialization Vector (24 bits)
PRNG: Pseudo-Random
Number Generator
ICV: Integrity Check Value

WEP Decryption Process



[Source: [https://technet.microsoft.com/pt-pt/library/cc757419\(v=ws.10\).aspx](https://technet.microsoft.com/pt-pt/library/cc757419(v=ws.10).aspx)]

Use-case: WEP



- **Auth Challenge:**
 - AP sends a (random) 128-bit challenge text
- **Auth Response:**
 - STA encrypts the challenge text with the secret key using WEP and sends the ciphertext to the AP
- **Auth Success:**
 - AP decrypts and compares the plaintext with the challenge; if it equals the challenge text, authentication succeeds

What can go wrong with wireless security?

How is your home AP configured?

3. Uses a weak password 😊



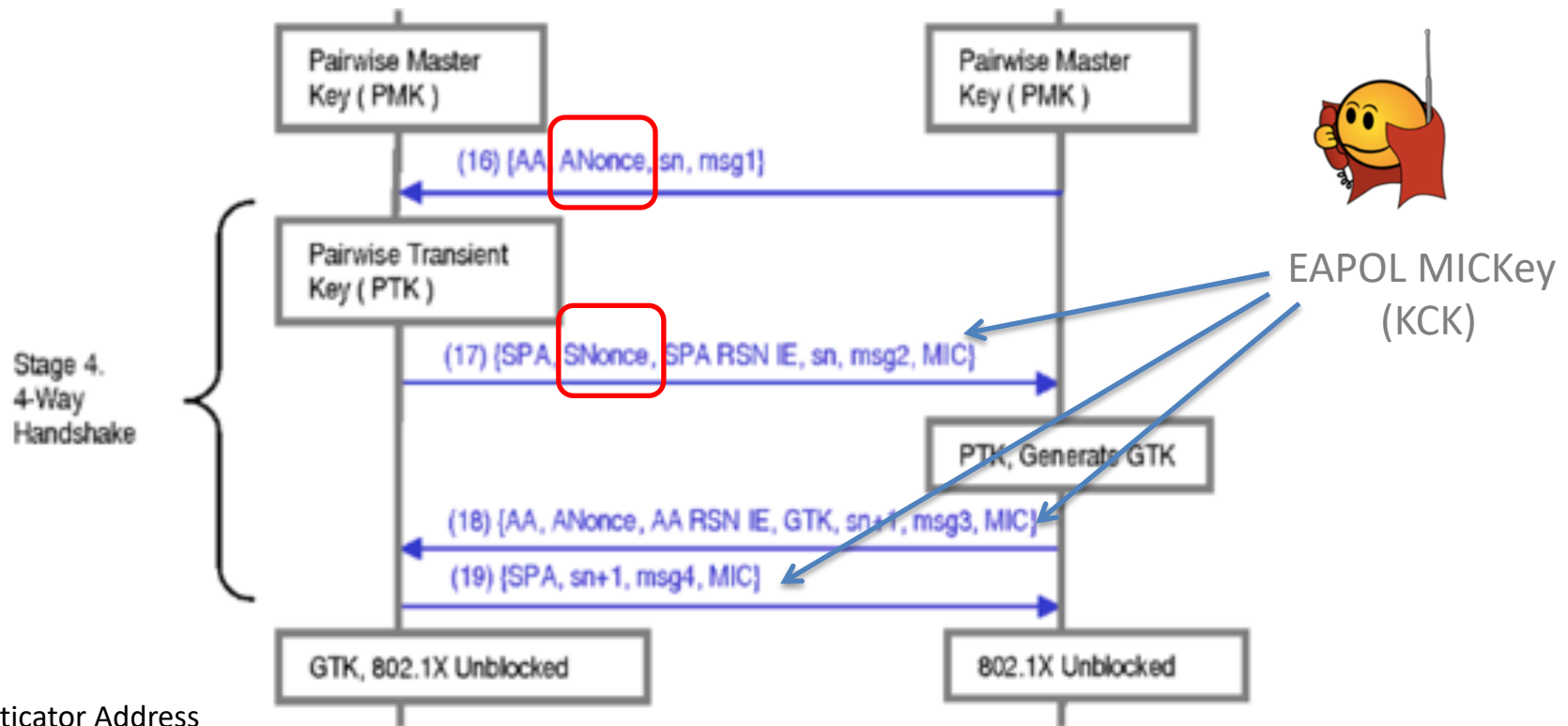
The screenshot shows the AirCrack-NG website. The top left has the logo and a navigation menu with links: Home, Forum, Wiki, GitHub, Blog, IRC. Below that is a 'Documentation' section with links: Getting started, Installation, Compatibility, Screenshots, In movies, Main Docs. A 'Misc' section contains links: Support, Resources, Contribute, Contact, License, Code of Conduct.

