∉ programma

Security in Wireless Cellular systems

(focus limited to authentication, at this stage)

Architecture of wireless cellular systems (abstracted)

2 livelli di "fiducia" diversa

less "trust"

ho SIM
e
TIM,
la sua sicurezza
dipende da TIM

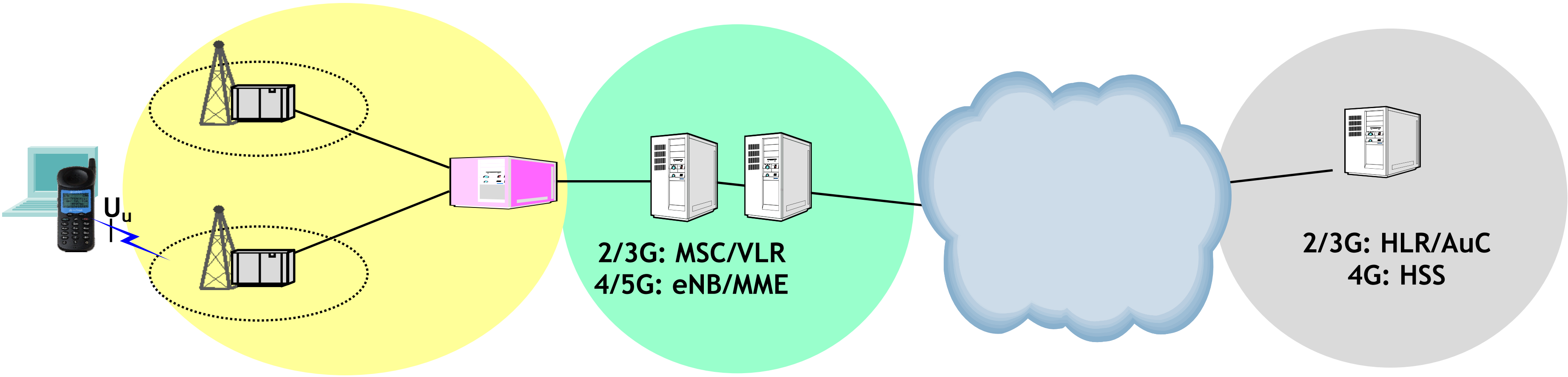
User
Equipment
UE
(telefono)

Radio
access

(NOT my provider)
Serving
network

IP network

(my provider)
Home
network
(TIM)


U_u
2/3G: MSC/VLR
4/5G: eNB/MME
2/3G: HLR/AuC
4G: HSS

Security in 1G

Security?
Nah...!

∅

GSM

Security in 2G

Security? No problem!
Let me do it!!

Can you
Protect us?

COMP-128 Security by obscurity

No mutual auth (Rogue BS)

No core network security

……

Security in 3G

OK, let's be serious now…

Pro to the rescue!!

(fairly) good ciphers - public scrutiny!

