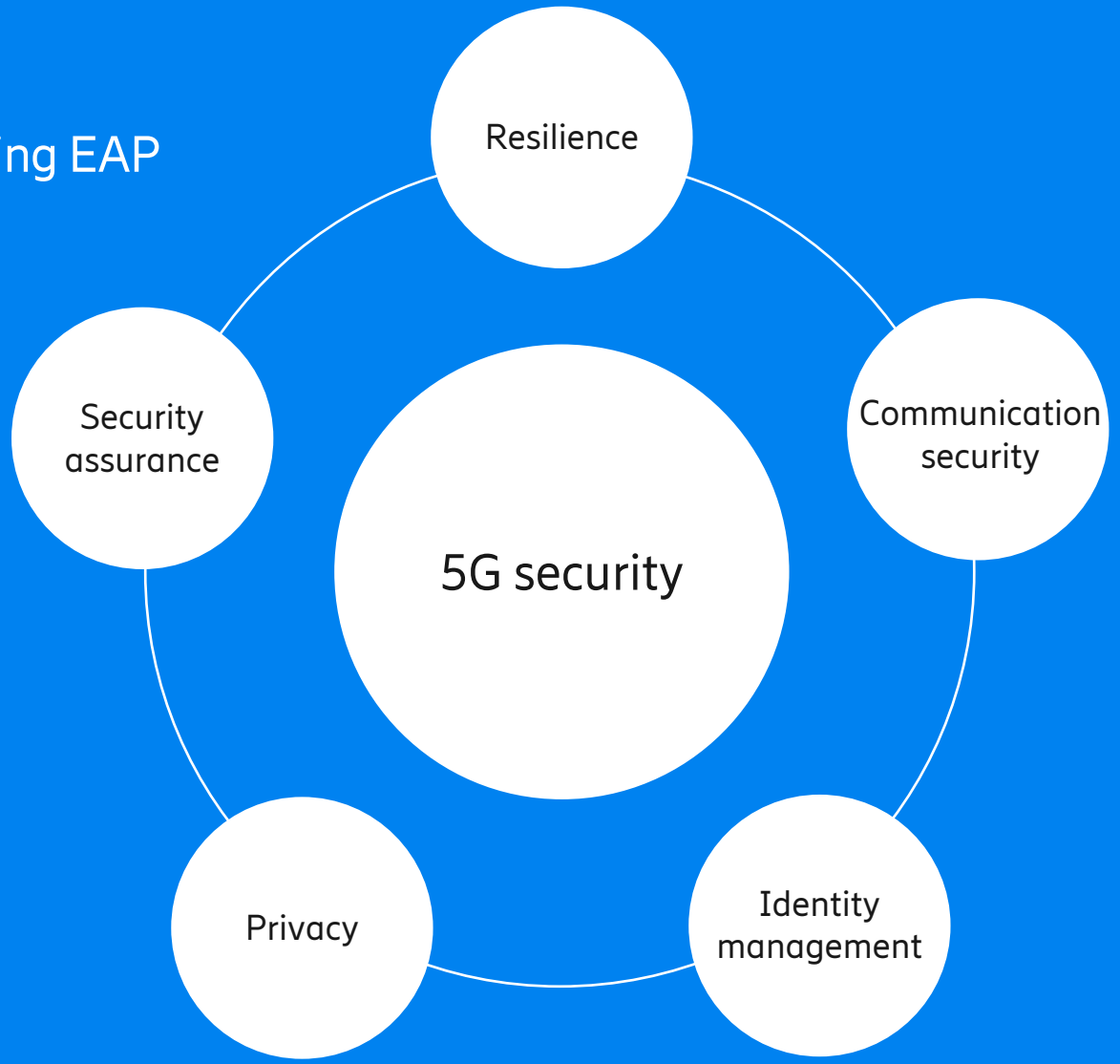

5G Security
TELEPHONE
87

Ericsson's 5G Security Goals

5G security is an evolution of 4G security. Some goals:

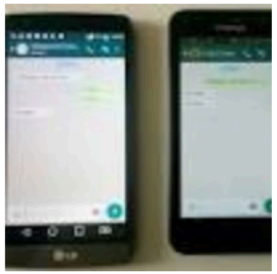
- New flexible and strong authentication framework using EAP
- Zero trust architecture inside and between networks
- Separation of network functions and signalling
- Encryption and integrity protection of all traffic in both signalling and user plane
- Prevent tracking and identification of users



Zero Trust Architecture Inside and Between Networks

Attacks on Interconnect Security

Your phone number is all a hacker needs to read texts, listen ...
The Guardian - 18 Apr 2016
Weaknesses within **mobile** phone network **interconnection** system allows ... When calls or text messages are made across networks **SS7** ...



