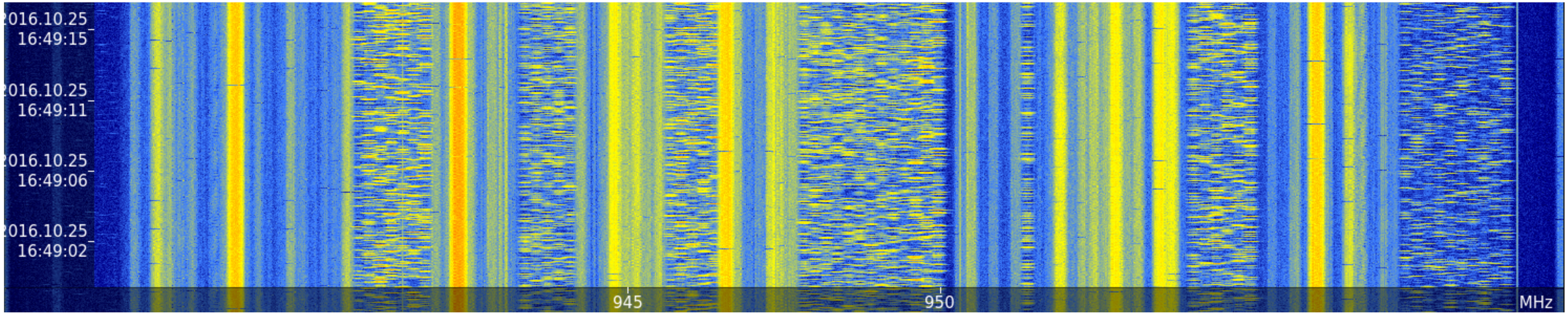
Mobile Networks Hacking Techniques

Tomas Rosa
crypto.hyperlink.cz

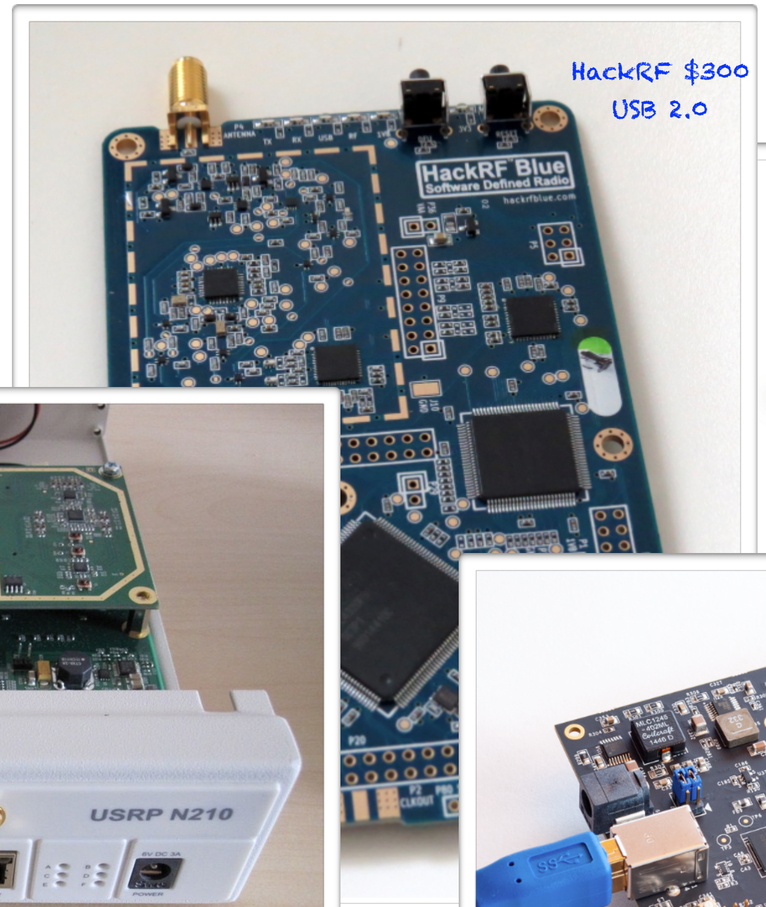
September 2017



List of Acronyms (Selected)

AuC - Authentication centre
BSC - Base station controller
BTS - Base transceiver station
CS - Circuit switching
CSFB - Circuit switched fallback
DSP - Digital signal processing
E-UTRAN - Evolved UMTS terrestrial radio access network
EDGE - Enhanced data rates for global (GSM) evolution
EIR - Equipment identity register
eNB - Evolved node B
EPC - Evolved packet core
GERAN - GSM EDGE radio access network
GGSN - Gateway GPRS support module
GMSC - Gateway mobile switching centre
GMSK - Gaussian minimum shift keying
GPRS - General packet radio service
GSM - Global system for mobile communication
HLR - Home location register
HSS - Home subscriber server
LTE - Long term evolution
MITM - Man in the middle
MME - Mobility management entity
MNO - Mobile network operator
MO - Mobile originated
MSC - Mobile switching centre
MT - Mobile terminated
Node B - UMTS base station (formerly a temporary name that stuck)
OFDM - Orthogonal frequency division multiple access
P-GW - Packet data network gateway
PCRF - Policy and charging rules function
PDN - Packet data network
PLMN - Public land mobile network
PS - Packet switching
PSD - Payment services directive
PSDN - Public switched data network
PSK - Phase shift keying
PSP - Payment service provider
PSTN - Public switched telephone network
QAM - Quadrature amplitude modulation
QPSK - Quadrature phase shift keying
RAN - Radio access network
RNC - Radio network controller
RTS - Regulatory technical standards
S-GW - Serving gateway
SAE - System architecture evolution
SDR - Software-defined radio
SGSN - Serving GPRS support node
SIM - Subscriber identity module
SMS - Short message service
SMS-SC - Short message service - service centre
SS7 - Signalling System No. 7
UE - User equipment
UMTS - Universal mobile telecommunication system
USIM - Universal subscriber identity module
UTRAN - UMTS terrestrial radio access network
VLR - Visitor location register
VoLTE - Voice over LTE
WCDMA - Wideband code division multiple access

Software Defined Radio

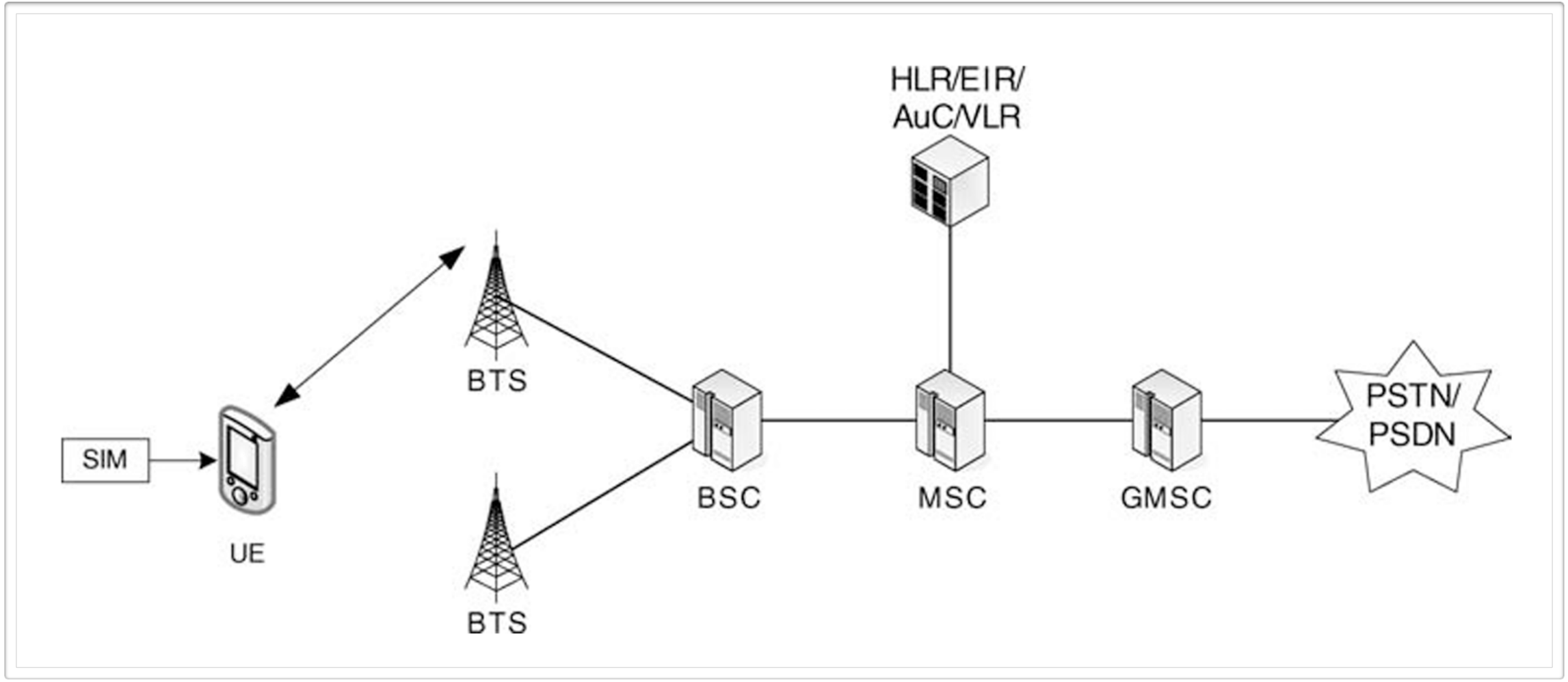


SDR as a Threat

DSP routines implementing an RF attack are indeed a piece of software, now. This can be shared, installed, and executed all around the world instantly with a very modest background.

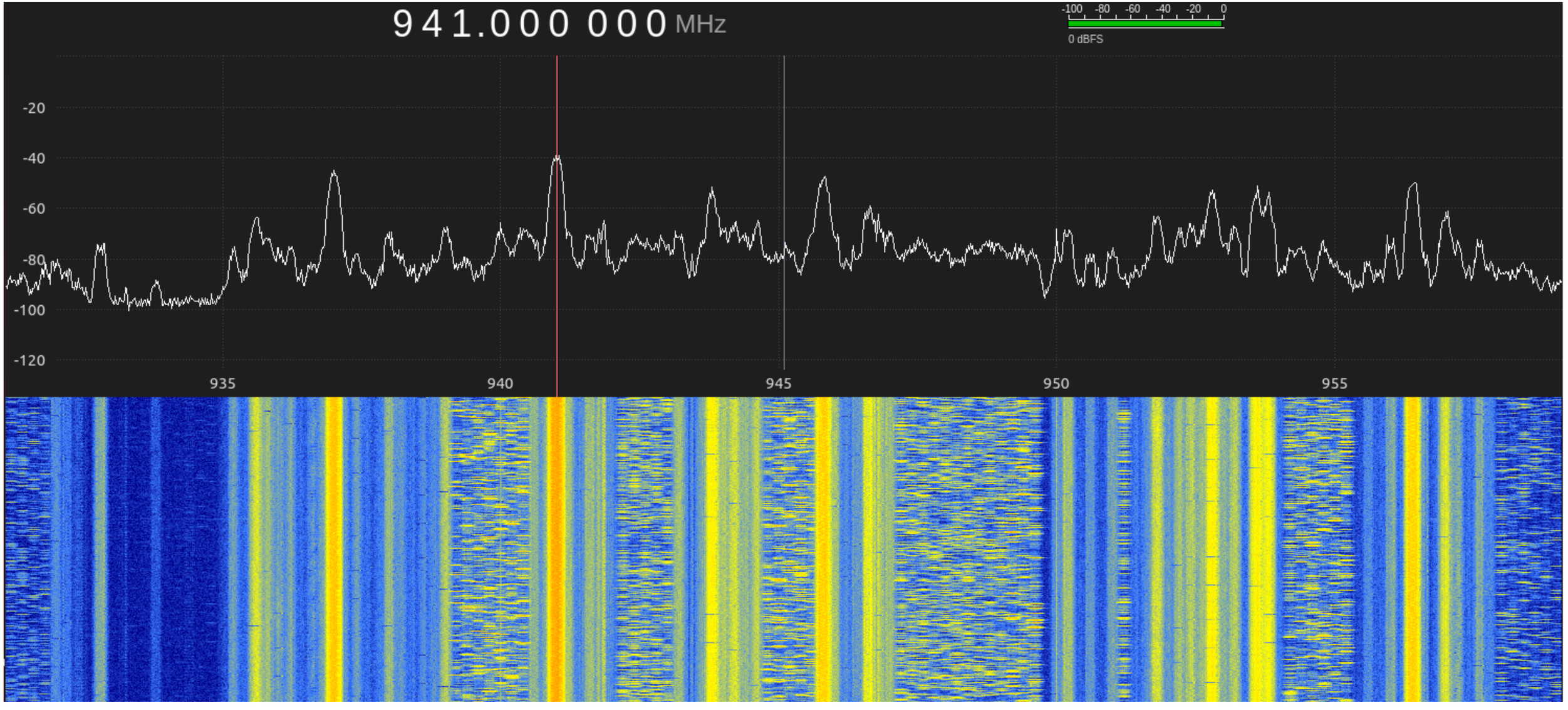
Just like any other exploit code.