Encryption AND (in part) Integrity

Multual authentication

Core network security

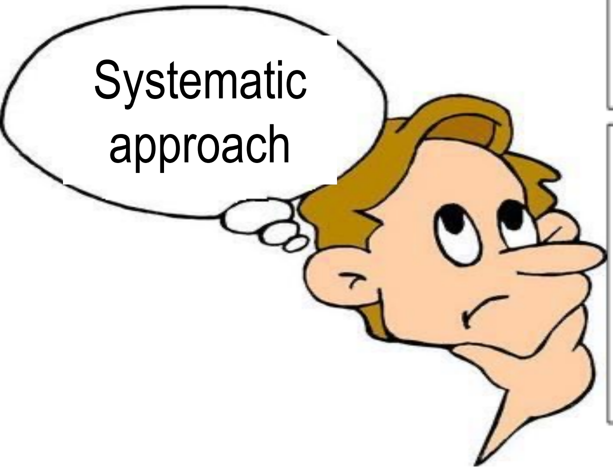
Multiple keys

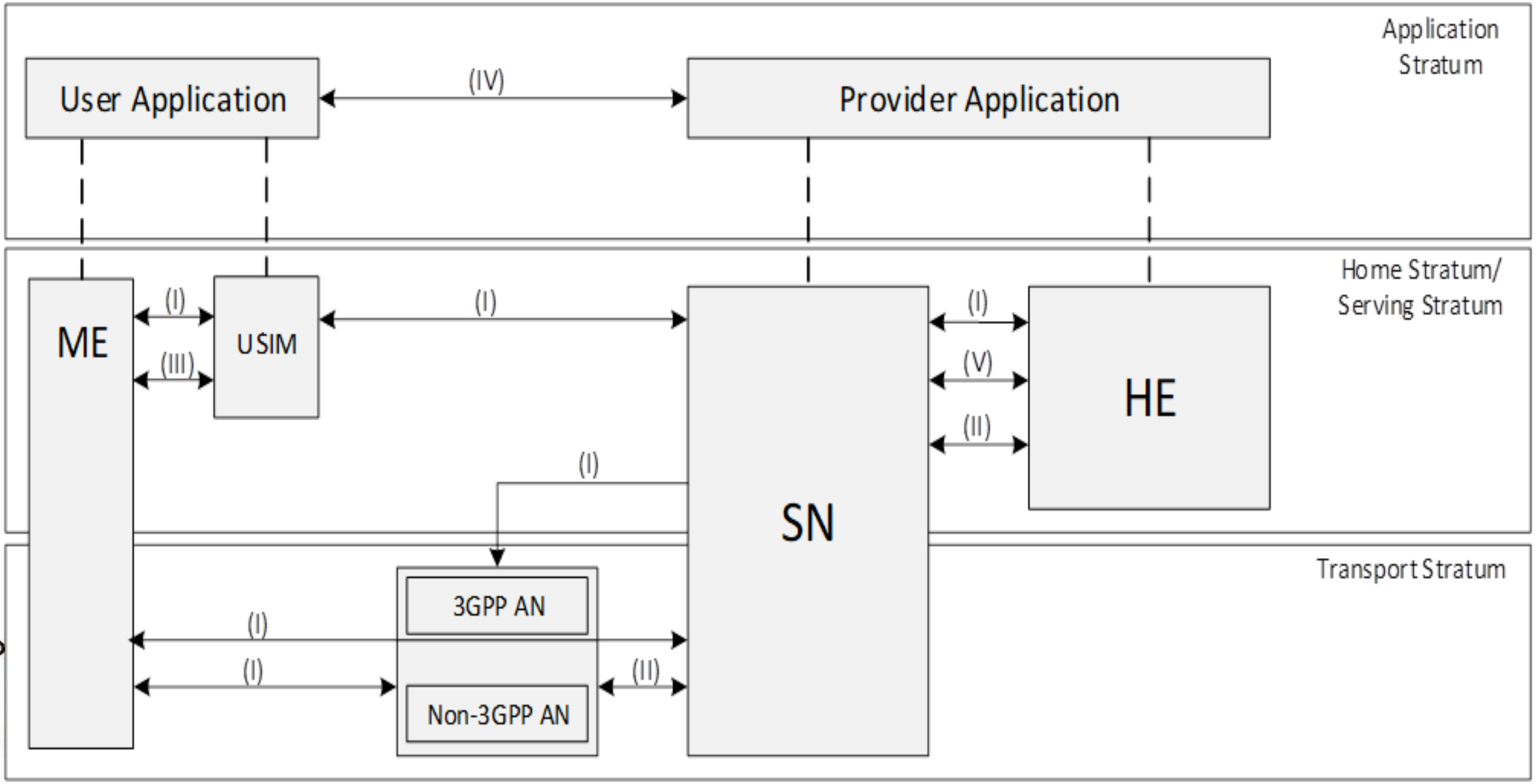
……

Security in 4G

("rinnovamento" generale, per avere un' organizzazione più "chiara", definizione di 'componenti')

Time for a Security architecture!


