Defining the Roads to 5G System Security Architecture

System plethora is not like network, from incarnation to practice

http://www.charisma5g.eu/wp-content/uploads/2016/05/security1.jpg

So finally the Frenzy of 5G Networks and how they will bridge the gaps between different industries and societies seems finally come to materialization .As most of the Tier1 Operators are working to build the Use cases that will support for early launch and market capture catalyst for early movers in the area still the area of 5G security seems gloomy with still lacking much detailed standards being output by ETSI and other SDO's compared to 5G technology itself.

There are many questions in the air need to address both from architecture point of view and from End to End working solution perspective. For example

1. Is 5G security same or conflicting with NV/SDN security?
2. How operators will develop a unified solution that can meet requirements from all industries

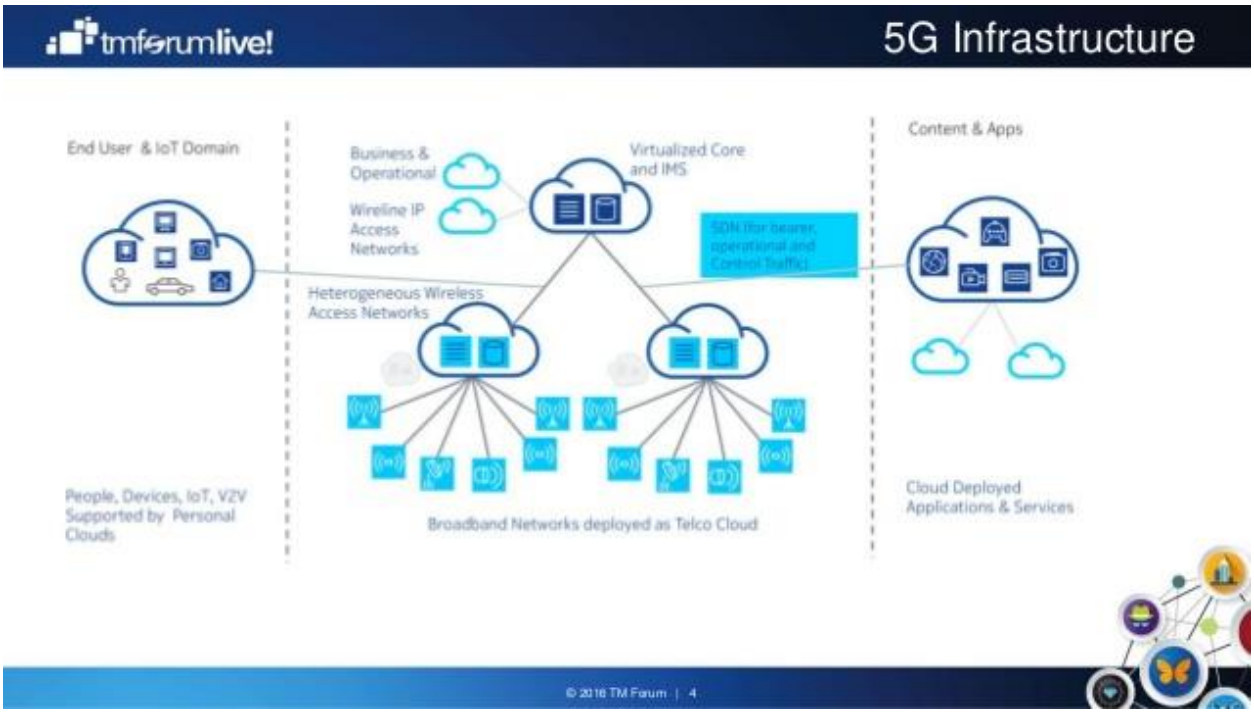
3. If a standard solution exist will it scale? Or finally in 2-3 Years down the road we need to live with lot of customized solution difficult to assure?
4. What about solution relevance in Open source networks with many players around
5. Finally how to imbue Cyber security dilemmas in the 5G Telco Networks.
6. Will End user privacy will be a killer decision in 5G

I think this list gives author enough challenges faced by 5G and verticals and in this paper I shall try to build a high level model to address them in a unified UML model.

