Unlicensed Mobile Access

Infrastruttura e Sicurezza

Guido Bolognesi
guido@kill-9.it

Cosa è?

...e soprattutto, cosa me ne faccio?

- utilizza infrastrutture esistenti (Wi-Fi, Bluetooth) per migliorare il servizio
- migliore copertura al chiuso, ovunque ci sia Internet wireless

UMA? GAN?

- UMA: Unlicensed Mobile Access
- fino ad Aprile 2005, poi
- ratificato dal 3GPP
  (3rd generation partnership project)
- GAN: Generic Access Network

Specifiche in “stage”

- Stage 1: User Requirements
- Stage 2: Architecture
- Stage 3: Protocols

www.umatechnology.org

E per usarlo?

Ci servono almeno tre cose:

- qualcuno che lo supporti lato “client” (UM)
- qualcuno che faccia hardware “server” (UNC/GANC)
- qualcuno che ci venda il primo, l’uso del secondo e della rete (telco)

Deployment

Network Hardware (UNC / GANC)

Deployment

Terminali:

Deployment

Telco:

A quante “G”?

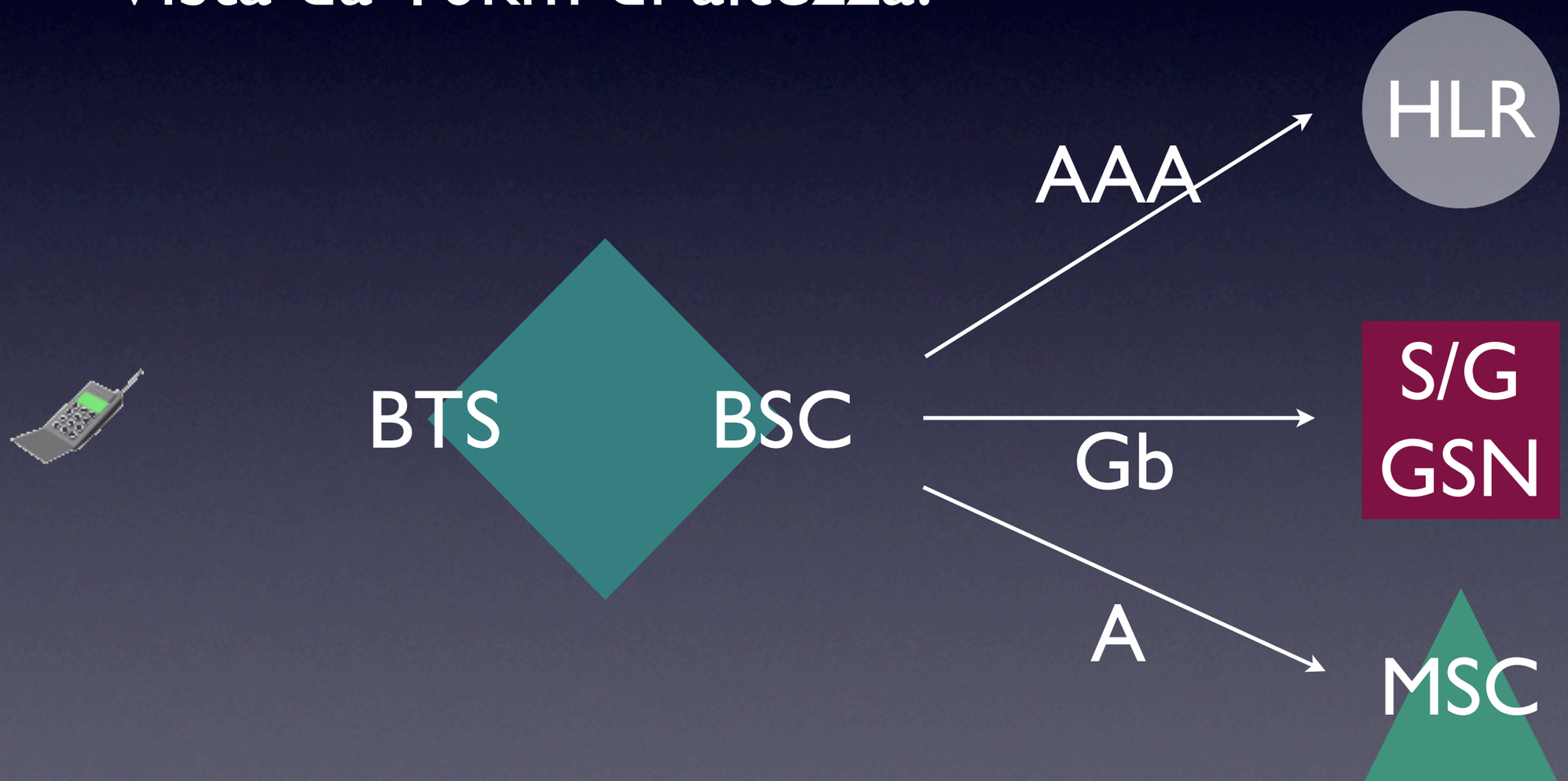
- 2G - GSM
- 2½G - GPRS
- 2¾G – EDGE
- 3G – UMTS, GAN