The main content area is divided into two columns. The left column is titled 'Download' and features a large green arrow pointing down to a CD icon. Below the icon are links for 'AirCrack-ng 1.5.2' (with sub-links for Sources and Windows) and 'Changelog'. A 'More downloads...' link is also present.

The right column is titled 'Description' and contains the following text:
AirCrack-ng is a complete suite of tools to assess WiFi network security.
It focuses on different areas of WiFi security:
• Monitoring: Packet capture and export of data to text files for further processing by third party tools
• Attacking: Replay attacks, deauthentication, fake access points and others via packet injection
• Testing: Checking WiFi cards and driver capabilities (capture and injection)
• Cracking: WEP and WPA PSK (WPA 1 and 2)
All tools are command line which allows for heavy scripting. A lot of GUIs have taken advantage of this feature. It works primarily Linux but also Windows, OS X, FreeBSD, OpenBSD, NetBSD, as well as Solaris and even eComStation 2.

Below the description are two sections: 'Fresh news' with a sub-section 'AirCrack-ng 1.5.2' dated 09 Dec 18, and 'Under the spotlights' with a sub-section 'Injection, -1 channel and other capture issues'. The 'Fresh news' section contains a paragraph about the release of version 1.5.2.

Use-case: WPA 4-way handshake protocol

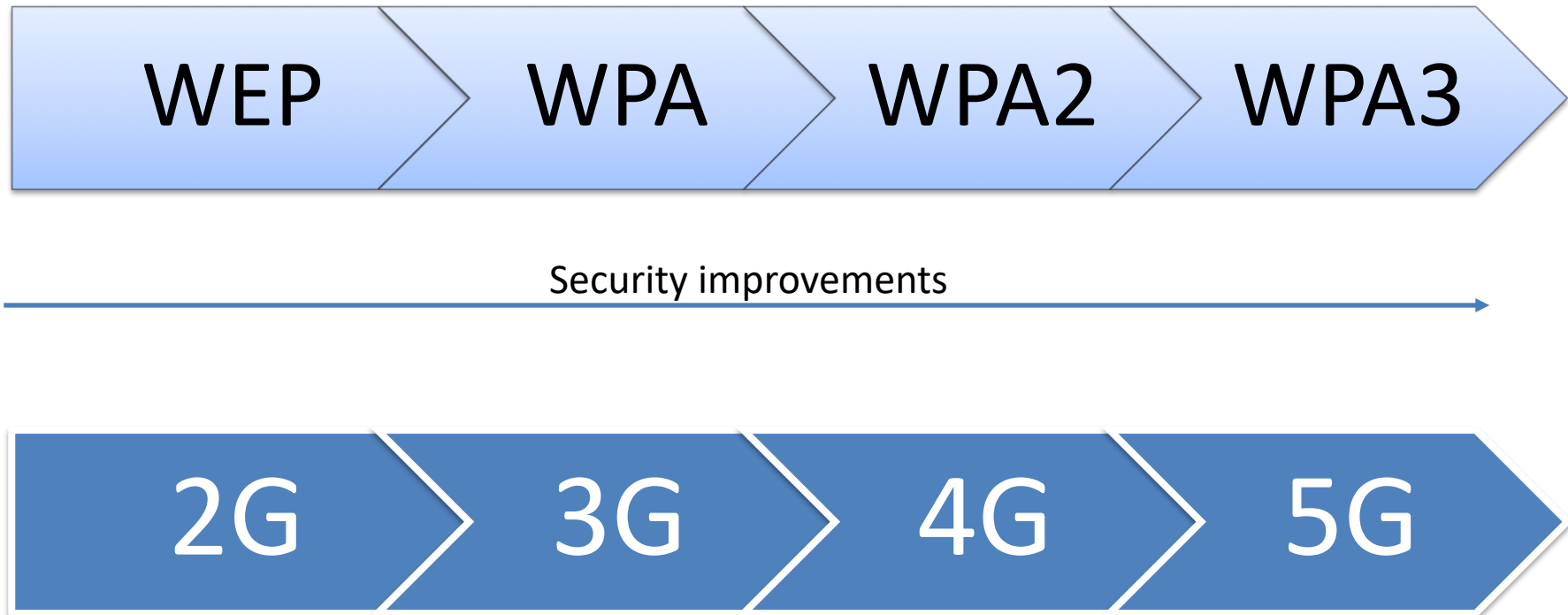


AA: Authenticator Address
SA: Supplicant Address
ANonce: nonce generated by the Authenticator (AP)