GSM - Circuit Switching Infrastructure

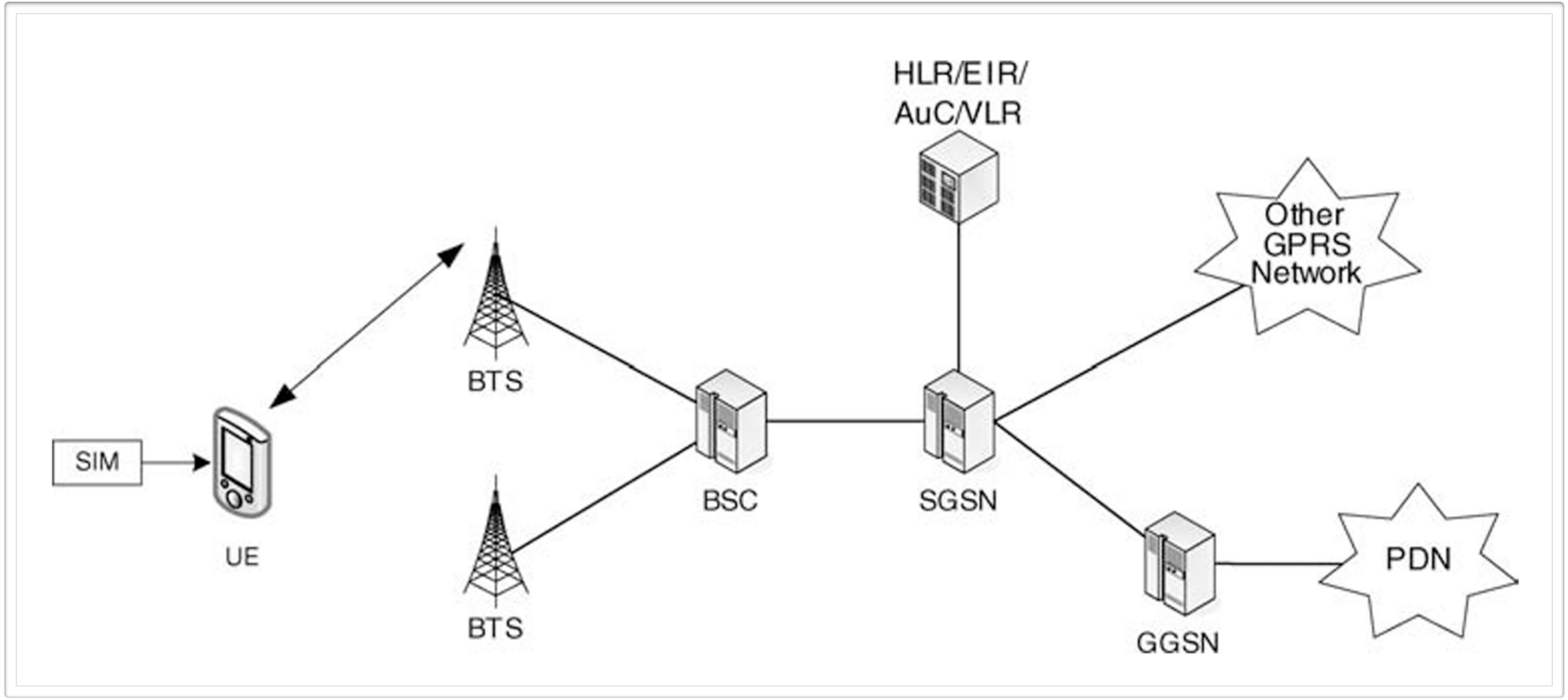


[Yi, Chun, Lee, Park, and Jung, 2012]

GSM / EDGE Radio Access Network (GERAN) Downlink Spectrogram

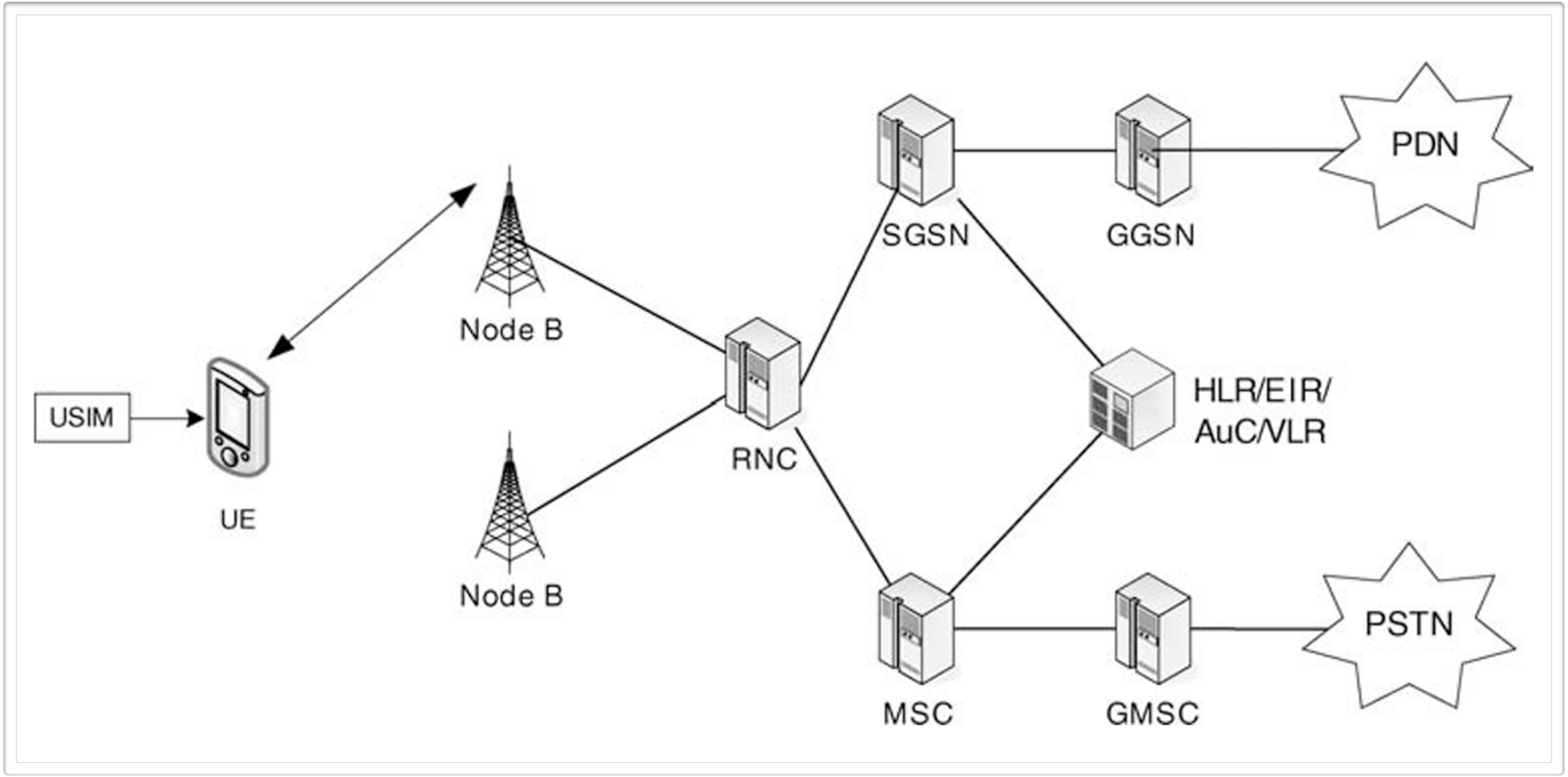


GPRS - Adding the Packet Switching Domain



[Yi, Chun, Lee, Park, and Jung, 2012]

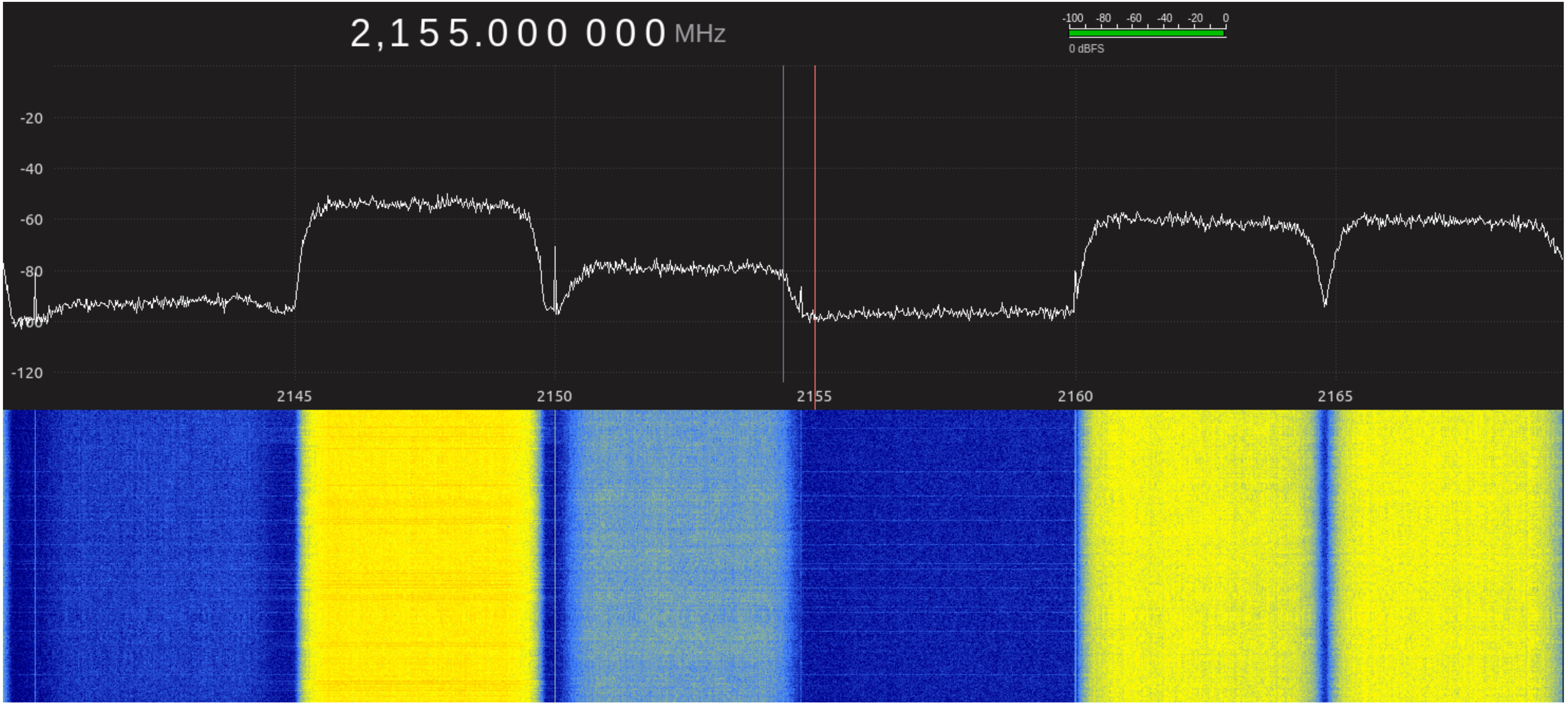
3G (UMTS) - Wideband* CDMA Radio, CS & PS Convergence