SS7 Attack Circumvents WhatsApp and Telegram Encryption
Softpedia News - 11 May 2016
... a new attack that uses the **SS7** mobile **telecommunications** protocol that allows attackers to ... 7 (**SS7**) protocol is a standard developed in 1975 that allows telco operators to **interconnect** fixed line and/or mobile telephone networks. ... Their demonstration proved that **surveillance** agencies don't ...

Newer **Diameter** Telephony Protocol Just As Vulnerable As **SS7**
BleepingComputer - 2 Jul 2018
Newer **Diameter** Telephony Protocol Just As Vulnerable As **SS7** .... for providing security testing and **monitoring** of mobile networks, urges 4G ...

Service Based Architecture (SBA) and Interconnect Security (N32)

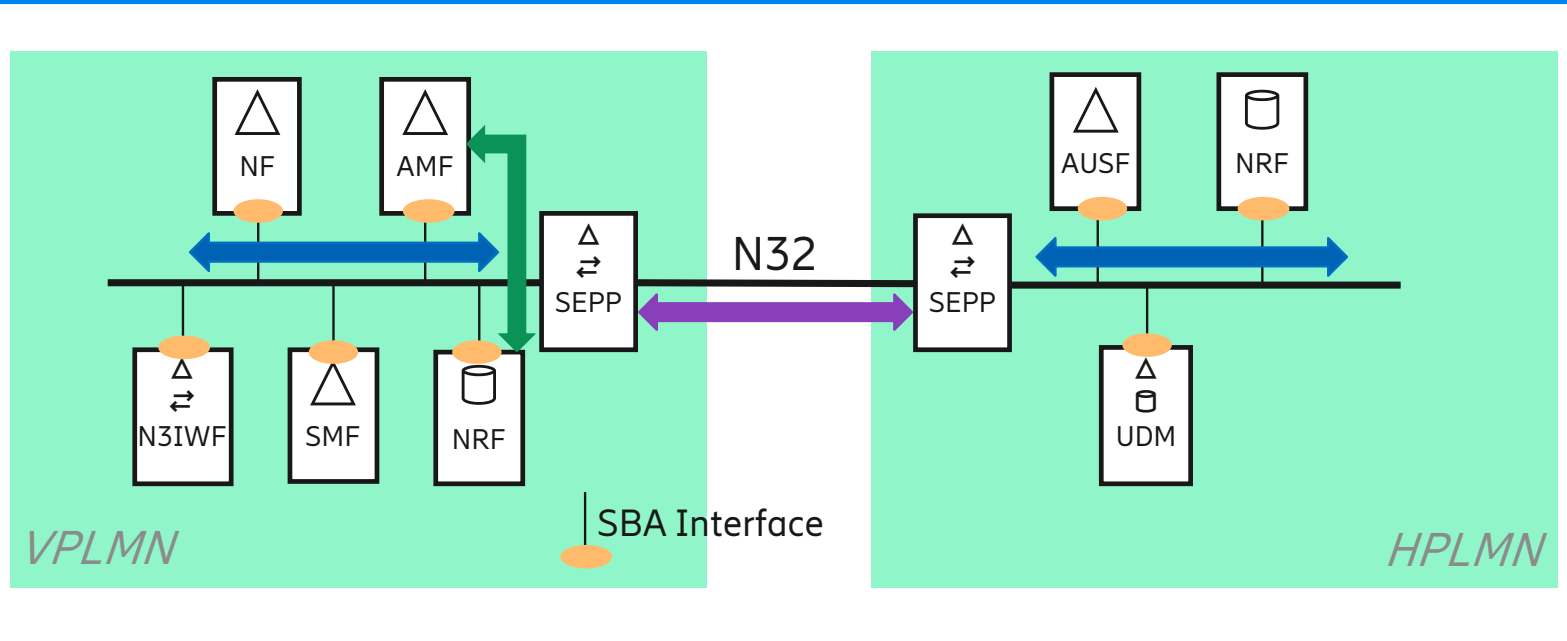
- Zero Trust Architecture: SBA and N32 security for communication inside and between core networks. Takes threats from legacy interconnect networks into account from the start.
- Interconnect Provider gets information on a need-to-know basis. Modifications made during interconnect are logged and signed.

TLS 1.3

TLS 1.3 with mutual authentication is mandatory to support for all Network Functions.

OAuth2.0 is mandatory to support for access authorization in SBA.