SNonce: nonce generated by the Supplicant (STA)
sn: sequence number

Encrypted data communication follows

[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i
<https://theory.stanford.edu/~jcm/papers/NDSS05.pdf>]

Security improvements



Breaking is easy! Securing is hard!



Key Reinstallation Attacks

Breaking WPA2 by forcing nonce reuse

Discovered by [Mathy Vanhoef](#) of [imec-DistriNet](#), [KU Leuven](#)

[INTRO](#)

[DEMO](#)

[DETAILS](#)

[PAPER](#)

[TOOLS](#)

[Q&A](#)

INTRODUCTION

We discovered serious weaknesses in WPA2, a protocol that secures all modern protected Wi-Fi networks. An attacker within range of a victim can exploit these weaknesses using **key reinstallation attacks** (KRACKs). Concretely, attackers can use this novel attack technique to read information that was previously assumed to be safely encrypted. This can be abused to steal sensitive information such as credit card numbers, passwords, chat messages, emails, photos, and so on. **The attack works against all modern protected Wi-Fi networks.** Depending on the network configuration, it is also possible to inject and manipulate data. For example, an attacker might be able to inject ransomware or other malware into websites.

[Source: <https://www.krackattacks.com/>]



DRAGONBLOOD

Analysing WPA3's Dragonfly Handshake

By [Mathy Vanhoef](#) (NYUAD) and [Eyal Ronen](#) (Tel Aviv University & KU Leuven)

[INTRO](#)

[NEW](#)

[DETAILS](#)

[PAPER](#)

[TOOLS](#)

[Q&A](#)

INTRODUCTION

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.

