Adventures in hardware standardization

Amelia Andersdotter

amelia.andersdotter@dataskydd.net

10 augusti 2019

ARTICLE 19

Table of contents

1. Good news
   - Best practice for identifiers
   - Beginning work on privacy policies
2. Bad news
   - Politics
   - Conflicts
3. So what can we do?
   - How to absorb good technical developments
   - How to block bad technical developments

Kranzberg, M.

"Technology is neither good nor bad; nor is it neutral."

ARTICLE19's work...

- Technical design matters.

ARTICLE19's work...

- Technical design matters.
- Introduce diversity in design process.

ARTICLE19's work...

- Technical design matters.
- Introduce diversity in design process.
- Work in IETF, IEEE, 3GPP, ITU, ICANN, etc.

ARTICLE19's work...

- Technical design matters.
- Introduce diversity in design process.
- Work in IETF, IEEE, 3GPP, ITU, ICANN, etc.
- Human rights considerations
  - IETF RFC 8280
  - IEEE 802 Privacy Recommendations (still draft)

Words of caution

- Standards are not mandatory. They are voluntary.
- Developing standards takes time, money and commitment.
- The standards are written by those who show up but...
- ...their impact is determined by whether they are implemented.

Hardware

3GPP (mobile networks) and IEEE 802 (WLAN —> WiFi)

Pre-Association Services amendment .11aq Privacy Enhancements

☑ Randomize MAC address pre-association

Deeper overview:

`https://mentor.ieee.org/802.11/dcn/19/11-19-1027-01-0rcm-do-not-fear-random-macs.pptx`

Pre-Association Services amendment .11aq Privacy Enhancements

- ☑ Randomize MAC address pre-association
- ☑ Not probe for specific SSIDs

Deeper overview:

https://mentor.ieee.org/802.11/dcn/19/11-19-1027-01-0rcm-do-not-fear-random-macs.pptx

Pre-Association Services amendment .11aq Privacy Enhancements

- ☑ Randomize MAC address pre-association
- ☑ Not probe for specific SSIDs
- ☑ Reset the sequence number counter used to identify MSDUs and MMPDUs when the MAC address changes

Deeper overview:

https://mentor.ieee.org/802.11/dcn/19/11-19-1027-01-0rcm-do-not-fear-random-macs.pptx

Pre-Association Services amendment .11aq Privacy Enhancements

- ☑ Randomize MAC address pre-association
- ☑ Not probe for specific SSIDs
- ☑ Reset the sequence number counter used to identify MSDUs and MMPDUs when the MAC address changes
- ☑ Reseed the OFDM scrambler when MAC address changes

Deeper overview:

`https://mentor.ieee.org/802.11/dcn/19/11-19-1027-01-0rcm-do-not-fear-random-macs.pptx`

Pre-Association Services amendment .11aq Privacy Enhancements

- ☑ Randomize MAC address pre-association
- ☑ Not probe for specific SSIDs
- ☑ Reset the sequence number counter used to identify MSDUs and MMPDUs when the MAC address changes
- ☑ Reseed the OFDM scrambler when MAC address changes
- ☑ Choose random MAC address to associate to an AP and retain that MAC address during the connection to the ESS

Deeper overview:

`https://mentor.ieee.org/802.11/dcn/19/11-19-1027-01-0rcm-do-not-fear-random-macs.pptx`

ARTICLE 19

Pre-Association Services amendment .11aq Privacy Enhancements

- ☑ Randomize MAC address pre-association
- ☑ Not probe for specific SSIDs
- ☑ Reset the sequence number counter used to identify MSDUs and MMPDUs when the MAC address changes
- ☑ Reseed the OFDM scrambler when MAC address changes
- ☑ Choose random MAC address to associate to an AP and retain that MAC address during the connection to the ESS
- ☑ Set MAC address to a previously used (random) MAC address when attempting to use some state on the AP bound to the previous MAC address

Deeper overview:

`https://mentor.ieee.org/802.11/dcn/19/11-19-1027-01-0rcm-do-not-fear-random-macs.pptx`

Ongoing scalable geolocation work

☑ Passive ranging/passive geolocation (like GPS)

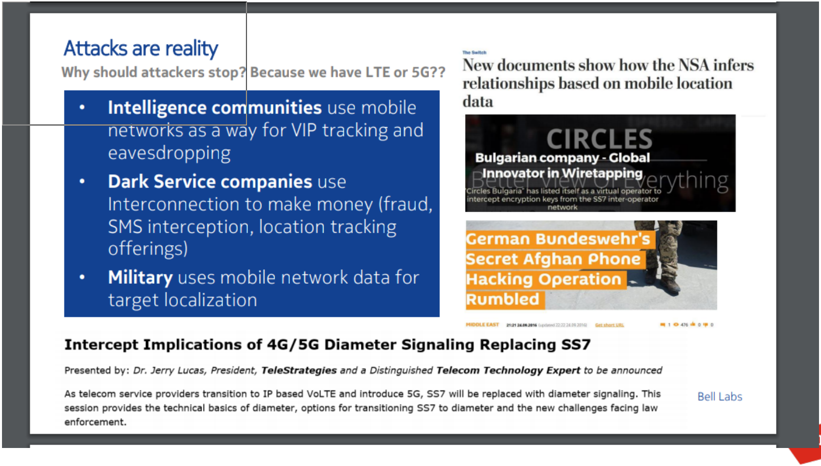
Ongoing scalable geolocation work

- ☑ Passive ranging/passive geolocation (like GPS)
- ☑ Bits in management frame to indicate privacy preference

Ongoing scalable geolocation work

- ☑ Passive ranging/passive geolocation (like GPS)
- ☑ Bits in management frame to indicate privacy preference
- ☑ Difference between “mechanism” and “policy” (will return to this)

S. Holtmanns, Nokia Bell Labs, ETSI Security Week 2018



Attacks are reality

Why should attackers stop? Because we have LTE or 5G??