Filosofia di base

- Deve essere una estensione all'esistente
- Non deve stravolgere architetture
- Deve costare il meno possibile
- Facilitare l'integrazione

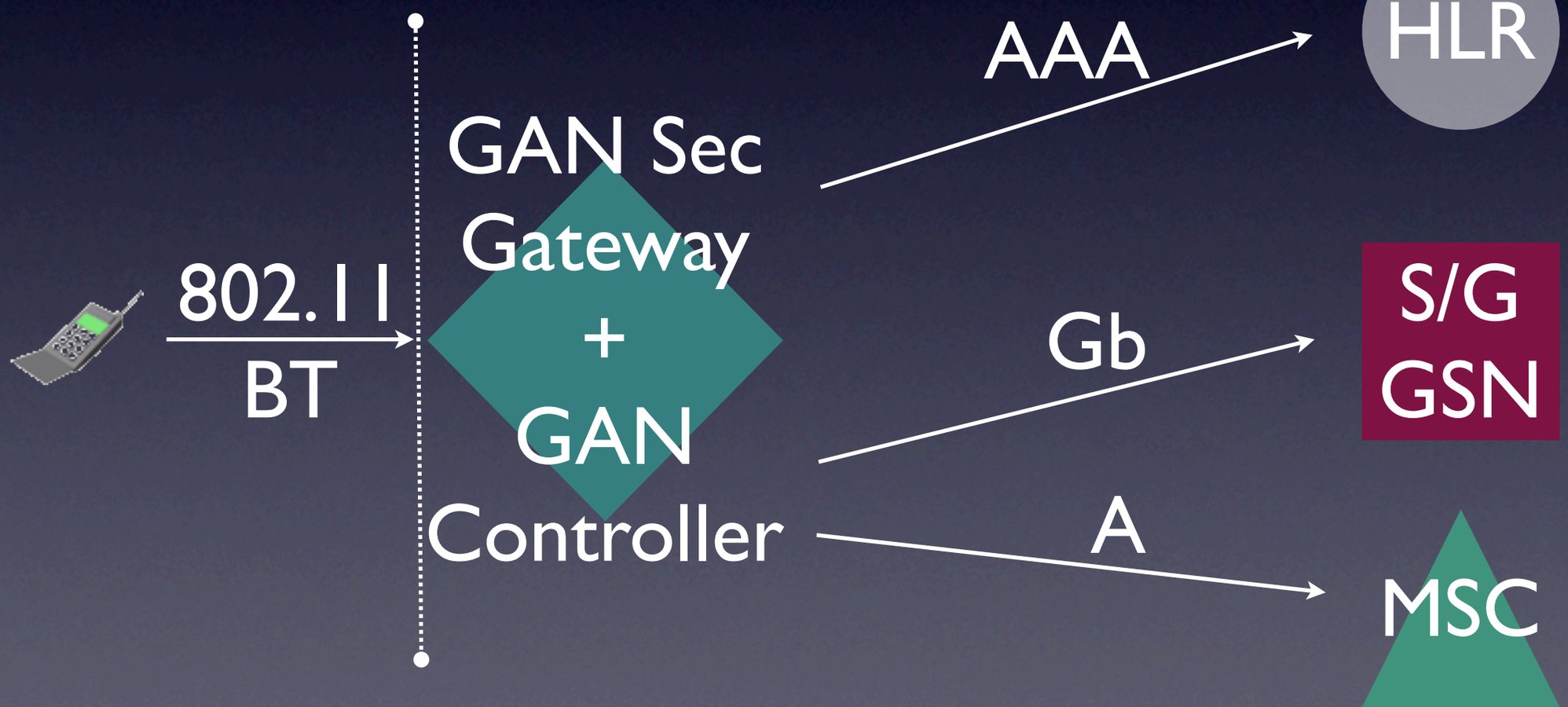
Come funziona GSM

Vista da 10km di altezza:



Come funziona GAN

Vista da 10km di altezza:



Differenze - Radio

- GSM / GPRS funziona su
  - 850MHz / 1900MHz (PCS)
    (N/S America, Canada, Australia, ...)
  - 900MHz (P/E/R-GSM) / 1800MHz (DCS)
    (Europa, UK, Russia, Cina, ...)
- WiFi - BlueTooth sono in 2400MHz

Differenze - Radio

Access point puo` supportare:

- WEP (RC4)
- WPA (TKIP)
- 802.1x (EAPOL)

Differenze - Trasporto

L'UM (chiamiamolo "telefono", ok?) quando trova disponibile un trasporto IP

- si associa
- chiede un IP address
- tenta di terminare un tunnel IPSec sul GAN-SG

IPSec?

- IKEv2 (semplice, rapido)
- 3DES/AES
- NAT-T (rfc3947/8) - ESP over UDP
- EAP-SIM (rfc4186)
- EAP-AKA per USIM (rfc4187)

IPSec? (2)

- il telefono si autentica al GAN-SG
- * il GAN-SG si autentica AL telefono * (certificati X.509)
- il tunnel rimane stabilito anche senza traffico voce
- volendo encryption NULL

E poi?

una volta stabilito il tunnel, il telefono passa

- last known cell ID
- MAC Address dell'AP

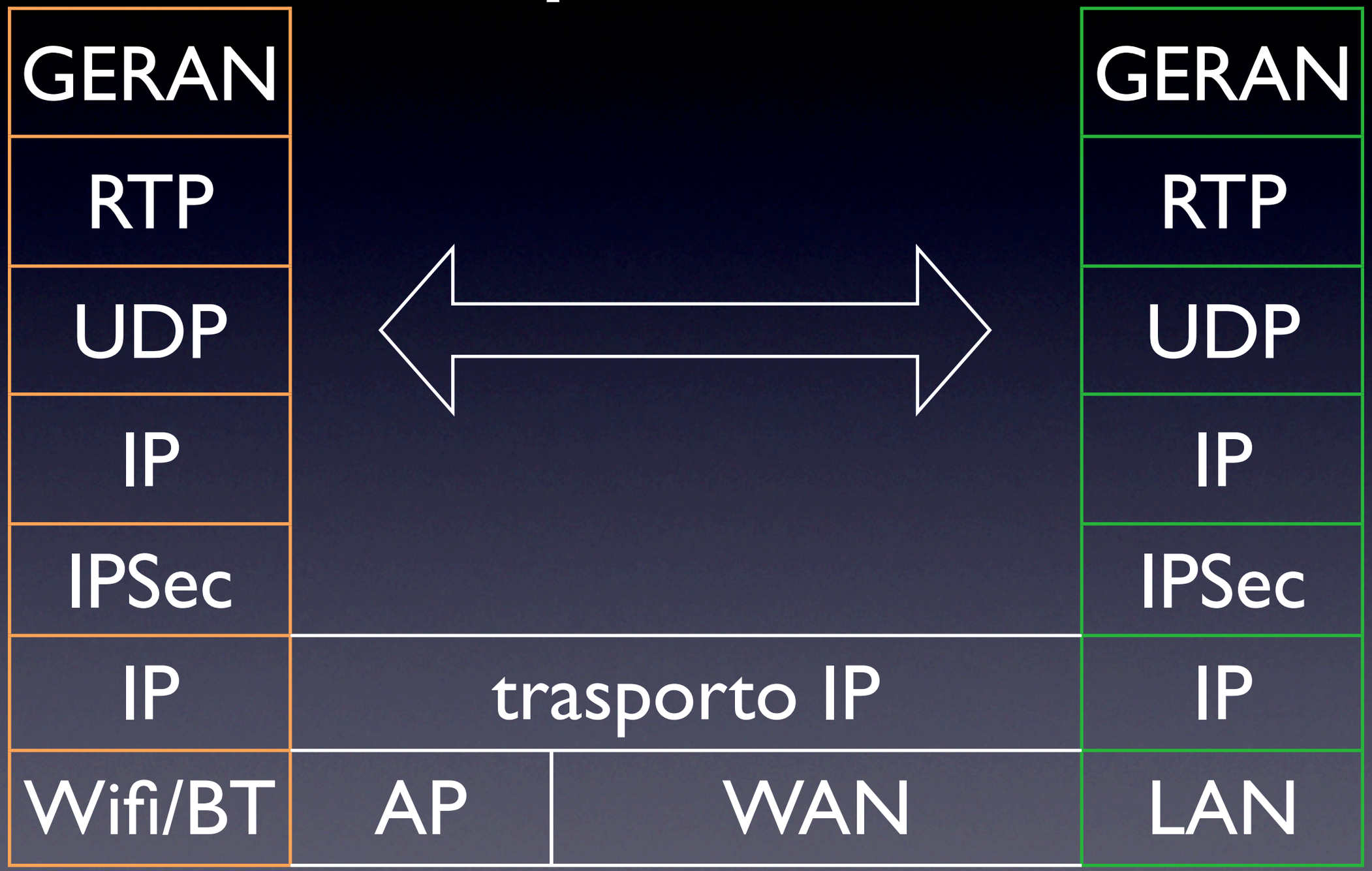
  (*trust client-side*!)