Systematic approach



Application Stratum
User Application
(IV)
Provider Application
Home Stratum/ Serving Stratum
ME
(I)
(III)
USIM
(I)
SN
(I)
(V)
(II)
HE
(I)
Transport Stratum
3GPP AN
Non-3GPP AN
(I)
(I)
(II)

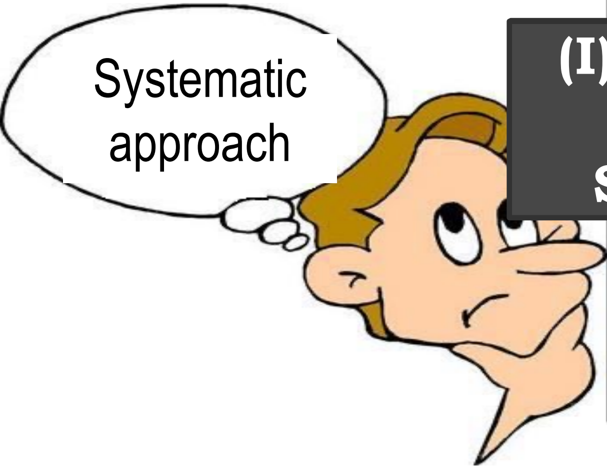
Security in 4G and 5G

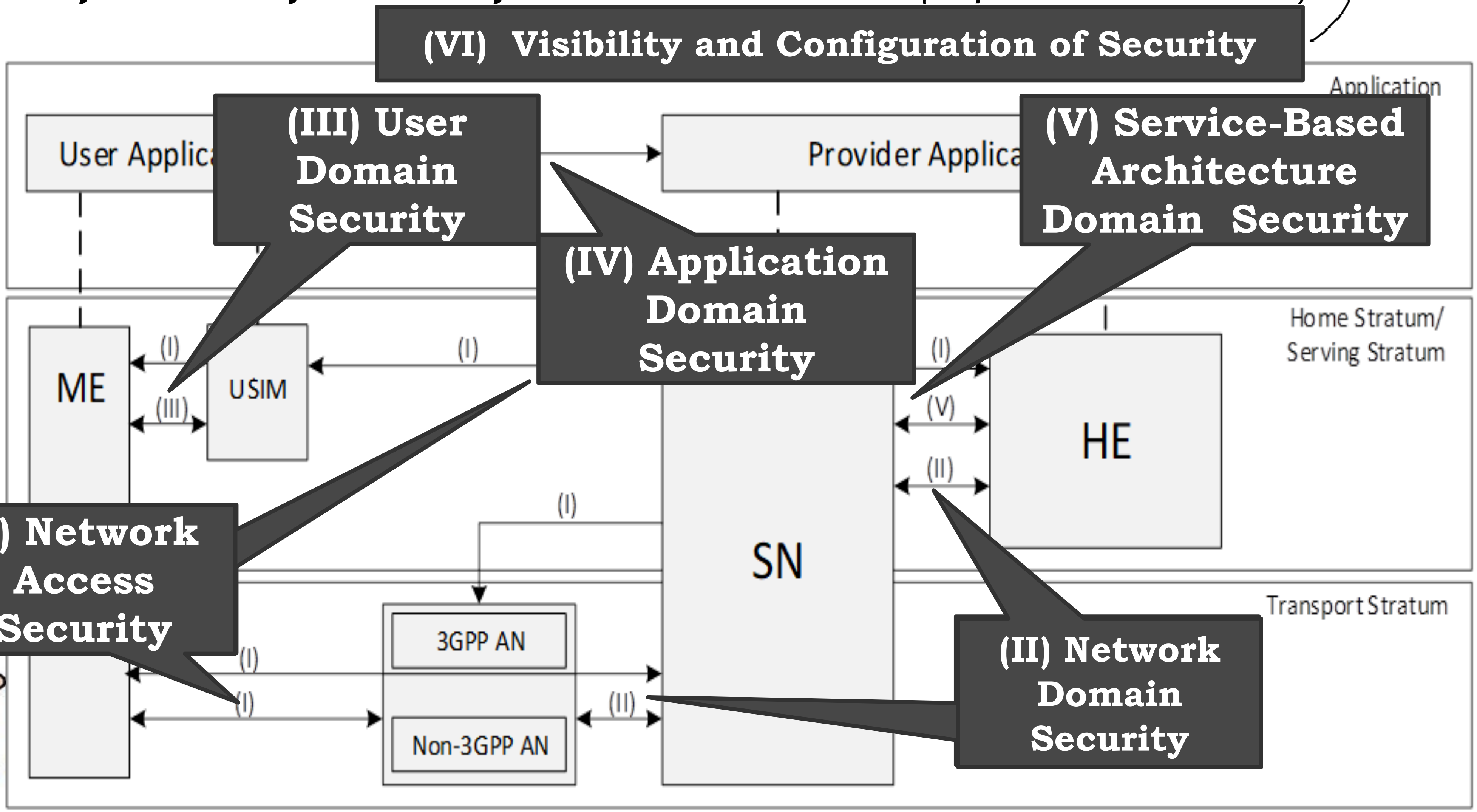
(oggi è 4G⁺, non 5G)