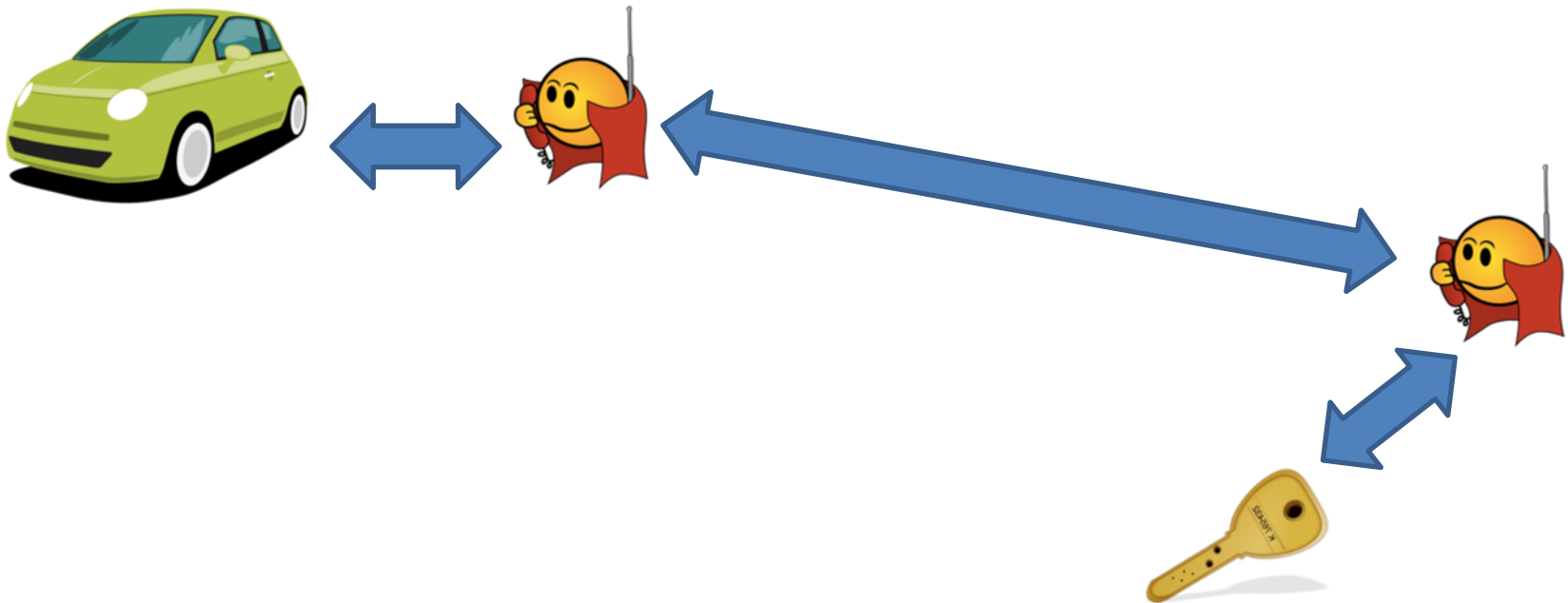
[Source: <https://wpa3.mathyvanhoef.com/>]

What can go wrong with wireless security?



Do you keep your vehicle key fob safe?

Relay attack



Do not confuse with replay attacks or Men-in-the-Middle (MitM) attacks!