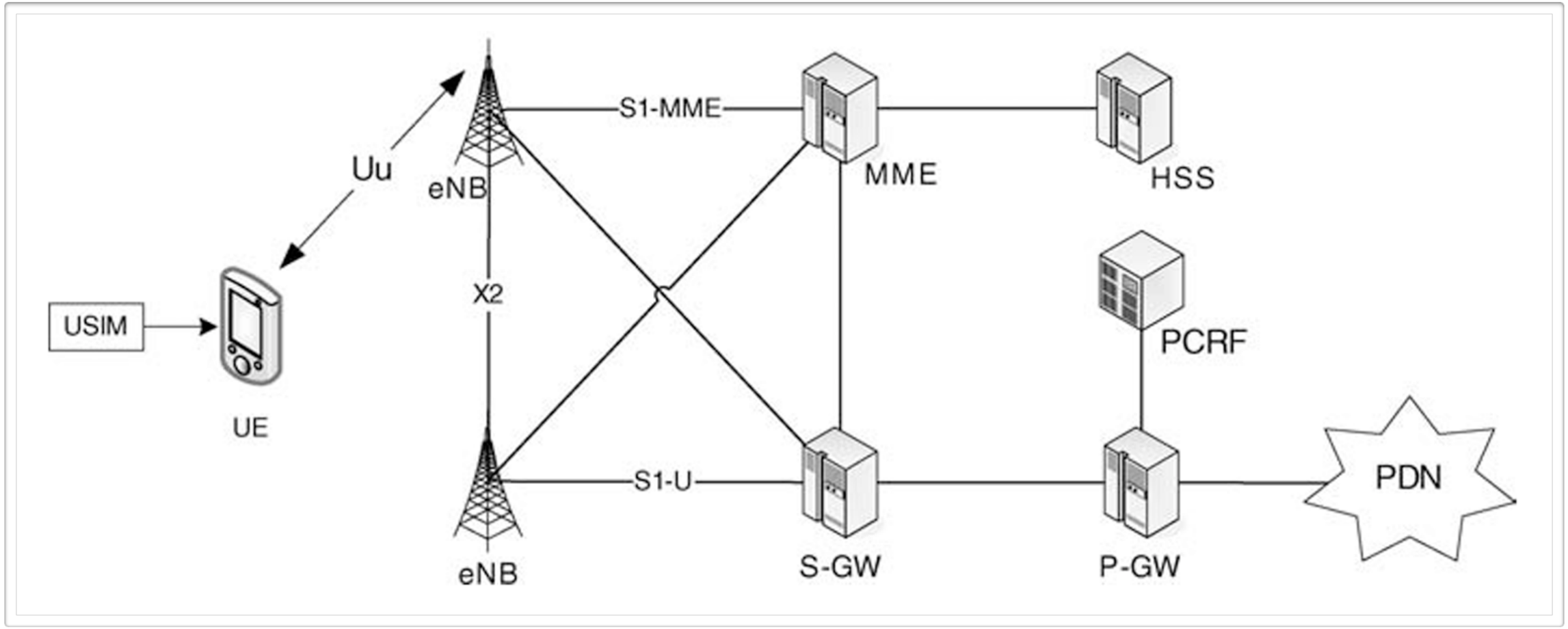
*) referring to the channel bandwidth when compared to 2G

[Yi, Chun, Lee, Park, and Jung, 2012]

UMTS Terrestrial Radio Access Network (UTRAN) Downlink Spectrogram



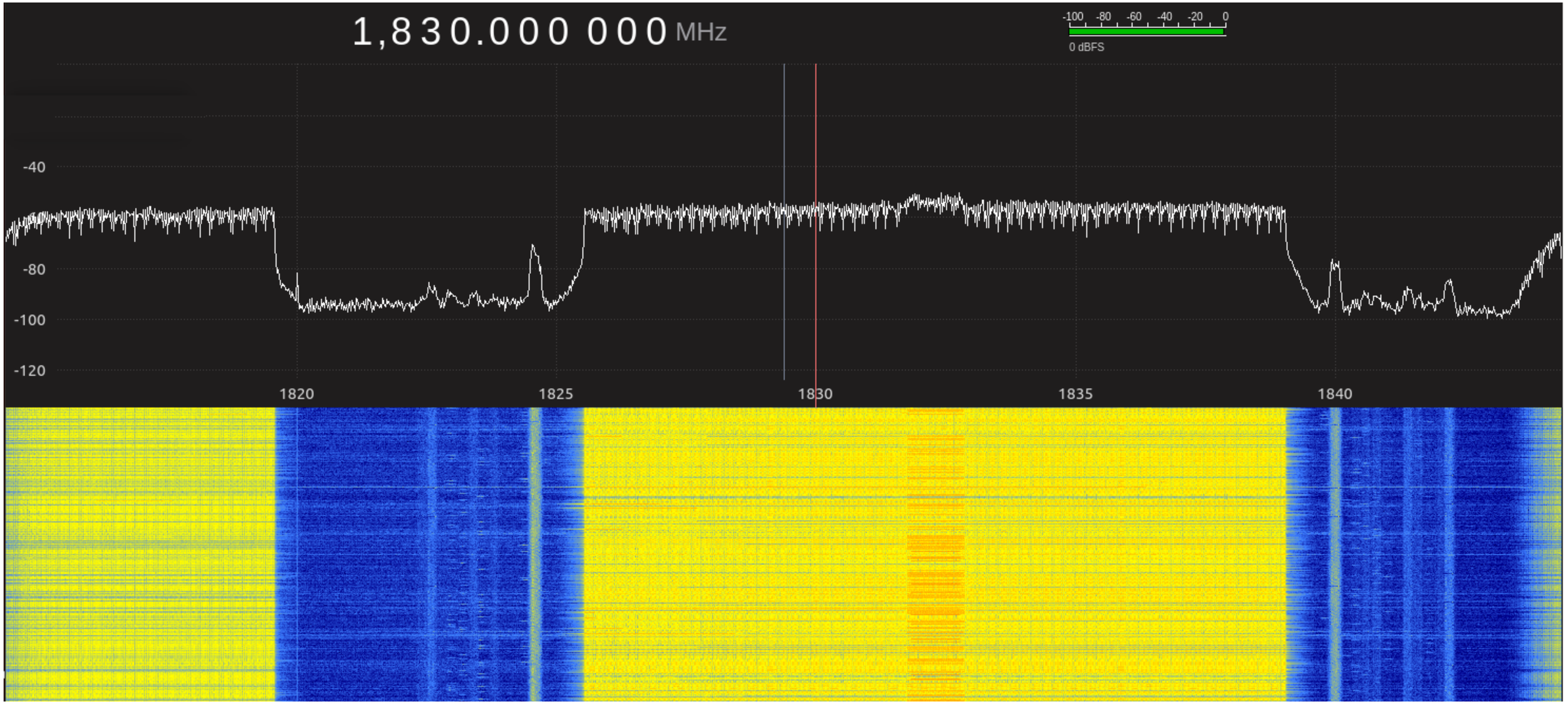
4G (LTE/SAE) - Massive Broadband* OFDMA Radio with Evolved **PS Core (no CS)**



*) referring to the big number of orthogonal sub-channels

[Yi, Chun, Lee, Park, and Jung, 2012]

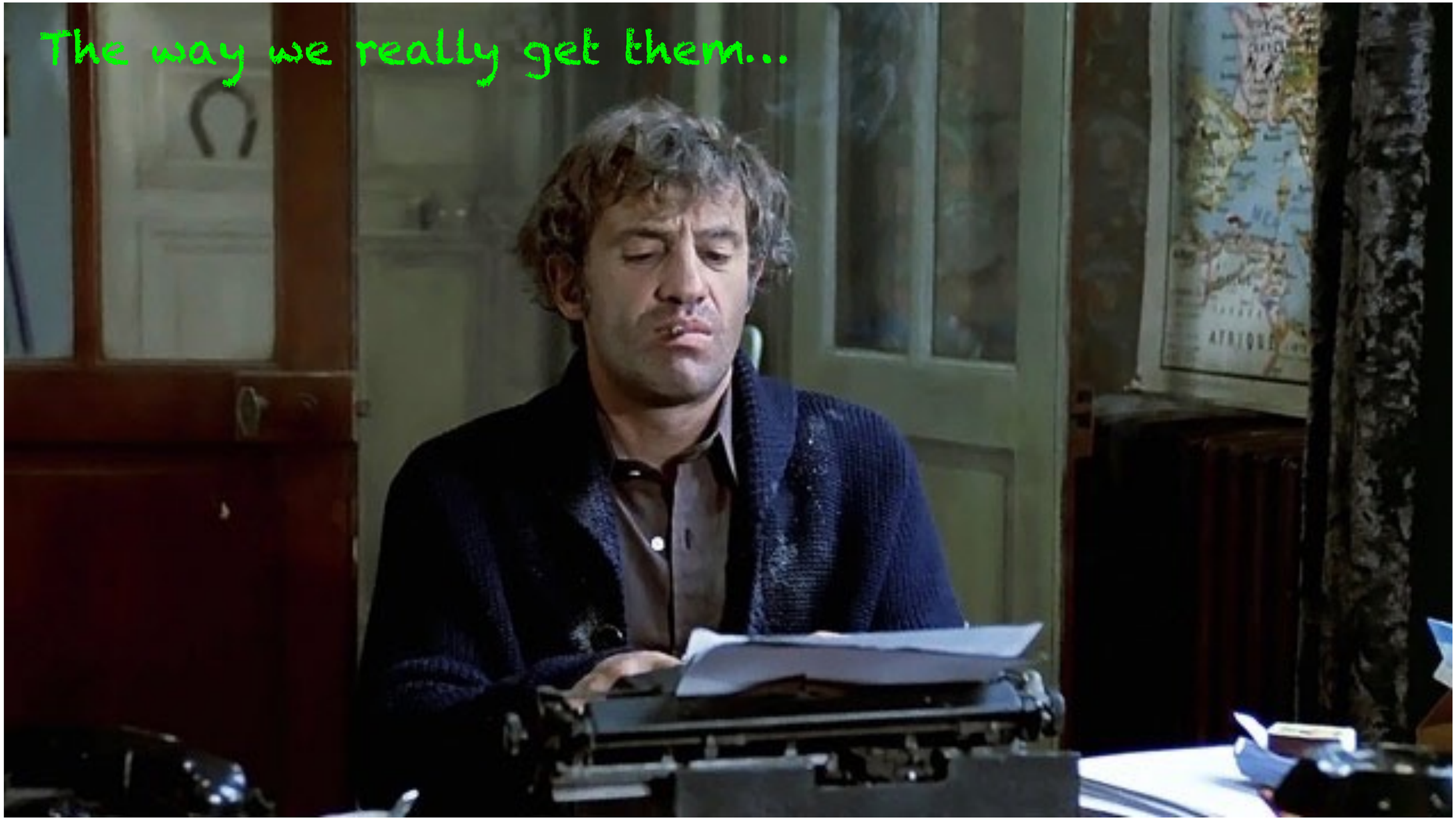
Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) Downlink Spectrogram