è importante poter distinguere ciò che è protetto da ciò che non lo è!

Actually… this is already the 5G security architecture… to save one slide (couple of differences over 4G)!

Time for a Security architecture!


Systematic approach


(VI) Visibility and Configuration of Security
Application
User Applic
Provider Applica
(III) User Domain Security
(IV) Application Domain Security
(V) Service-Based Architecture Domain Security
Home Stratum/ Serving Stratum
ME
USIM
(I)
(III)
(I)
(I)
(V)
(II)
HE
SN
(I)
Transport Stratum
(I) Network Access Security
3GPP AN
Non-3GPP AN
(I)
(I)
(II)
(II) Network Domain Security

inizialmente Wifi ≠ Rete cellulare, col 5G anche Wifi può usare stessi metodi di autenticazione

AMF: Access Management Function

SEAF: Security Anchor Function

5G Security Architecture -

The 5G «vault» ☺: User data (UDR) and credentials (ARPF) used by UDM authentication/identification functions

Manage Network Access Security
(AMF+SEAF co-implemented)

No security support in DU (deployed in untrusted sites)

Test Framework SCAS for Security Assurance

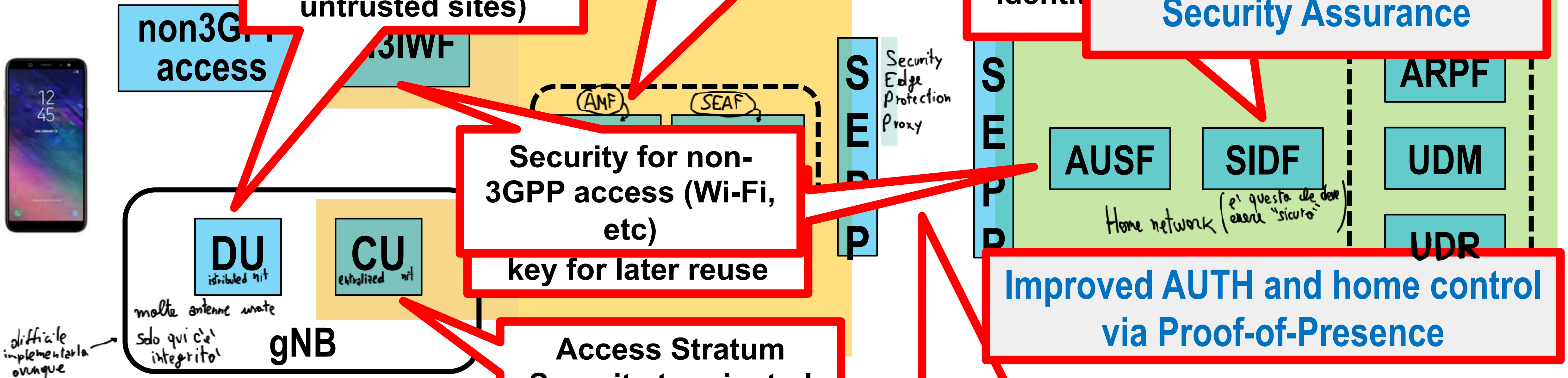
Security for non-3GPP access (Wi-Fi, etc)