JSON Object Signing and Encryption (JOSE) are used for N32 application layer security.



Battle Against IMSI catchers

Attacks from IMSI Catchers or False Base Stations

Tracking devices hidden in London's recycling bins are ...
Wired.co.uk - 9 Aug 2013
Tracking devices hidden in London's recycling bins are stalking your ... unique MAC address of **their smartphones** recorded by Renew **London**.

No, this isn't **a** scene from Minority Report. This trash can is ...
Ars Technica - 9 Aug 2013

Spying Cell Towers May Be Spread Across **US**
Tom's Guide - 3 Sep 2014
Also known as "**IMSI catchers**," they're used by law enforcement in many ... "A lot of these interceptors are right on top of **U.S. military bases**," Goldsmith told ...

Phone Firewall Identifies Rogue Cell Towers Trying to ...
In-Depth - Wired - 3 Sep 2014

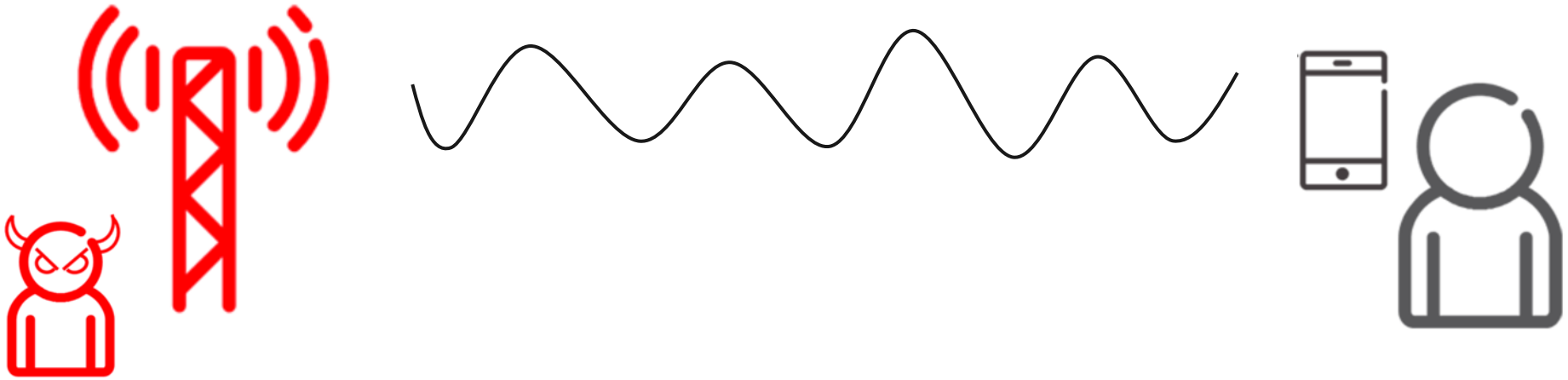
"StingRay" surveillance devices found near the **White House**
Yahoo News - 12 Sep 2019
Israel's leader is denying a report claiming his government planted surveillance devices around Washington, D.C., including near the **White House**. The devices ...

Attacks from IMSI Catchers or False Base Stations

— False base station are also known as Stingrays, IMSI catchers, Cell site simulators, Man-in-the-middle base station, Rogue base stations, etc.

— **False base stations able to mimic all functions** on a network was mitigated already in 3G with network authentication. US operators have completely shut down 2G, but most phones will still attach to a false 2G base station. These types of false base stations will try to get devices to connect to them and then stay for as long as possible.

— **Simpler false base stations** just asks devices to send their long-term identifier IMSI. This can aid the attacker to identify and track users. This is mitigated in 5G.



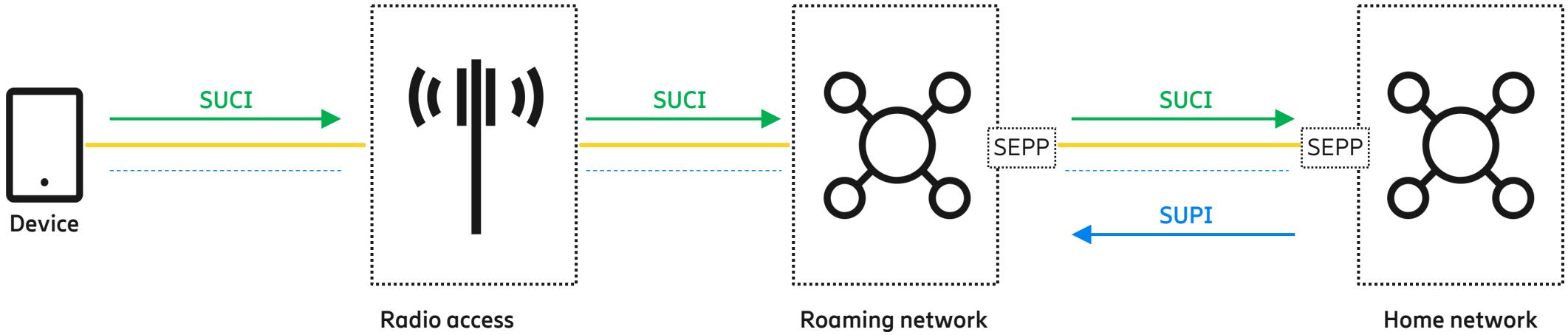
5G: An End to the Battle Against False Base Stations?