What can go wrong with wireless security?



[Source: <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>]

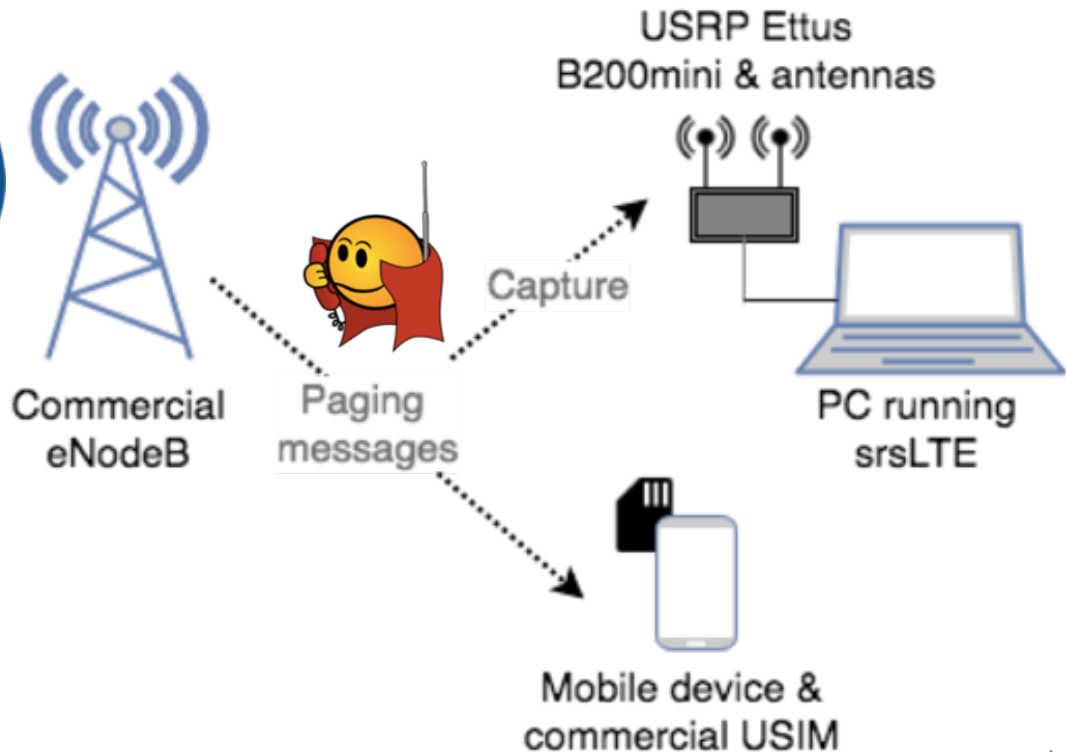
What can go wrong with wireless security?