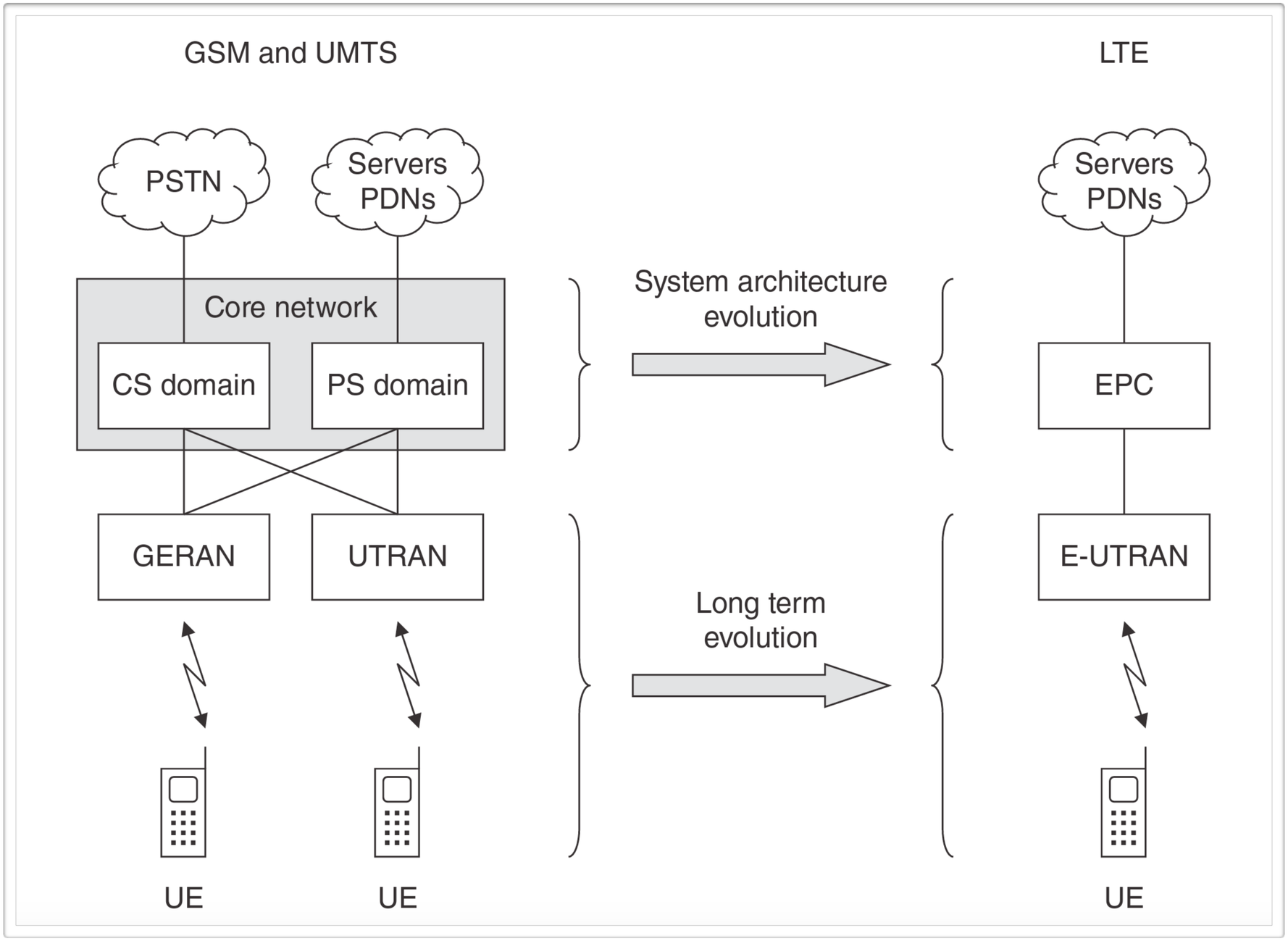


PLMN Threats

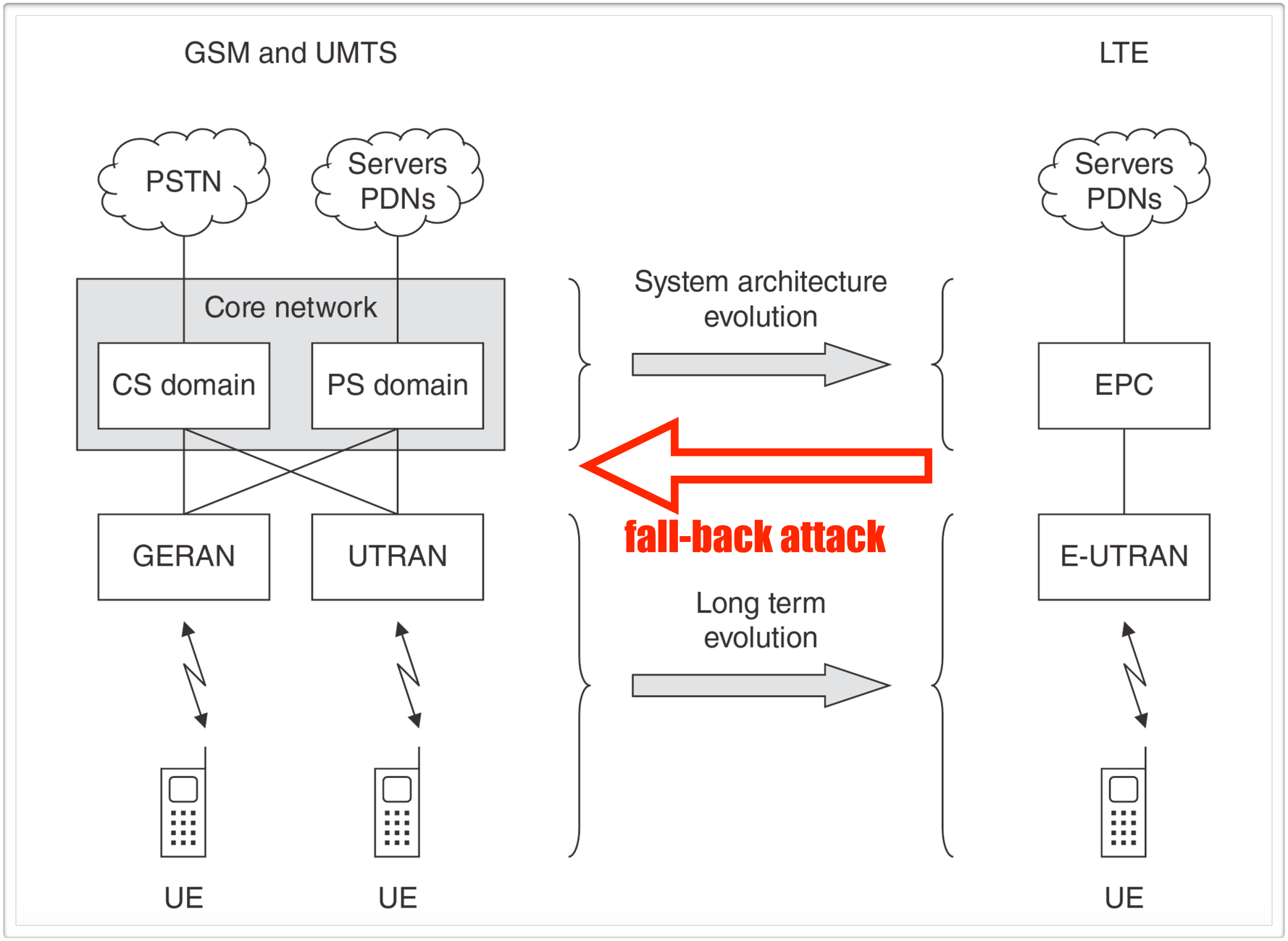
- **Billing frauds**
  - identity theft / impersonations
- **Privacy breach**
  - user tracking
  - voice / data interception
- **Integrity violation**
  - identity / data spoofing


The way we present research results

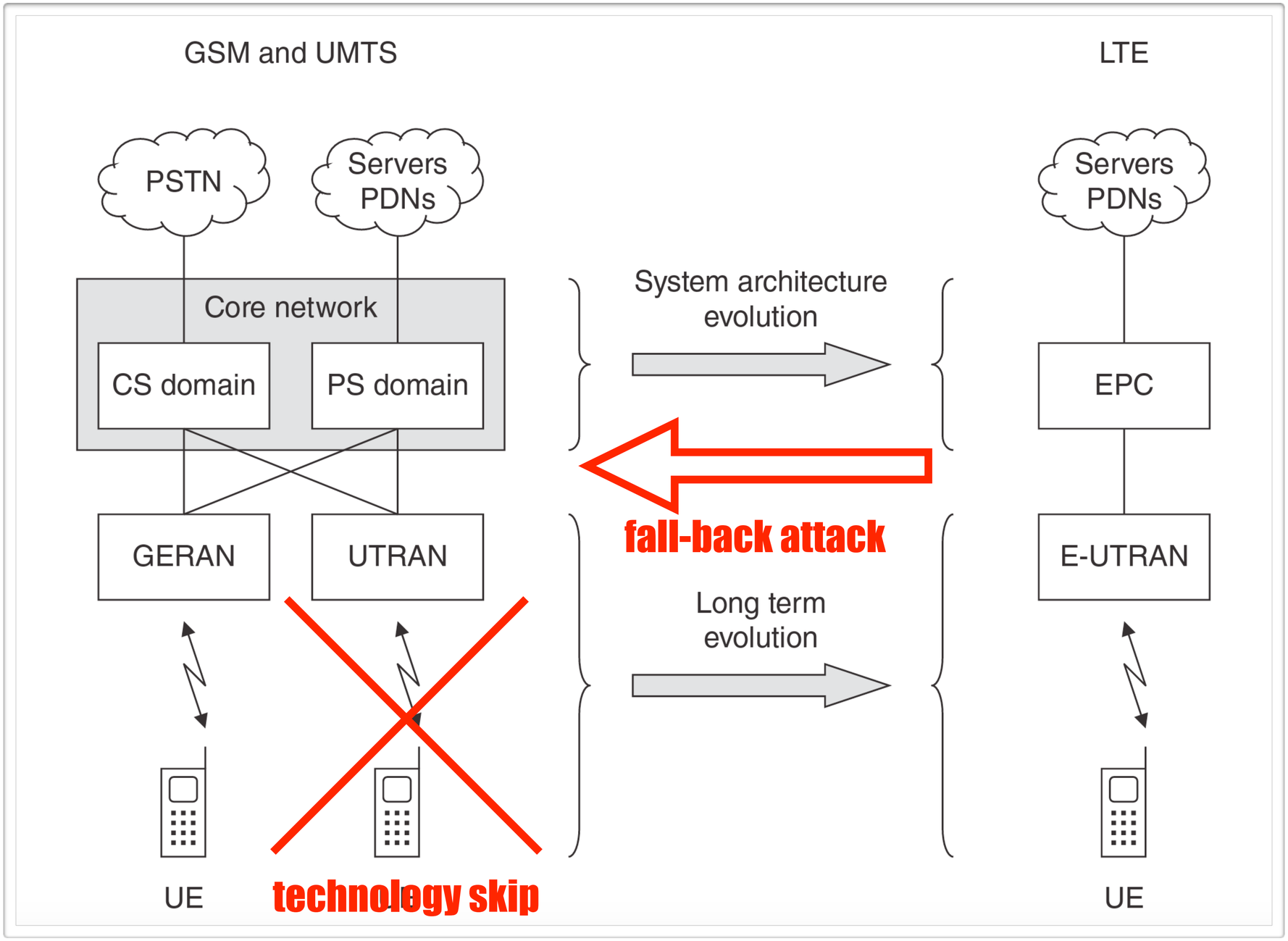

The way we really get them...