- **Intelligence communities** use mobile networks as a way for VIP tracking and eavesdropping
- **Dark Service companies** use Interconnection to make money (fraud, SMS interception, location tracking offerings)
- **Military** uses mobile network data for target localization

The Switch

New documents show how the NSA infers relationships based on mobile location data

CIRCLES
Bulgarian company - Global Innovator in Wiretapping
Better View Of Everything
Circles Bulgaria' has listed itself as a virtual operator to intercept encryption keys from the SS7 inter-operator network

German Bundeswehr's Secret Afghan Phone Hacking Operation Rumbled

MIDDLE EAST 21:21 24.09.2016 (updated 22:22 24.09.2016) Get short URL 1 476 0 0

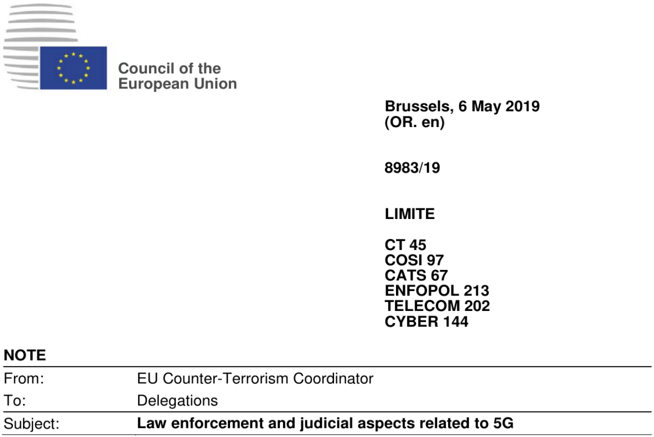
Intercept Implications of 4G/5G Diameter Signaling Replacing SS7

Presented by: *Dr. Jerry Lucas, President, **TeleStrategies** and a Distinguished **Telecom Technology Expert** to be announced*

As telecom service providers transition to IP based VoLTE and introduce 5G, SS7 will be replaced with diameter signaling. This session provides the technical basics of diameter, options for transitioning SS7 to diameter and the new challenges facing law enforcement.

Bell Labs

Europol and Eurojust at EU Council



Council of the
European Union

Brussels, 6 May 2019
(OR. en)

8983/19

LIMITE

CT 45
COSI 97
CATS 67
ENFOPOL 213
TELECOM 202
CYBER 144

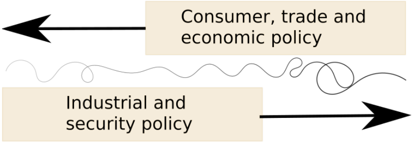
NOTE

From:	EU Counter-Terrorism Coordinator
To:	Delegations
Subject:	**Law enforcement and judicial aspects related to 5G**

ARTICLE 19

Bizarre struggles

European Union — **Member states**



Consumer, trade and economic policy

Industrial and security policy

Data protection — **National security**

Some weird consequences of this

- ☑ End-to-end encryption is being blocked not just by conservative companies but also by telcos terrified of losing their license.

Some weird consequences of this

- ☑ End-to-end encryption is being blocked not just by conservative companies but also by telcos terrified of losing their license.
- ☑ The “lawful intercept” working group actively encourages data maximization business models, in direct contradiction with European law, to enable more data retention.

Some weird consequences of this

- End-to-end encryption is being blocked not just by conservative companies but also by telcos terrified of losing their license.
- The “lawful intercept” working group actively encourages data maximization business models, in direct contradiction with European law, to enable more data retention.
- Proposals of dubious legality appear to be introduced as “requirements” on mobile networks, but can later come back in discussions on how laws should be changed (real-time access standard ETSI TS102657 is an example).

I propose: this is not useful

This is not a terrific position for mobile network equipment vendors and operators to be in.

Standards are good but how to we get them deployed?

The distressing example of website accessibility.

Standards are good but how to we get them deployed?

The distressing example of website accessibility.

- Radio Equipment Directive, Art. 3.3.e (privacy requirements)
- Data Protection Regulation, Art. 40 or 42 (Codes of Conduct and Certification)
- Support public procurements, for instance WIFI4EU procurements or similar.

How to make sure European values prevail?

- Probably counter-balancing representation in 3GPP (preferably institutional, e.g. Data Protection Authorities).
- NGOs (requires a lot of resources, money and time).
- National security interests work really long-term – it can take 20 years from the construction of a standard to a policy-washing attempt. European values must be supported by similarly long-term efforts.