Do you use a smartphone?



Listen to paging messages



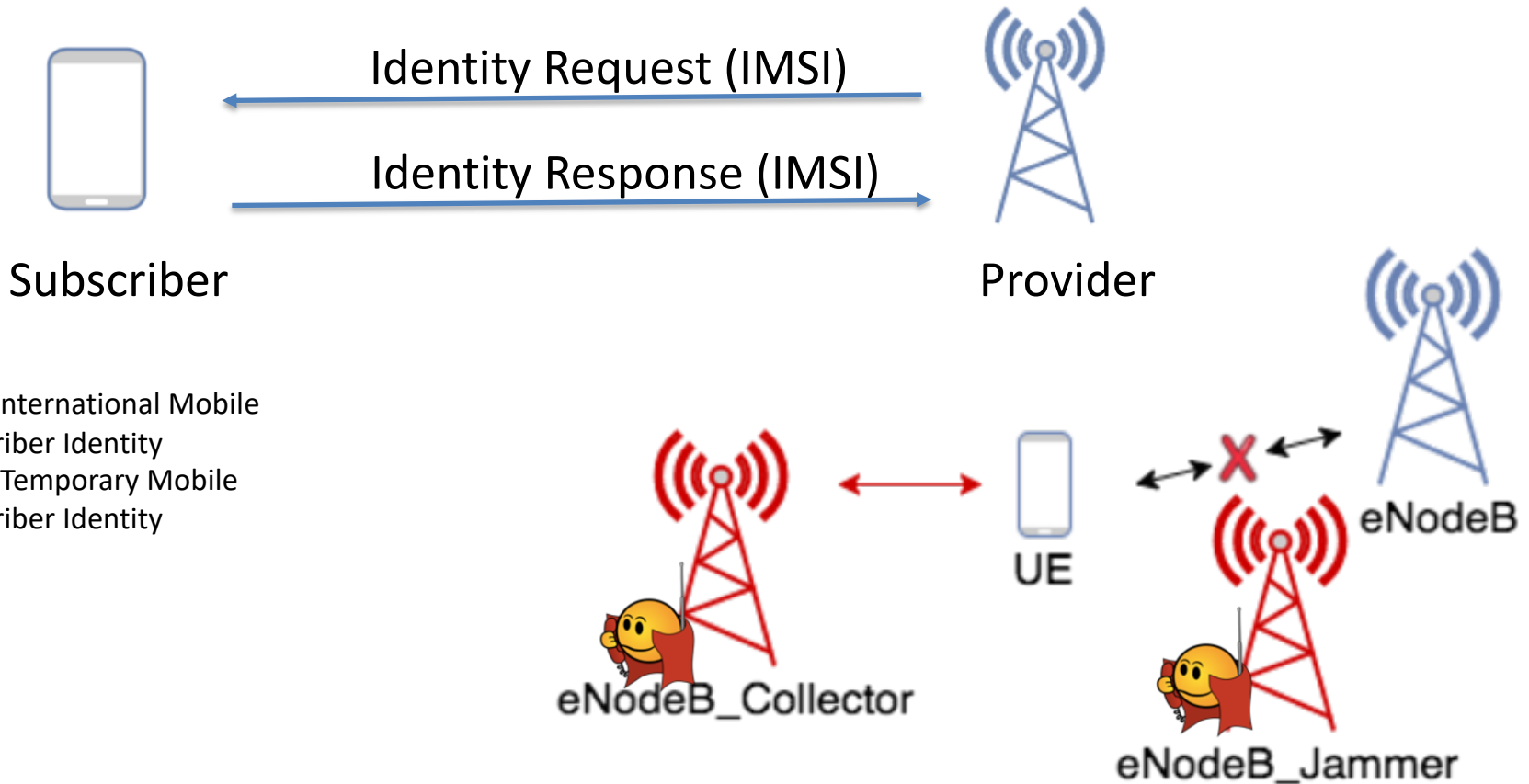


What can go wrong with wireless security?

```
<PCCH-Message>
  <message>
    <cl>
      <paging>
        <pagingRecordList>
          <PagingRecord>
            <ue-Identity>
              <s-TMSI>
                <mmecc>00111000</mmecc>
                <m-TMSI>11010000001111110111001110010000</m-TMSI>
              </s-TMSI>
            </ue-Identity>
            <cn-Domain>
              <ps/>
            </cn-Domain>
          </PagingRecord>
        </pagingRecordList>
      </paging>
    </cl>
  </message>
</PCCH-Message>
```

```
7 bytes decoded.
*** DECODING SUCCESSFUL ***
```

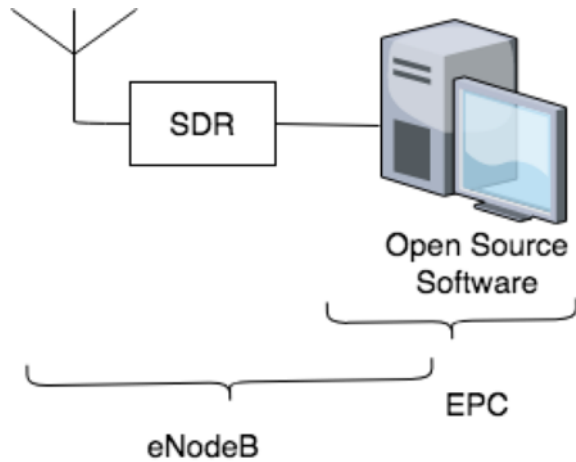
What can go wrong with wireless security?



IMSI: International Mobile
Subscriber Identity
TMSI: Temporary Mobile
Subscriber Identity



What can go wrong with wireless security?