GSM and UMTS
LTE
PSTN
Servers
PDNs
Core network
CS domain
PS domain
GERAN
UTRAN
UE
UE
System architecture
evolution
Long term
evolution
Servers
PDNs
EPC
E-UTRAN
UE

[Cox, 2014]

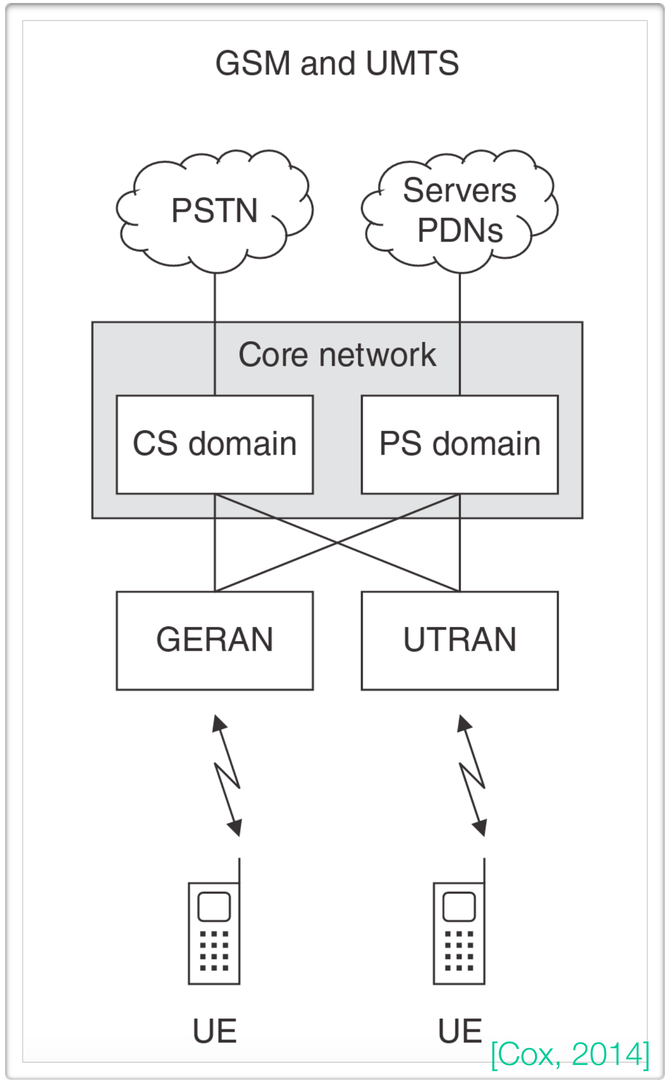

GSM and UMTS
LTE
PSTN
Servers PDNs
Core network
CS domain
PS domain
GERAN
UTRAN
UE
UE
System architecture evolution
fall-back attack
Long term evolution
Servers PDNs
EPC
E-UTRAN
UE

[Cox, 2014]


GSM and UMTS
LTE
PSTN
Servers PDNs
Servers PDNs
Core network
CS domain
PS domain
EPC
System architecture evolution
fall-back attack
GERAN
UTRAN
E-UTRAN
Long term evolution
UE
technology skip
UE

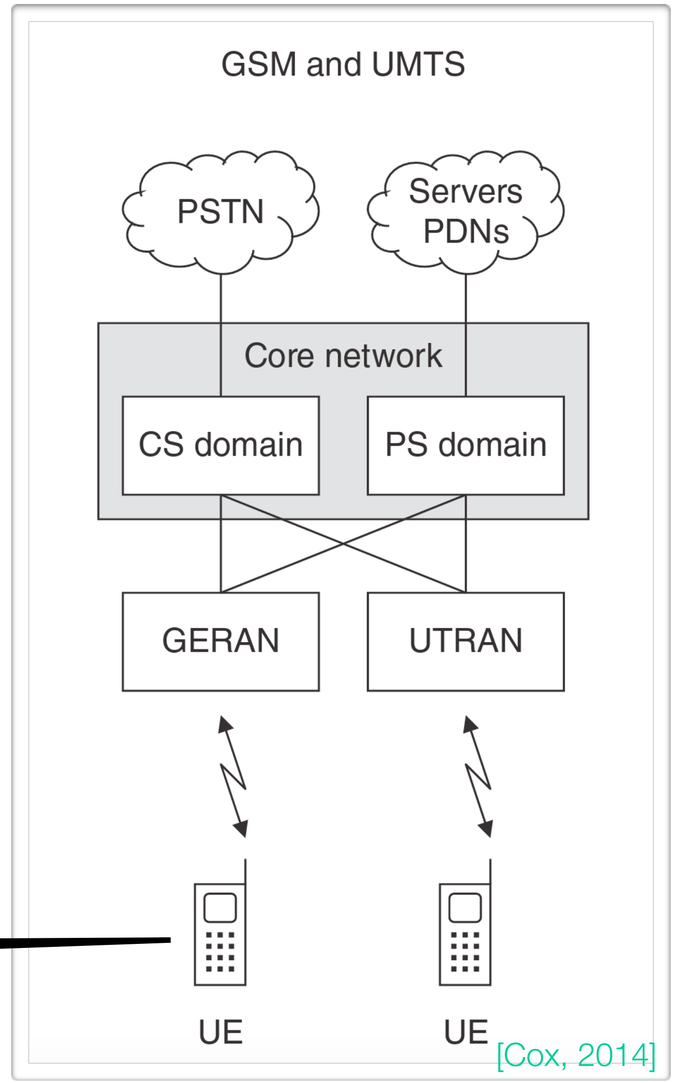
[Cox, 2014]

2G/3G Attacks Playground



[Cox, 2014]

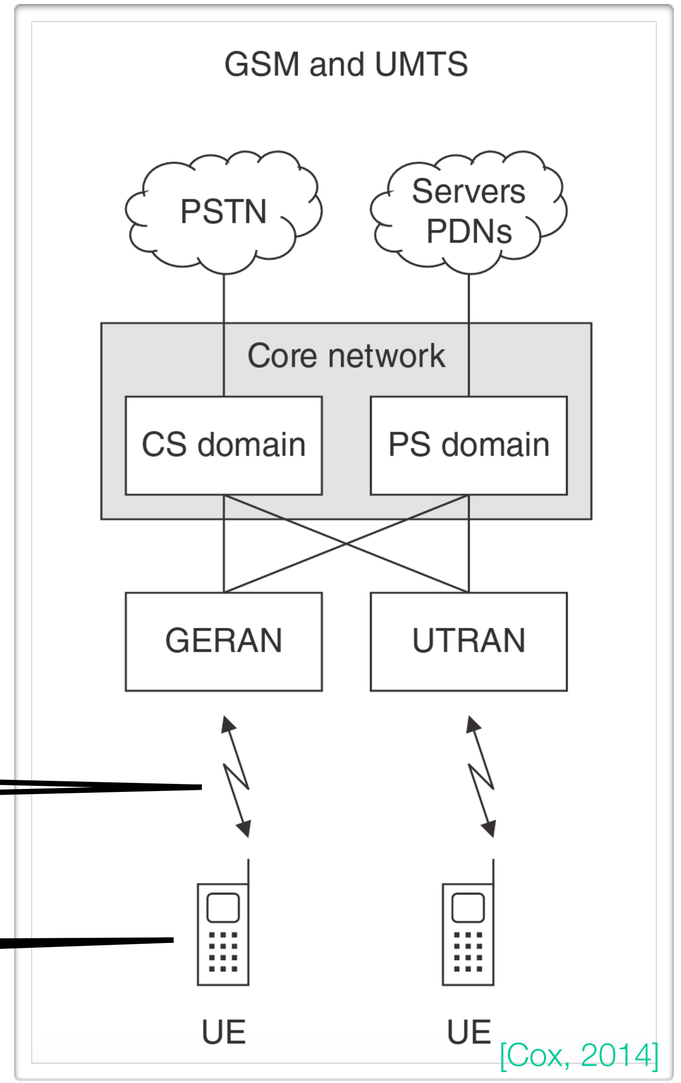
2G/3G Attacks Playground



[Cox, 2014]

mobile malware, SIM swap

2G/3G Attacks Playground



passive/active RF attacks

mobile malware, SIM swap

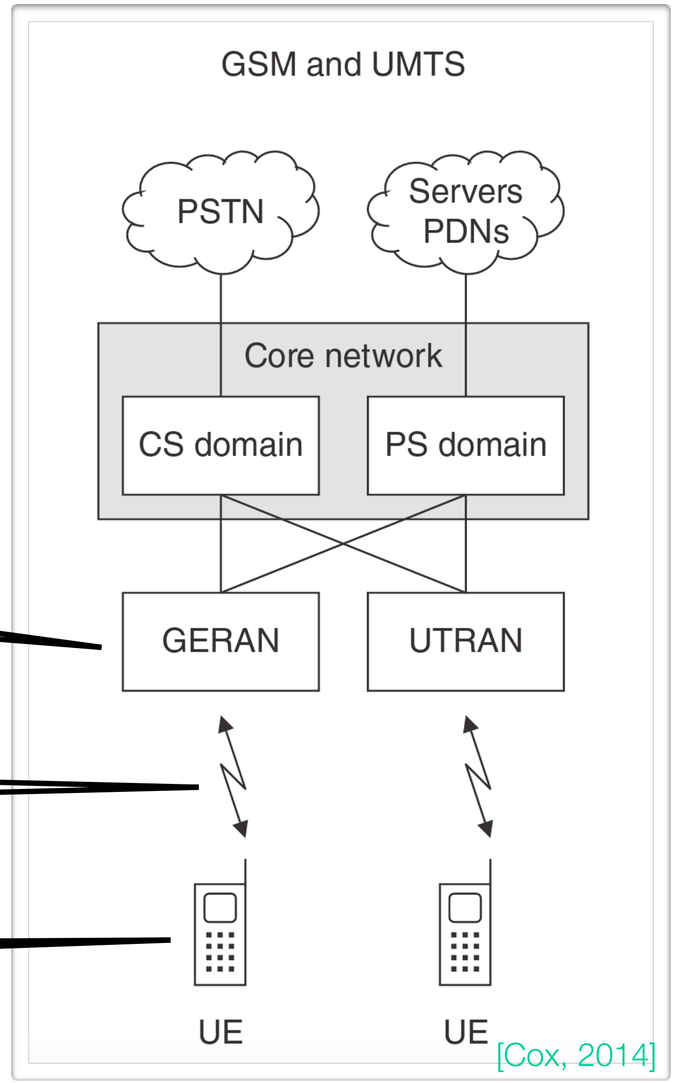
[Cox, 2014]

2G/3G Attacks Playground

fake BTS / femtocell hacking

passive/active RF attacks

mobile malware, SIM swap



[Cox, 2014]