key for later reuse

Improved AUTH and home control via Proof-of-Presence

Access Stratum Security terminated at CU (in una cabina)

Security for interconnection traffic


non3GPP access
N3IWF
AMF
SEAF
SEPP
Security Edge Protection Proxy
SEPP
Deco
Identit
AUSF
SIDF
ARPF
UDM
UDR
Home network (è questo che deve essere "sicuro")
DU
distributed unit
CU
centralized unit
molte antenne usate
solo qui c'è integrità
difficile implementarla ovunque
gNB

Improved ke

fe

omains) → + SICURO ← − SICURO

e-siz

G/6G network!

geo-political security debate is in part ill-posed)

L2 message integrity?

Breaking LTE on Layer Two

David Rupprecht
Ruhr-University Bochum
david.rupprecht@rub.de

Katharina Kohls
Ruhr-University Bochum
katharina.kohls@rub.de

Thorsten Holz
Ruhr-University Bochum
thorsten.holz@rub.de

Christina Pöpper
New York University Abu Dhabi
christina.poepper@nyu.edu

DU	
CU	
N3IWF	
SEPP	Security Edge Protection Proxy
ARPF	Auth credential Repository & Processing Fct
UDM	Unified Data Management
UDR	Unified Data Repository

But sys… …mplex

BUT SYSTEMS ARE WAY MORE COMPLEX

5G e' ± sicuro degli altri?

· ∃ tantissimi aspetti da considerare

5G/6G systems' security: A small part of a bigger picture!!

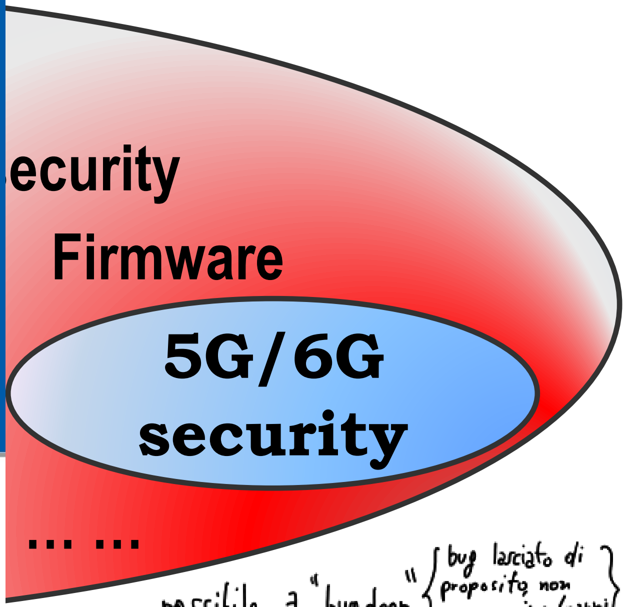
SECURITY IN 5G SPECIFICATIONS

Controls in 3GPP Security Specifications (5G SA)

FEBRUARY 2021

enisa

SECURITY IN 5G SPECIFICATIONS
February 2021



possibile ∃ "bug door" {bug lasciato di proposito, non possono incolparti}

No 5G security if SW/HW implementation is insecure!

(e' come luce o l'acqua)

Critical infrastructure = high tier threats

«They» might *design* vulnerabilities!

SW networks, third party suppliers:

Complexity, increased threat surface!

Too many «optional/should»

In the standard!

Very risky! (you might believe you are secured, while…)