VoLTE Security in NG PRDs

Background

A number of different audits and security analysis of various VoLTE networks have been performed.

- See also FSAG WP “VoLTE Security Threats and Attacks”

The observation from the audits were in the following areas from a network perspective (listing the most critical issues):

- IMS Authentication and signalling protection was not used by some operators
- Media allowed to be sent between terminals prior the call has been answered
- Operators allowed direct communication between terminals
- Phone could access internet over IMS APN

In addition, a number of Smartphone issues has been observed:

- It can be observed that not all the Smartphone issues are VoLTE specific. In contrary, many things such as making unwanted (premium) calls and replacing voice media with data, are equally applicable to 2G/3G CS as it is for VoLTE.

VoLTE Security in NG PRDs

Threats and UE countermeasures

Source: VoLTE Security Threats and Attacks

Threats:

- Free Data on signalling bearer
- Overbilling
- Pre-emptive data
- Data DoS
- Muted Voice (DoS)
- Other than voice in RTP
- Spoofing
- Mobile User Battery Drain
- Service Halt

UE countermeasures

Prevent UE from being hackable, even if rooted

- Use embedded SIP stack and not downloadable
- Prevent RTP stack being hackable on the UE (use embedded stack).

Network countermeasures

- Apply correct traffic policies at the P-GW for IMS signalling bearer
- Use of IMS-ALG/IMS-AGW to rate control signalling and filter SIP signalling messages
- Restriction on simultaneous calls within the IMS core
- Dynamic allocation of IP addresses to UEs

VoLTE Security in NG PRDs

- Firewalls at edge of operator's network
- Dedicated bearer is strictly rate controlled
- Use IMS-AKA mutual authentication at IMS registration
- Apply IMS level encryption or integrity protection between P-CSCF and UE
- Use SIP P-Asserted-Id header
- Input data validation to avoid misconfiguration of Network nodes
- Lack of proving/hardening of Network node

Some more details on potential problems and countermeasures:

I- Problem:

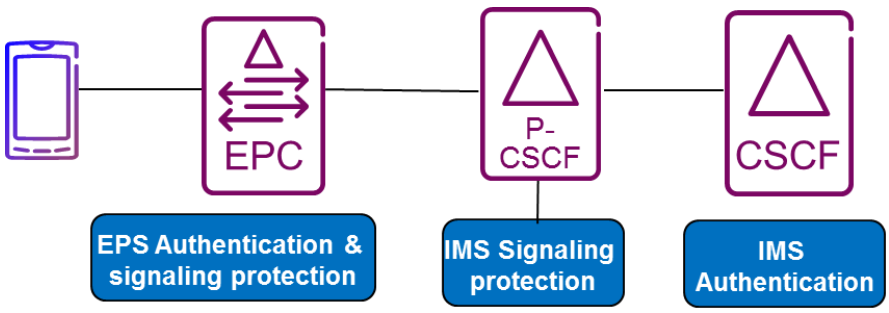
- In some networks, authentication and signaling protection has not been enabled.
- Risk for call spoofing / fraud etc.

Observation:

- GSMA IR.92 mandates IMS AKA with IPsec (with at least integrity protection).

How can this be solved?

- From GSMA perspective, the currently mandated signaling security for VoLTE is considered enough to handle the problems listed

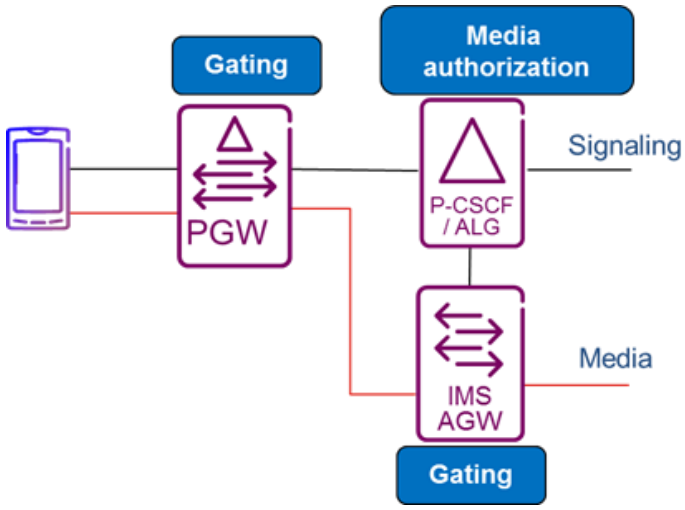


VoLTE Security in NG PRDs

II – Problem

- Media allowed to be sent between terminals prior the call has been answered over IMS signaling bearer
- Operators allowed direct communication between terminals over IMS signaling bearer
- Phone could access internet over IMS signaling bearer
- All of these can result in implications on charging (bypass), fraud, and risk of overloading the IMS signaling bearer (which is the high priority bearer)

- Observation:
  - There may also be implications on visited network in case of IMS Roaming using S8HR if allowing other traffic than SIP (to P-CSCF)
  - GSMA had discussed other issues of allowing e.g., media over the IMS signaling bearer, and agreed CRs preventing media on the IMS signaling bearer.
- How can this be solved?
- :
  - Only allow SIP traffic on IMS signaling bearer, and have strict policing of the dedicated bearers for media (both connectivity and bandwidth)



VoLTE Security in NG PRDs

Conclusion and Recommendation

- GSMA PRD IR.92 has already addressed a number of the more high risk issues identified, including charging and avoiding media on QCI-5.
- In addition, 3GPP has defined the basic framework to allow policing of SIP signaling bearer as well as of the default bearers to avoid that direct communication and unauthorized usage can be done.
- GSMA PRD IR.65 has been updated to describe “Gate Control and Traffic Policing” using the IMS Application Level Gateway (IMS-ALG) and IMS Access Media Gateway (IMS-AGW) covering
  - Policing of SIP signaling bearer and of dedicated bearers, e.g. to avoid direct communication between UEs, and unauthorized usage.
  - Uplink and downlink service level gating control by the PDN GW
  - Ensuring that all traffic via the PDN connection to the IMS well-known APN is only between the PDN-GW and the P-CSCF / IMS-AGW; and
  - Preventing downlink media via the signalling bearer on the PDN connection to the IMS APN.
- Prevent UE from being hackable, even if rooted
- Follow the 3GPP and GSMA guidelines.