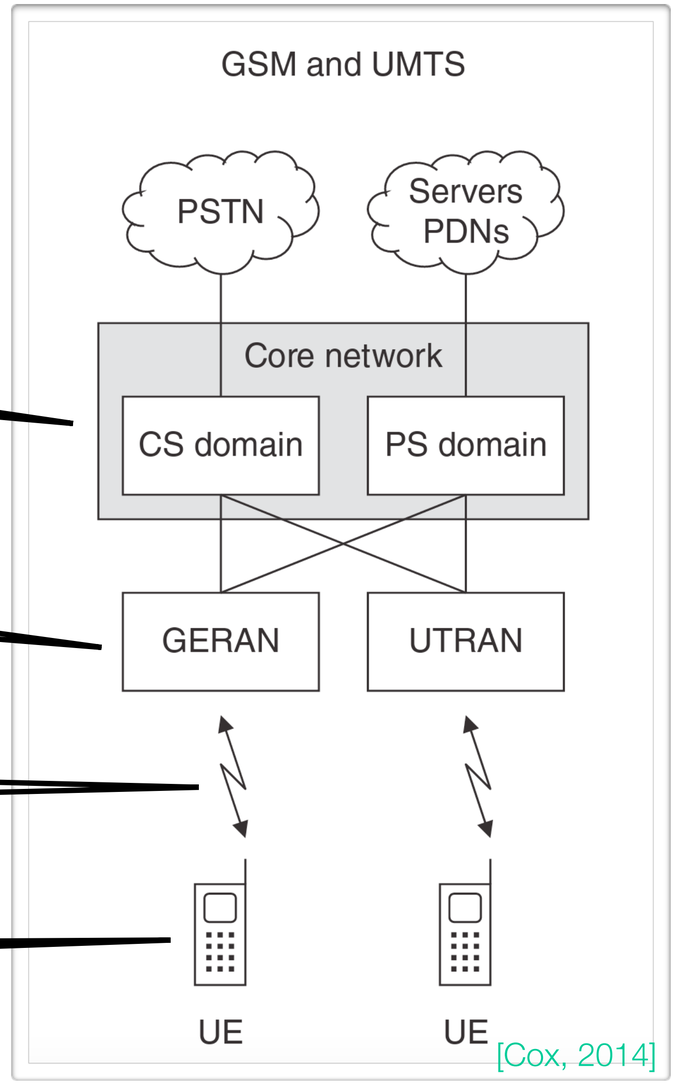
2G/3G Attacks Playground

SS7 “gadgets” abuse

fake BTS / femtocell hacking

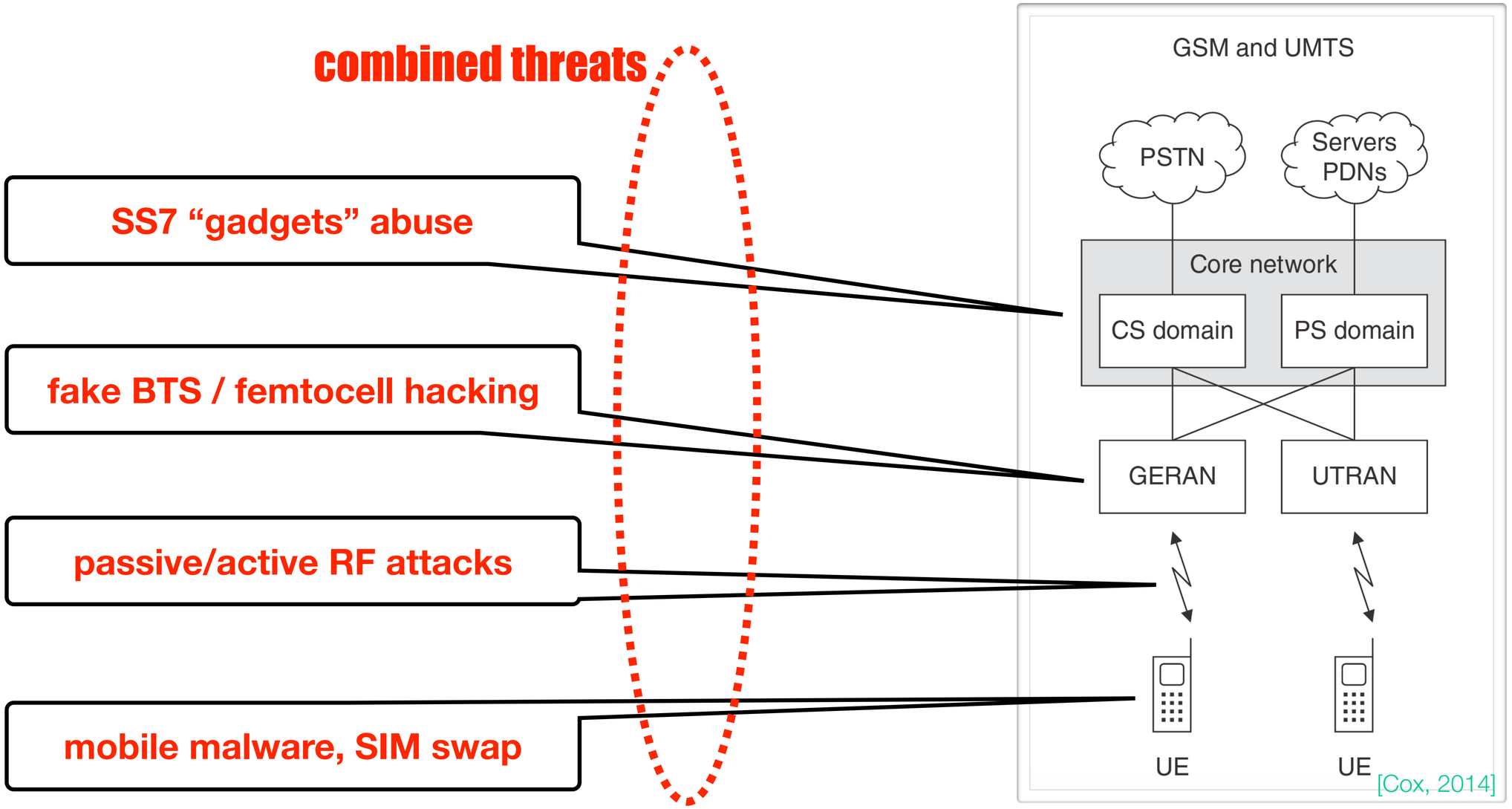
passive/active RF attacks

mobile malware, SIM swap



[Cox, 2014]

2G/3G Attacks Playground



[Cox, 2014]

Further 4G Attacks

- …besides the forced fall-back [2016]
- Exploitation of missing authentication in an ordinary CSFB from 4G to 3G/2G [2017]
- User tracking and activity monitoring based on authentication key agreement protocol leakage in 4G/3G [2017]
- …and we can expect more, because of the high interest combined with SDR-based easy access to E-UTRAN

Mobile-Terminated (MT) versus Mobile-Originated (MO)

- If any, we shall definitely **stay with MT services** (SMS reception, voice call answer) if we want to get at least “something”
- MO-based checks (SMS sender, voice call originator) are far easier to spoof
- Paris Hilton was already able to use a Caller ID spoofer in 2009

[Paris Hilton, 2012]

Scams

Sim-swap fraud claims another mobile banking victim

Chris Sims' account emptied and loan for £8,000 taken out as fraudsters continue to exploit way banks use customers' mobiles

> EE said it has recordings of two calls where the fraudster failed security. You'd think this would set bells ringing
>
> **Chris Sims**

Miles Brignall

Saturday 16 April 2016 07.00 BST

Shares 464 Comments 111

Save for later

[The Guardian, 2016]

PSD2 RTS final report on draft EBA/RTS/2017/02

Article 21
Association with the payment service user

1. Payment service providers shall ensure that only the payment service user is associated with the personalised security credentials, with the authentication devices and the software in a secure manner.

2. For the purpose of paragraph 1, payment service providers shall ensure that each of the following requirements is met:

(a) the association of the payment service user's identity with personalised security credentials, authentication devices and software is carried out in secure environments. In particular, the association shall be carried out in environments under the payment service provider's responsibility and taking into account risks associated with devices and underlying components used during the association process that are not under the responsibility of the payment service provider. The environments under the payment service

PSD2 RTS final report on draft EBA/RTS/2017/02

Article 9
Independence of the elements

1. Payment service providers shall ensure that the use of the elements of strong customer authentication referred to in Articles 6, 7 and 8 shall be subject to measures in terms of technology, algorithms and parameters, which ensure that the breach of one of the elements does not compromise the reliability of the other elements.

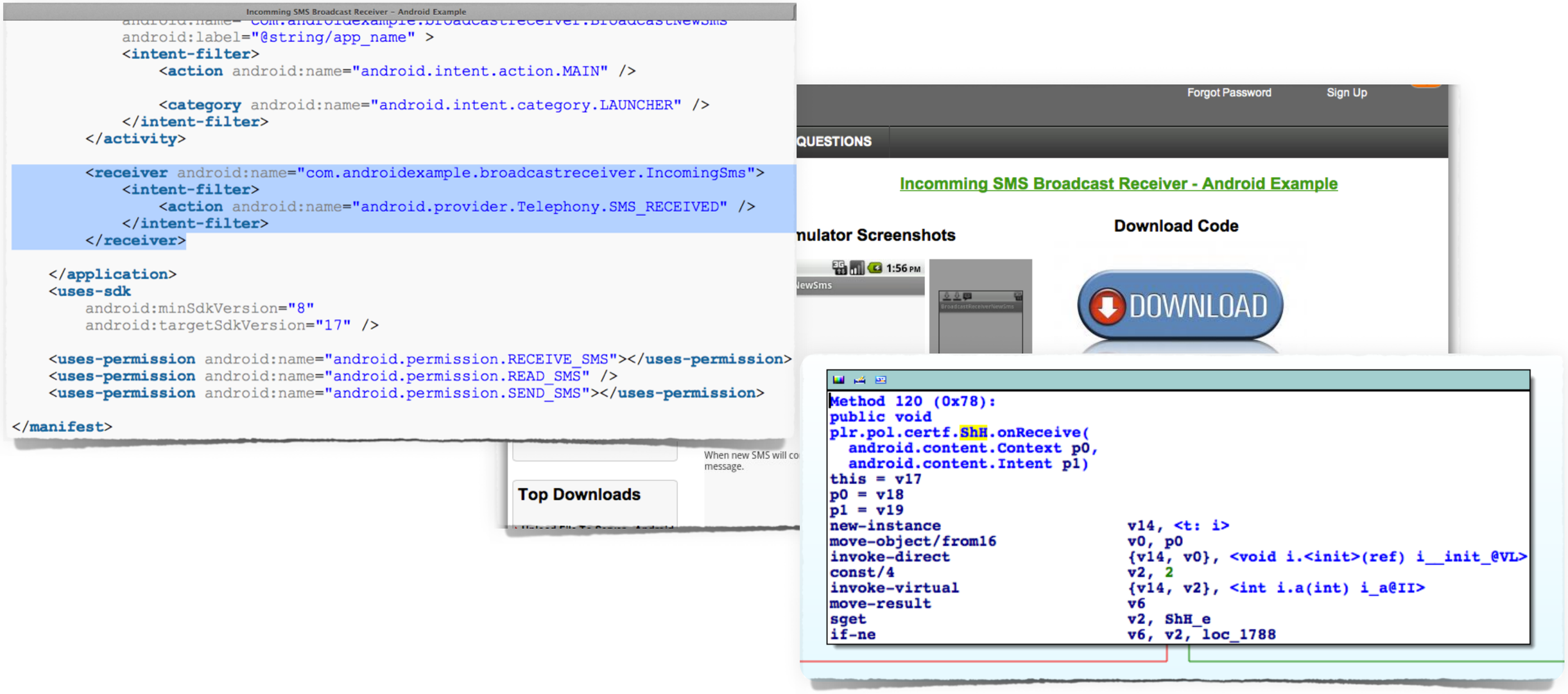
2. Where any of the elements of strong customer authentication or the authentication code is used through a multi-purpose device including mobile phones and tablets, payment service providers shall adopt security measures to mitigate the risk resulting from the multi-purpose device being compromised.