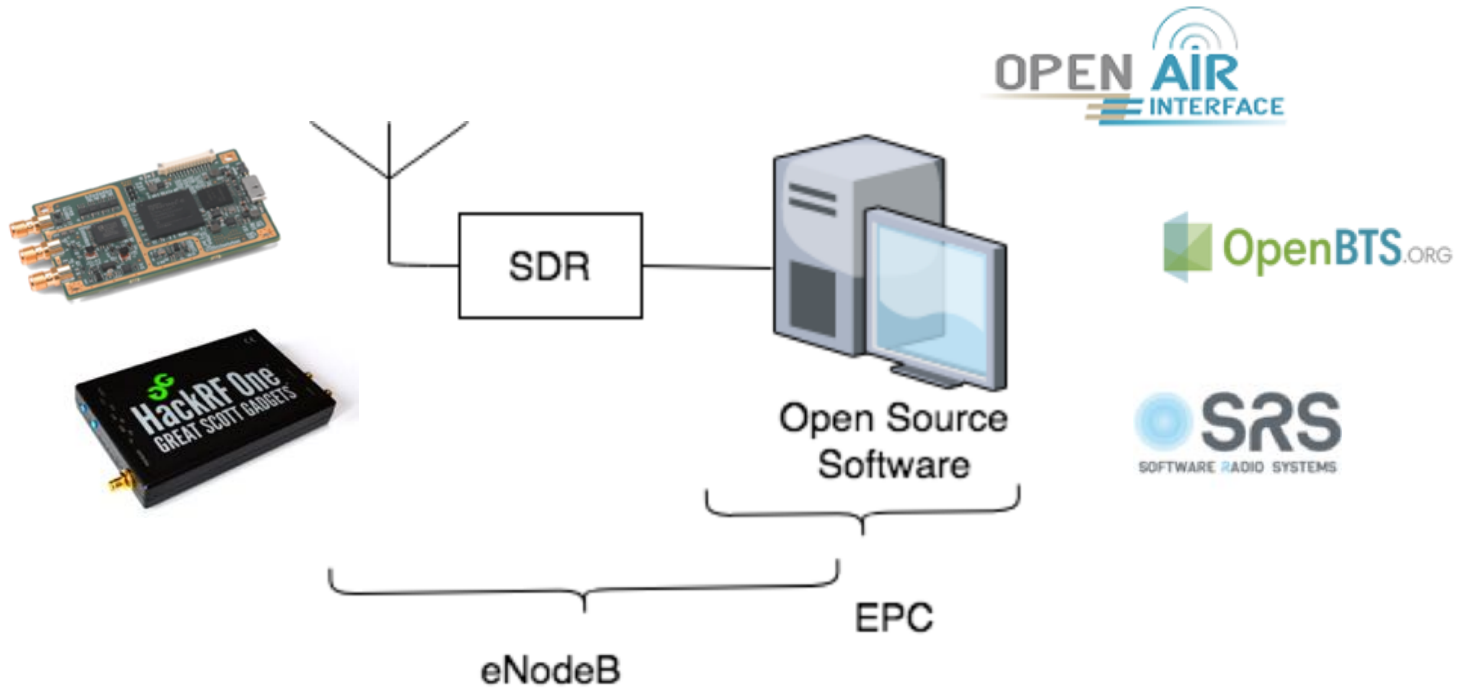


SDR: Software Defined Radio

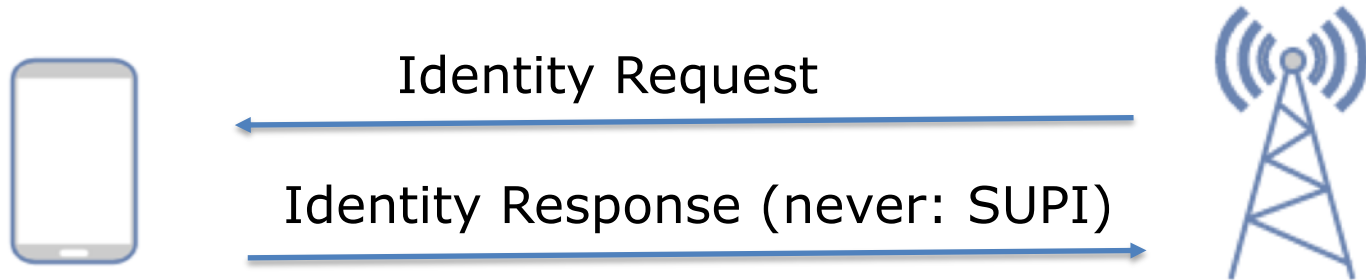
```
200 id-InitialUEMessage, Attach request, PDN connectivity request
110 SACK id-downlinkNASTransport, Identity request
146 SACK id-uplinkNASTransport, Identity response
110 SACK id-downlinkNASTransport, Attach reject
182 id-InitialUEMessage, Tracking area update request
110 SACK id-downlinkNASTransport, Tracking area update reject
94 id-downlinkNASTransport, EMM status
214 id-InitialUEMessage, Attach request, PDN connectivity request
```

```
NAS-PDU: 17f49d7386090756082924505902830303
  Non-Access-Stratum (NAS)PDU
    0001 .... = Security header type: Integrity protected (1)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    Message authentication code: 0xf49d7386
    Sequence number: 9
    0000 .... = Security header type: Plain NAS message, not security protected (0)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    NAS EPS Mobility Management Message Type: Identity response (0x56)
    Mobile identity - IMSI [REDACTED]
```

What can go wrong with wireless security?