E se non voglio?

Non e` **obbligatorio** fare handover
ne` in un senso, ne` nell'altro :)

- GERAN-only (solo GSM)
- GERAN-preferred
- GAN-preferred
- GAN-only (solo WiFi/BT)

Ricapitolando



"Tell me, Mr. Anderson...

what good is a phone call

if you're unable to speak?

(Agent Smith)

GSM Security

- SIM per l'autenticazione
- Cifratura sul layer radio
- chiavi effimere
- IMEI (non protetto)
- piattaforma CHIUSA

IMEI non utilizzato per protezione - ma antifrode

Difficile per l'utente interagire con GSM

GAN Security?

Due aspetti fondamentali da considerare

- Protezione della infrastruttura (business continuity)
- Protezione dell'utente (frode, privacy, qualita` del servizio)

GAN Security?

- Su GSM non serve IP per telefonare, qui si`
- Su GSM e` “difficile” impersonare una BTS, qui basta un AP
- Su GSM e` “difficile” impersonare un telefono...

Un terminale GAN

- ✓ GERAN
- ✓ RTP
- ✓ UDP
- ✓ IPSec
- ✓ IP
- ✓ WiFi/BT

Attacchi al terminale

- Locali (malware / trojan / ...)
- Remoti
- IPSec usera` una forma di split tunnel?
- Fault injection (pagine malformate, MMS...)
- servizi in ascolto?

Attacchi al terminale

- Il protocollo di GAN prevede che due telefoni (anche sulla stessa wlan) non comunichino mai direttamente (handover)
- ...ma attraverso il trasporto dati fornito dalla telco?

Attacchi al trasporto

- WiFi
  - deauthentication / disassociation
  - WPA?
  - WEP?
- Fake DHCP
- Fake DNS replies
- Fake Access point (MITM?, device abuse?)

Attacchi all'infrastruttura

Ricordiamo che il GANC e` esposto su Internet

- (D)DoS classico (flood)
- (D)DoS con traffico malformato
- DoS prima o durante l'autenticazione - potrebbe impattare anche parte della rete tradizionale (AAA/HLR)

Attacchi all'infrastruttura

- Trasporto AP - GANC
- saturazione risorse verso S/GGSN
- Attacchi alla parte IP della telco, se comuni (DNS)
- attacchi da parte di utenti autenticati!

I have always wished

for my computer

to be as easy to use

as my telephone;

my wish has come true

because I can no longer
figure out

how to use my telephone.

(Bjarne Stroustrup)

GAN e` una tecnologia

- nuova
- non ancora largamente diffusa

ma, come detto

- abbastanza complessa
- da implementare su terminali “poveri”
- aperta ad eventuali “test esterni”

Q&...A?

Thanks & greetings

- Stefano S. , Giovanni A.
- IEEE.org
- sikurezza.org

guido@kill-9.it