Many mitigations against false base stations are part of the 5G standard.

- Encryption of permanent identifier
- Strict refreshment of temporary identifier
- Decoupling of permanent identifier from the paging mechanism
- Integrity protection of user plane traffic
- Secure radio redirections
- False base station detection

Most important is encryption of permanent identifiers. With this enabled, the permanent identifier is never sent in clear over the air.

- Encryption is done using a public key stored on the device. Uses state-of-the-art cryptography like Curve25519.
- In 5G, the long-term identity is called SUPI. SUPI is often an IMSI. An encrypted SUPI is called SUCI.



Limiting Impact from Compromised Long-term Keys with PFS and Diffie-Hellman

Limiting Impact from Compromised Long-term Keys

Report: **Spies Stole** SIM Encryption **Keys**
BankInfoSecurity.com - 21 Feb 2015
A British-American intelligence team hacked into Gemalto, the world's largest maker of SIM cards, resulting in the theft of numerous encryption **keys** for the cards ...

How American and British **spies** hacked the world's largest ...
Quartz - 20 Feb 2015

The NSA Has the Master **Key to** Unlock Your Phone's Messages
Gizmodo - 19 Feb 2015

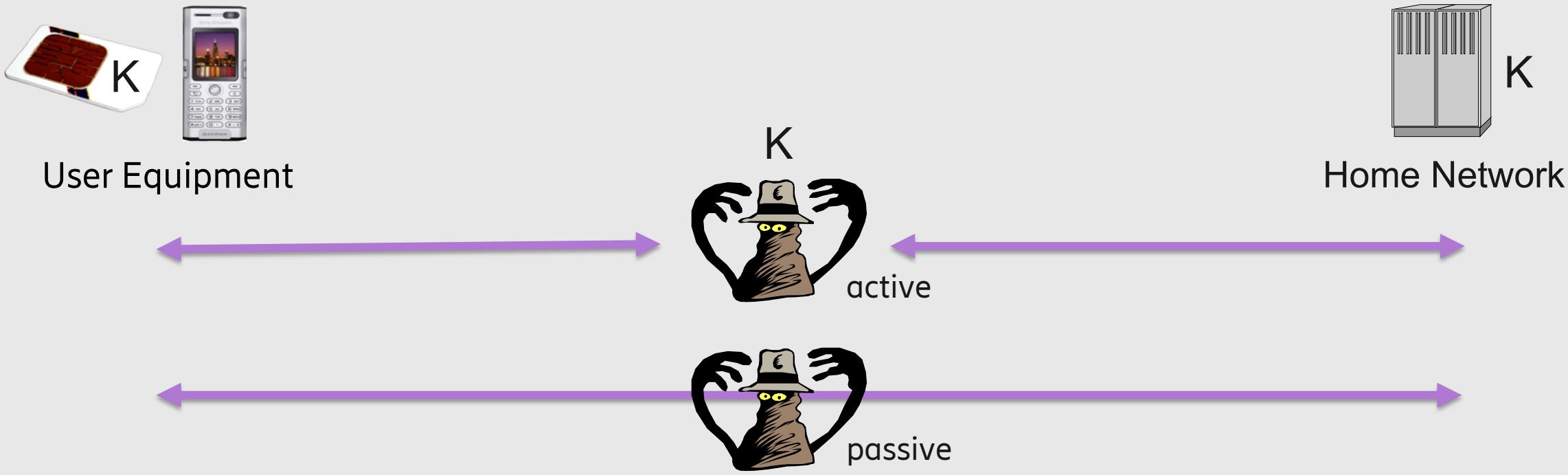
Sim card database hack gave US and UK **spies** access to ...
In-Depth - The Guardian - 20 Feb 2015

Questions About the Alleged Gemalto Hack
Blog - Wall Street Journal (blog) - 20 Feb 2015