3. For the purposes of paragraph 2, the mitigating measures shall include each of the following:

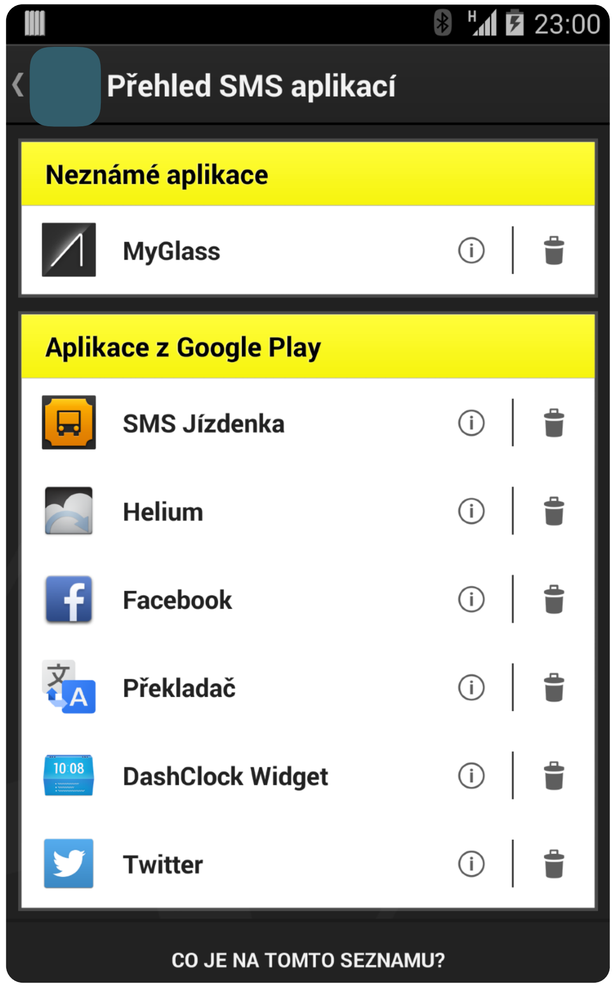
   (a) the use of separated secure execution environments through the software installed inside the multi-purpose device;

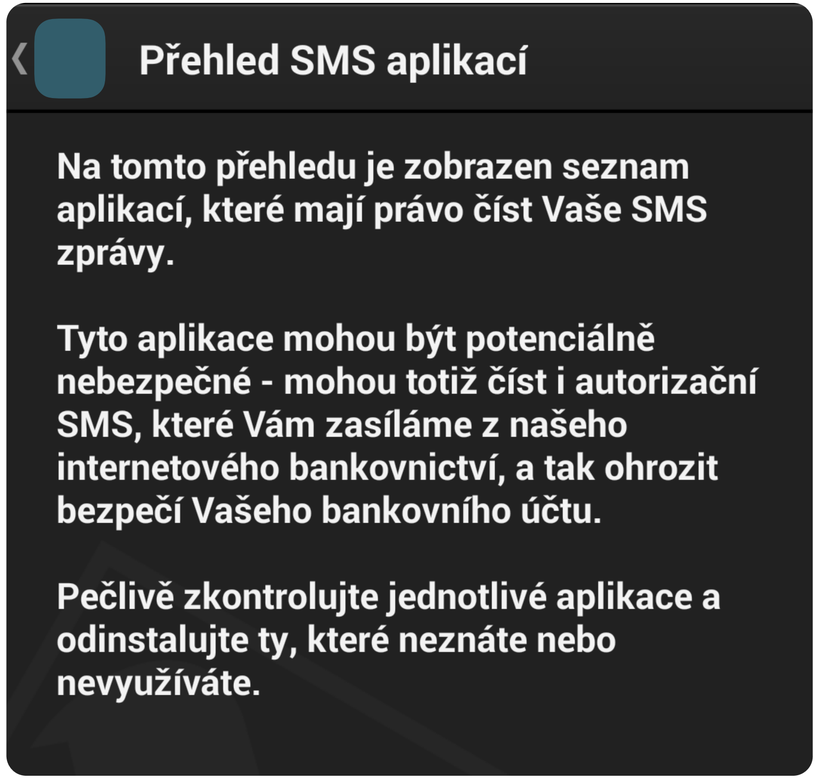
   (b) mechanisms to ensure that the software or device has not been altered by the payer or by a third party or mechanisms to mitigate the consequences of such alteration where this has taken place.

Android SMS Interception Trojan



S.A.S. Sidekick of a Mobile Banking Application





- Seek-And-Smash
- This honest mobile application searches for the specific type of *broadcast receiver* that is potentially capable of SMS interception
- When found, it issues a warning to the user suggesting the suspicious application removal

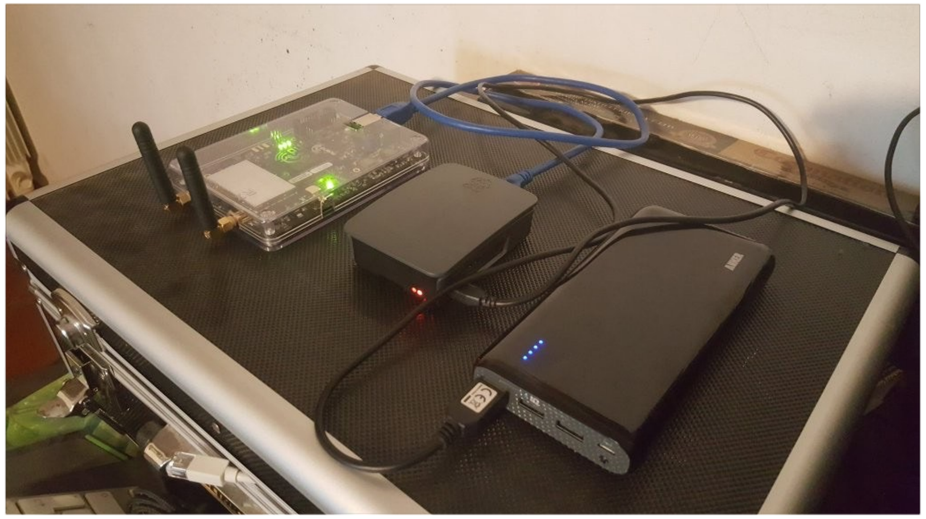
GERAN Vulnerabilities Review

- Passive interception
  - usable wherever A5/1 (or A5/2) is still employed
  - also possible with the help of SS7 key stealing gadgets
- Active session hijacking with encryption suppression
  - paging channel race condition (usually 100 to 500 km^2 coverage) together with weak (re)authentication or SS7 sidekick
  - fake BTS or a rogue femtocell

UTRAN (3G) compatible approach

RTL-SDR.COM

RTL-SDR (RTL2832U) and software defined radio news and projects. Also featuring Airspy, HackRF, FCD



OCTOBER 4, 2016

BUILDING YOUR OWN ROGUE GSM BASESTATION WITH A BLADERF

Over on his blog author Simone Margaritelli has added a tutorial that shows how to set up a bladeRF to act as a GSM basestation (cell tower). Having your own GSM basestation allows you to create your own private and free GSM network, or for more malicious illegal users it can allow you to create a system for intercepting peoples calls and data. Simone stresses that it is well known that GSM security is broken (and is probably broken by design), and now it is about time that these flaws were fixed.

In his tutorial he uses a single bladeRF x40 and a Raspberry Pi 3 as the processing hardware. The bladeRF is a $420 transmit and receive capable software defined radio with a tuning range of 300 MHz – 3.8 GHz and 12-bit ADC. He also uses a battery pack which makes the whole thing portable. The software used is Yate and YateBTS which is open source GSM basestation software. Installation as shown in the tutorial is as simple as doing a git clone, running a few compilation lines and doing some simple text configuration. Once set up mobile phones will automatically connect to the basestation due to the design of GSM.

Once setup you can go further and create your own private GSM network, or make the whole thing act as a “man-in-the-middle” proxy to a legitimate GSM USB dongle, which would allow you to sniff the traffic on anyone who unknowingly connects to your basestation. This is similar to how a “Stingray” operates, which is a IMSI-catcher device used by law enforcement to intercept

Robust Approach to Active 2G/3G/4G MITM Attacks

Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunication

Nico Golde, Kévin Redon, Ravishankar Borgaonkar
Security in Telecommunications
Technische Universität Berlin
{nico,kredon,ravii}@sec.t-labs.tu-berlin.c

VĚSTNÍK VEŘEJNÝCH ZAKÁZEK

ID Formuláře: 87840
Evidenční číslo zakázky: 60021365
Evidenční číslo formuláře: 6002136503001
Datum uveřejnění ve VVZ: 18. 08. 2008
Typ: Řádný

IČO zadavatele: 00007064
IČO dodavatele: 492 42 954

Evropská unie
Vydání dodatku k Úřednímu v

2, rue Mercier, 2985 Luxembourg, Lu
E-mail: ojs@publications.europa.eu

portable IMSI catchers delivery demanded

II.1.4) Stručný popis zakázky nebo nákupu(ů) *

Dodání kufříkových zařízení IMSI catcher.

II.1.5) Společný slovník pro veřejné zakázky (CPV)

	Hlavní slovník	Doplňkový slovník (je-li to relevantní)
Hlavní předmět *	30259400-3	

I.1) Název, adresa a kontaktn

Úřední název *

Česká republika - Ministerstvo vnitra

Poštovní adresa *

Nad Štolou 936/3

Obec *		**PSČ**	170 34
		Stát *	CZ
		Tel.	+420 974 835 052

CZ ministry of interior

[https://old.vestnikverejnychzakazek.cz/en-us/Form/Display/87840]

Hacking

SS7 hack explained: what can you do about it?

A vulnerability means hackers can read texts, listen to calls and track mobile phone users. What are the implications and how can you protect yourself from snooping?

Samuel Gibbs

Tuesday 19 April 2016 15.51 BST

Shares
663

Save for later

[The Guardian, 2016]

The Register®
Biting the hand that feeds IT

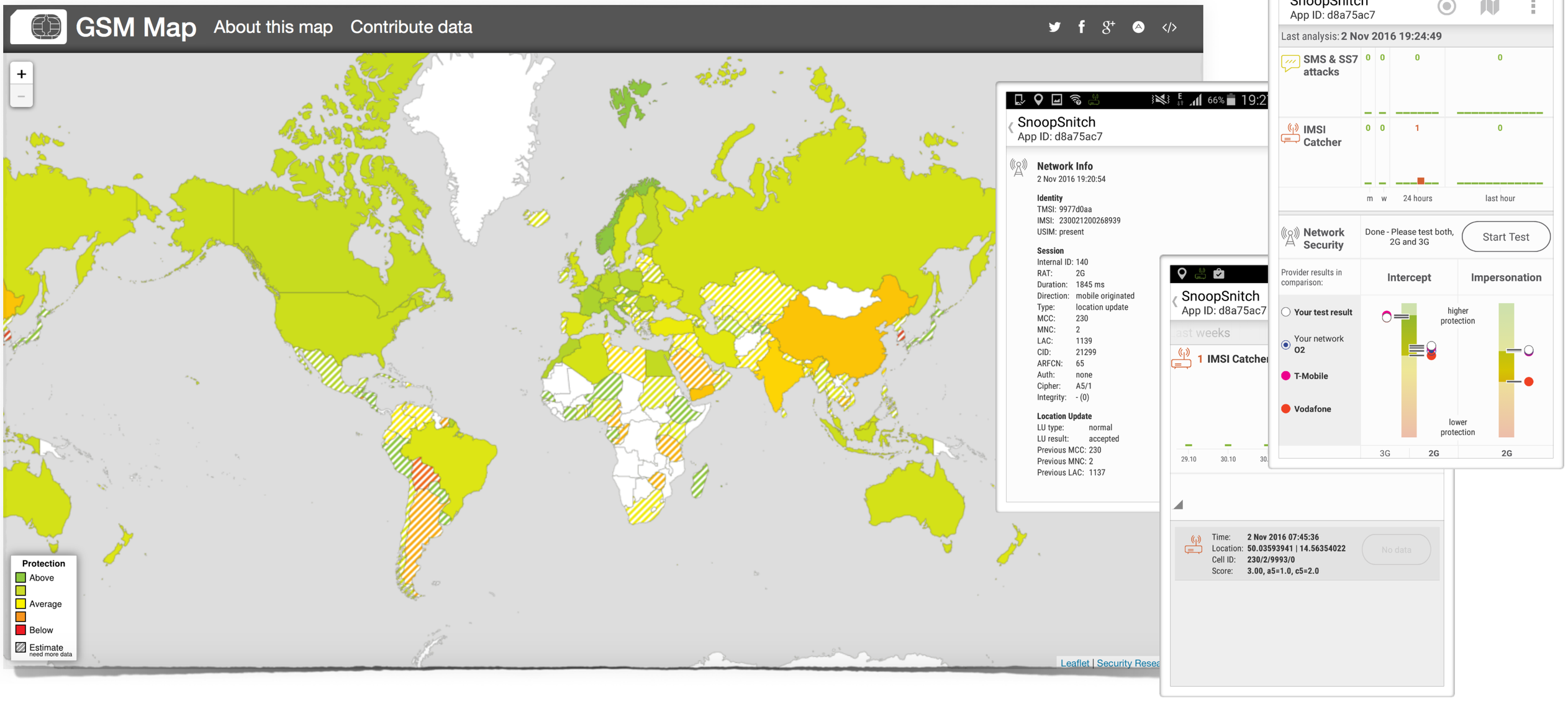
Security

48

After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts

O2 confirms online thefts using stolen 2FA SMS codes

Remember: One weak MNO to rule them all, … to find them, … to bring them all and in the darkness bind them