Use-case: 5G



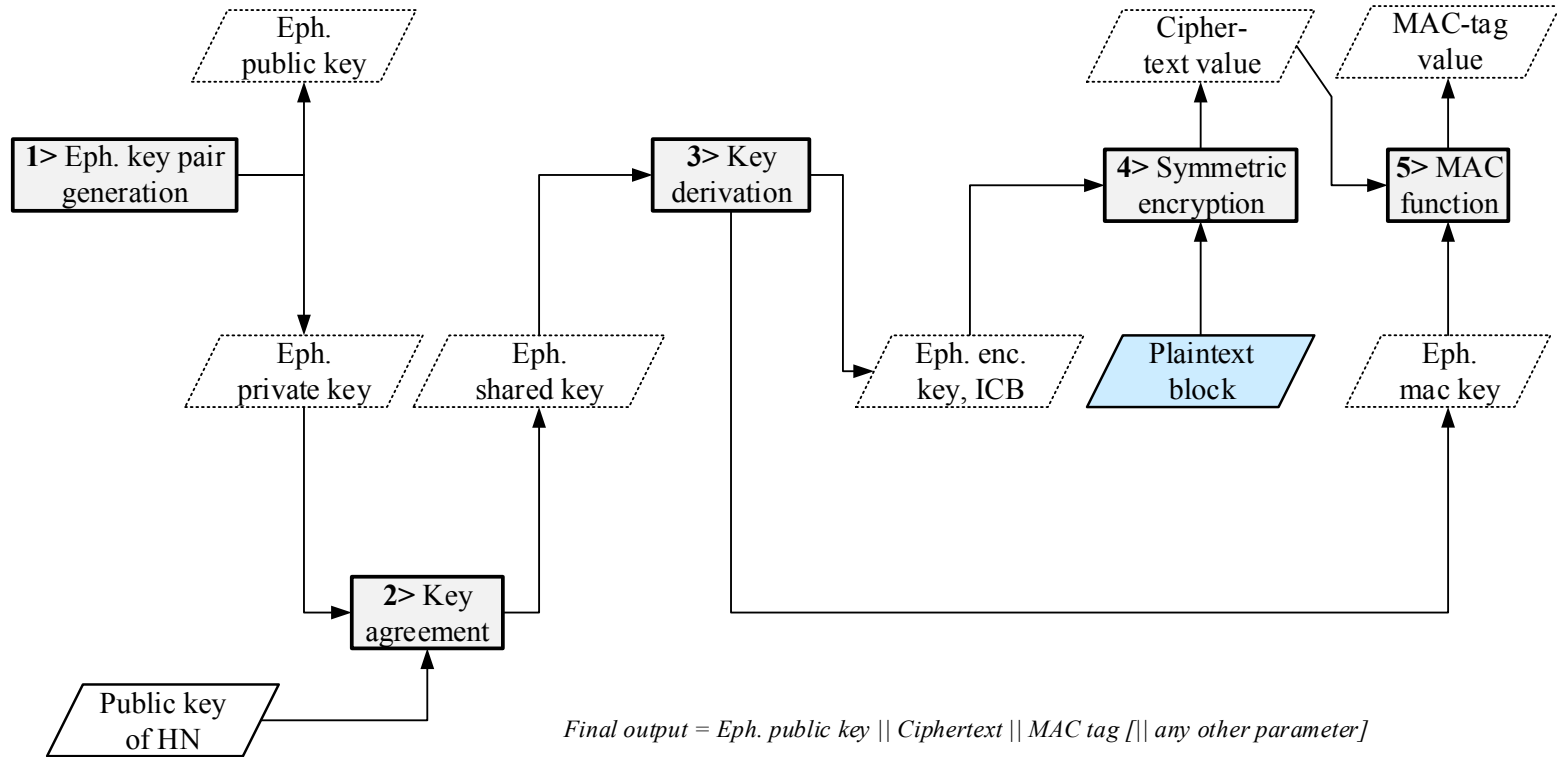
“In response to the Identifier Request message, the UE never sends the SUPI.”

[Source: ETSI TS 133 501 V15.2.0 (2018-09)]

SUPI: Subscription Permanent Identifier



Use-case: 5G



[Source: ETSI TS 133 501 V15.2.0 (2018-09)]

Evolution in time...



Security improvements

Increased technical capabilities for the large public



Easy to make the phone
accept a fake tower...

But difficult to get the
tools for it

More difficult to make
the phone accept a fake
tower...

But easy to obtain the
necessary tools

How can we improve wireless security?



Think to the future

(e.g., longer keys, quantum-resistant algorithms)

Make protocols public
(Kerckhoffs's principle)



Secure usage

(e.g., increase awareness, secure your devices, try not to use deprecated technologies)



Build better protocols

(e.g., mutual authentication, confidentiality, privacy, integrity)

Usage of temporary identities / contextual keys
(e.g., TMSI, key hierarchy -> freshness + separation)



Thank you!



Q&A