Mobile phones hacked: can the NSA and GCHQ listen to all ...
In-Depth - The Guardian - 20 Feb 2015

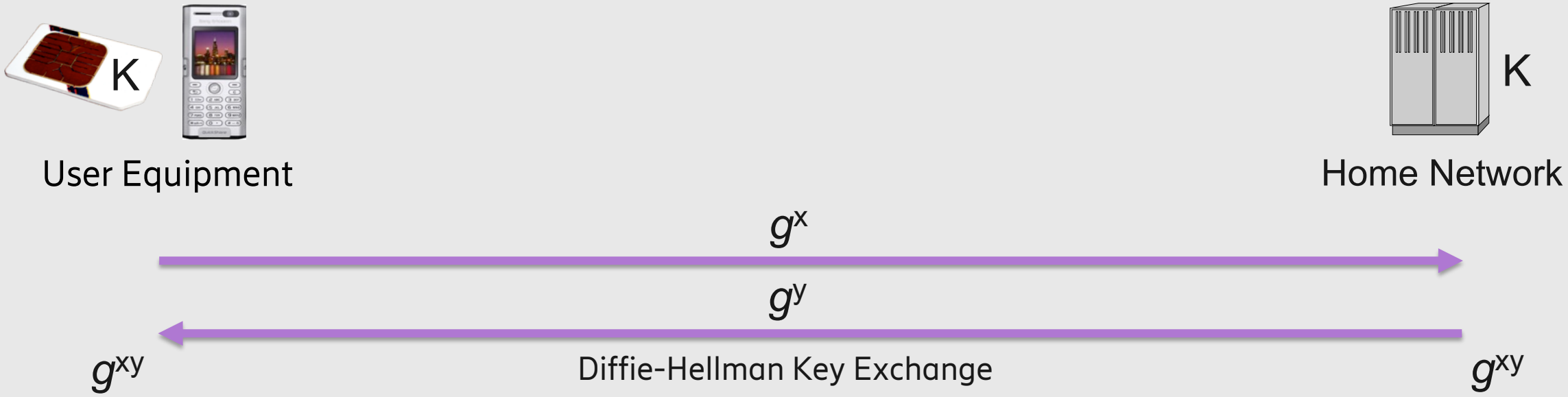
Heartbleed Used to **Steal Private Keys** from OpenVPN
Threatpost - 18 Apr 2014
Worse, researchers have been able to chain together exploits to **steal private keys** from traffic moving through the open source virtual private network software ...

What Can an Attacker Do with Long-term Keys?



- An **active attacker** can authenticate as UE or Network.
  - Hard to do on large scale, relatively expensive, high risk of being detected.
- A **passive attacker** can eavesdrop on information sent over the air.
  - Easier to do on large scale, relatively inexpensive, small risk of being detected.
  - Attack can be done on communication recorded in the past.

What is PFS and Diffie-Hellman and How Do They Help?



- With Perfect Forward Secrecy (PFS), compromise of long-term keys does not lead to compromise of past session keys. Often achieved with Ephemeral Diffie-Hellman which also mitigates future passive attacks.
- Many older security protocols do not have PFS. In 5G, EAP authentication can be used for all types of access. Private 5G networks can use **EAP-TLS**. Ongoing work in IETF and 3GPP to define **EAP-AKA with PFS**. This effectively mitigates pervasive monitoring.
- For SBA and N32, 5G core networks support TLS 1.3 which always use Ephemeral Diffie-Hellman.

References

5G security:

- https://www.ericsson.com/en/white-papers/5g-security---enabling-a-trustworthy-5g-system
- https://www.ericsson.com/en/blog/2019/7/3gpp-5g-security-overview
- https://www.ericsson.com/en/security/a-guide-to-5g-network-security

5G privacy:

- https://www.ericsson.com/en/white-papers/privacy-in-mobile-networks
- https://www.ericsson.com/en/blog/2019/2/privacy-mobile-networks

5G and mitigation of false base stations:

- https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3539
- https://www.ericsson.com/en/blog/2017/6/protecting-5g-against-imsi-catchers
- https://www.ericsson.com/en/blog/2018/6/detecting-false-base-stations-in-mobile-networks
- https://www.ericsson.com/en/blog/2019/1/3gpp-release15
- https://www.ericsson.com/en/blog/2019/5/fighting-imsi-catchers-5g-cellular-paging-privacy

5G authentication with PFS and Diffie-Hellman:

- https://tools.ietf.org/html/draft-ietf-emu-aka-pfs
- https://tools.ietf.org/html/draft-ietf-emu-eap-tls13