Conclusion

- We shall primarily consider any 2G/3G/4G or even the emerging 5G service to be **just yet another computer network**

  … so, being essentially a subject to the same bunch of threats and vulnerabilities as we know them from e.g. the internet domain

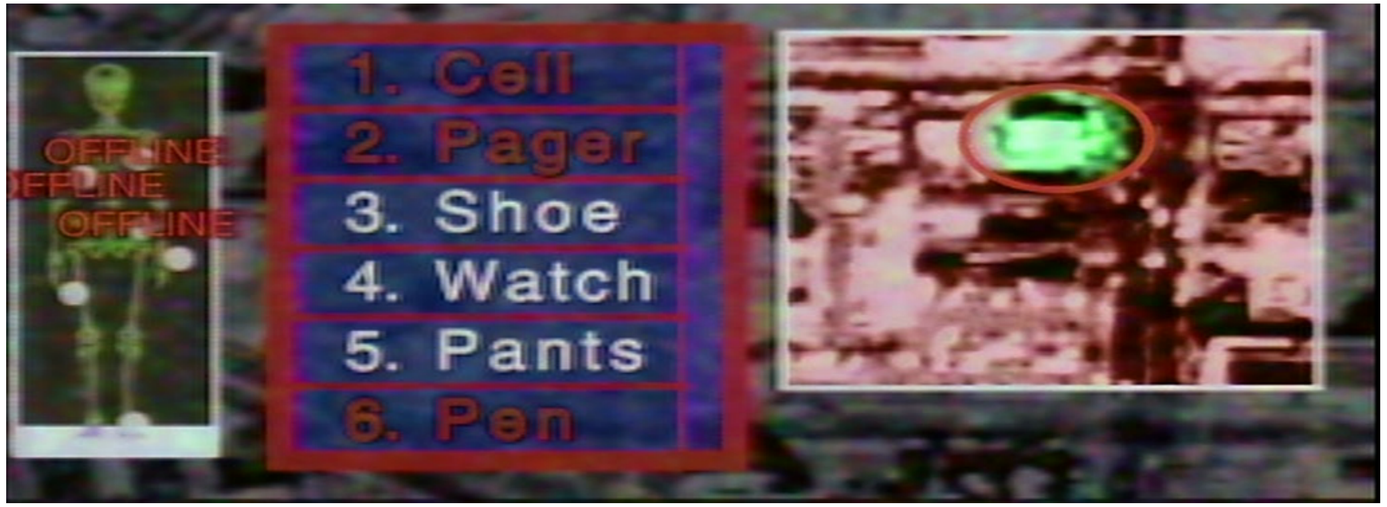
- There is no end-to-end encryption, the “last mile” over-the-air protection is far from being ideal, and the mobile operators interworking is like TCP/IP in early ‘90s

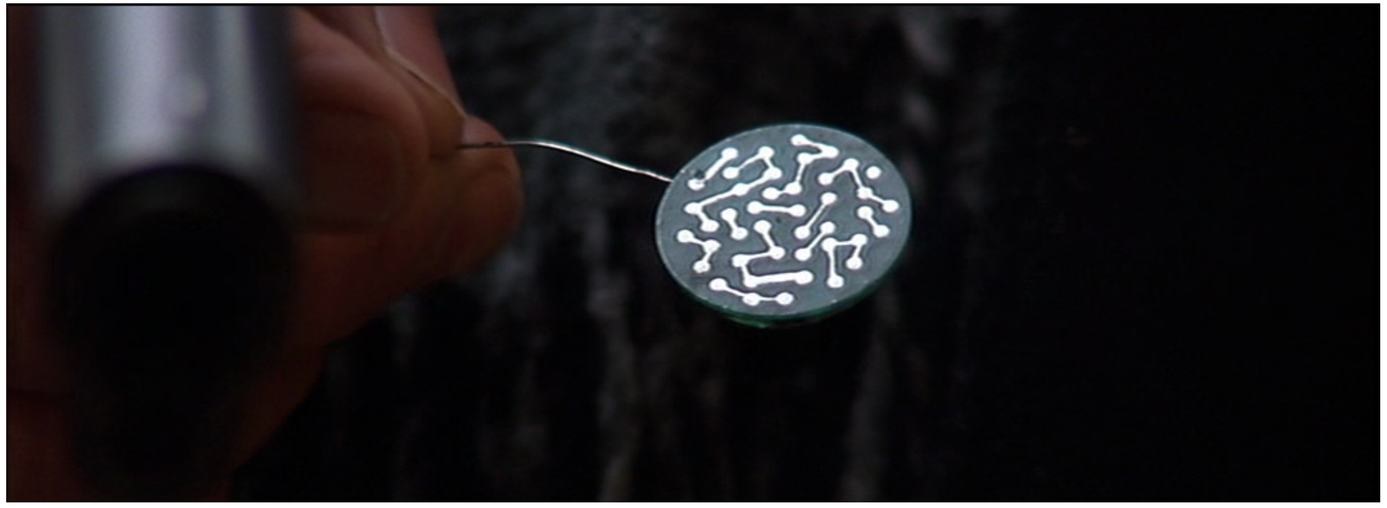
- Missing open Radio Access Network adapters together with obscure SS7 infrastructure used to keep a lot of elite network hackers apart

  … **now, software-defined radios bring affordable RAN adapters and SS7 access nodes can be rent for a few hundreds of EUR**

  … we shall expect those formerly theoretical attacks will become a practical hacking routine soon and a lot of new vulnerabilities will probably be discovered

Stay Tuned
Spy Bugs - Principle, Detection, Counter-Detection





Acknowledgements

The author is grateful to Jiří Buček (FIT CTU), Tomáš Jabůrek (RBCZ), Lukáš Jirovský (RBCZ), Radek Komanický (RBCZ), and Martin Opava (truconneXion).

They all have contributed with non-trivial help to make the humble research possible and pleasant.

References - General Monograph

1. 3GPP Specifications, http://www.3gpp.org/specifications
2. Cox, C.: An Introduction to LTE: LTE, LTE-Advanced, SAE, VoLTE and 4G Mobile Communications, 2nd Ed., Wiley, 2014
3. Cox, C.: Essentials of UMTS, The Cambridge Wireless Essentials Series, Cambridge University Press, 2008
4. Dahlman, E., Parkvall, S., and Skold, J.: 4G, LTE-Advanced Pro and The Road to 5G, 3rd Ed., Academic Press, 2016
5. Eberspächer, J., Vögel, H.-J., Bettstetter, C., and Hartmann, C.: GSM - Architecture, Protocols and Services, 3rd Ed., Wiley, 2009
6. Forsberg, D., Horn, G., Moeller, W.-D., and Niemi, V.: LTE Security, 2nd Ed., Wiley, 2013
7. Henry-Labordere, A. and Jonack, V.: SMS and MMS Interworking in Mobile Networks, Artech House, 2004
8. Iedema, M.: Getting Started with OpenBTS - Build Open Source Mobile Networks, O'Reilly Media, Inc., 2015
9. Mehrotra, A.: GSM System Engineering, Artech House, 1997
10. Mouly, M. and Pautet, M.-B.: The GSM System for Mobile Communications, Telecom Publishing, 1992
11. Russel, T.: Signaling System #7 - Implementing SS7-to-Diameter Interfaces, 6th Ed., McGraw-Hill Education, 2014
12. Sauter, M.: From GSM to LTE-Advanced: An Introduction to Mobile Networks and Mobile Broadband, 2nd Ed., Wiley, 2014
13. Yi, S.-J., Chun, S.-D., Lee, Y.-D., Park, S.-J., and Jung, S.-H.: Radio Protocols for LTE and LTE-Advanced, 1st Ed., Wiley, 2012

References - Hacking

14. Wright, J. and Cache, J.: Hacking Exposed Wireless, 3rd Ed., McGraw-Hill Education, 2015
15. Dabrowski, A., Pianta, N., Klepp, T., Mulazzani, M., Weippl, E.: IMSI-Catch Me If You Can: IMSI-Catcher-Catchers, In Proc. of the 30th Annual Computer Security Applications Conference (ACSAC) '14, pp. 246-255, ACM, 2014
16. Engel, T.: Locating Mobile Phones using Signalling System #7, 25C3, Chaos Computer Club, 2008
17. Engel, T.: SMS & all its features, 18C3, Chaos Computer Club, 2001
18. Engel, T.: SS7: Locate. Track. Manipulate., 31C3, Chaos Computer Club, 2014
19. Geovedi, J. and Mende, D.: HITB Labs: Practical Attacks Against 3G/4G Telecommunication Networks, HITB Secconf, Malaysia, 2011
20. Ghigonis, L. and De Oliveira, A.: SS7map : Mapping Vulnerability of the International Mobile Roaming Infrastructure, 31C3, Chaos Computer Club, 2014
21. Golde, N. and Redon, K.: Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunication, NDSS, 2012
22. Golde, N., Redon, K., and Seifert, J.-P.: Let Me Answer That For You: Exploiting Broadcast Information in Cellular Networks, Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13), pp. 33-48, 2013
23. Holtmanns, S., Rao, S.-P., and Oliver, I.: User Location Tracking Attacks for LTE Networks Using the Interworking Functionality, IFIP Networking 2016, pp. 315 - 322, 2016
24. Huang, L.: LTE Redirection - Forcing Targeted LTE Cellphone into Unsafe Network, HITB Secconf, Amsterdam, 2016
25. Hulton, S.-D.: Intercepting GSM Traffic, BlackHat DC, 2008
26. Jover, R.-P.: LTE Security and Protocol Exploits, ShmooCon, January 2016

References - Hacking

27. Kune, D.-F., Koelndorfer, J., Hopper, N., and Kim, Y.: Location Leaks on the GSM Air Interface, ISOC NDSS, 2012
28. Nohl, K. and Munaut, S.: Wideband GSM Sniffing, 27C3, Chaos Computer Club, 2010
29. Nohl, K. and Paget, C.: GSM – SRSLY?, 26C3, Chaos Computer Club, 2009
30. Nohl, K.: Mobile Self-Defense, 31C3, Chaos Computer Club, 2014
31. Perez, D. and Pico, J.: A practical attack against GPRS/EDGE/UMTS/HSPA mobile data communications, BlackHat DC, 2011
32. Sengar, H., Dantu, R., Wijesekera, D., and Jajodia, S.: SS7 Over IP: Signaling Interworking Vulnerabilities, IEEE Network, Vol. 20, Issue 6, , pp. 32-41, 2006
33. Borgaonkar, R., Hirshi, L., Park, S., Shaik, A., Martin, A., and Seifert, J.-P.: New Adventures in Spying 3G & 4G Users: Locate, Track, Monitor, BlackHat USA, Las Vegas, 2017
34. Zheng, Y., Huang, L., Yang, Q., Shan, H., Li, J.: Ghost Telephonist - Link Hijack Exploitations in 4G LTE CS Fallback, BlackHat USA, Las Vegas, 2017