In a world where computing is ubiquitous, where a mist of data and devices diffuses into our lives, where that mist becomes inseparable— indistinguishable—from reality, trustworthy computing is but axiomatic. (*David James Marcos /NSA)*

1. **Decentralized Architecture:** The biggest problem that lies ahead is that the Telco Networks are programmed to work not the way around. It actually means they do not predict and obviously do not interpolate to the scale of issues 5G will go to face. This is an architecture issue because like in 3G/4G source of security seems like in Core Network, in NFV/SDN it seem to imbue in the platform but for 5G planning a single control unit to handle and process all data seems impossible. But if we decentralize how to control it. We cannot decentralize without control it and how to control a device we do not trust? I think 5G must model a concept like Block Chain in Banking sector to share security but in a trusted manner and in addition not point of failure due to compromise in a unit or layer

   The understanding of 5G System architecture and how it will influence the present Telco Services migration along with how it can make a thriving eco system is key area of interest for the architect. There are different dimensions like first we need to understand 5G is based on a SBA architecture which requires whole network separated from Infrastructure which makes NFV/SDN almost an inevitable enabler for it . It will allow the deployment of network a slice to support each use case separately. Currently how to model one solution and can it be applicable to customize it for each offering is key area of discussion in ETSI.



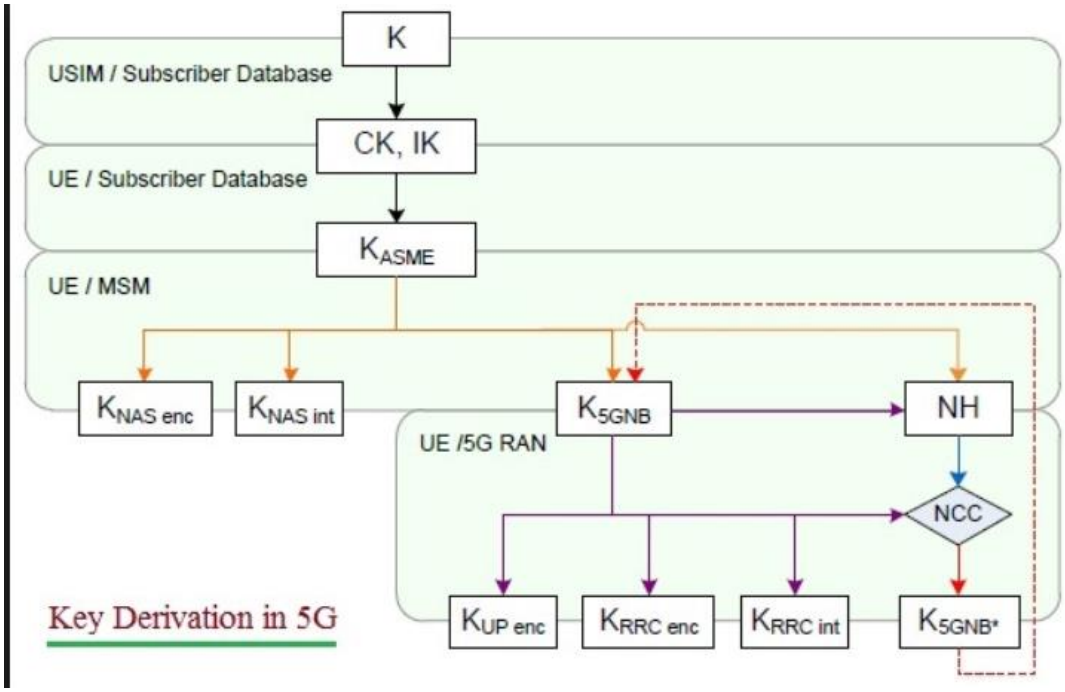
https://www.slideshare.net/ianoliver79/5g-security-in-an-ultraconnected-world

2. **Resource demarcation:** This is a scary topic because IMT2000 already divided network in three domains as per latency use case requirement. The dilemma is that it require different RF resource need to map to a different NFV/SDN DC resource in the Cloud is biggest problem that lies ahead is that the Telco Networks are programmed to work not the way around. It actually means they do not predict and obviously do not interpolate to the scale of issues 5G will go to face. This is an architecture issue because like in 3G/4G source of security seems like in Core Network, in NFV/SDN it seem to imbue in the platform but for 5G planning , so in a broad sense multi RAT for each slice may not be the right approach

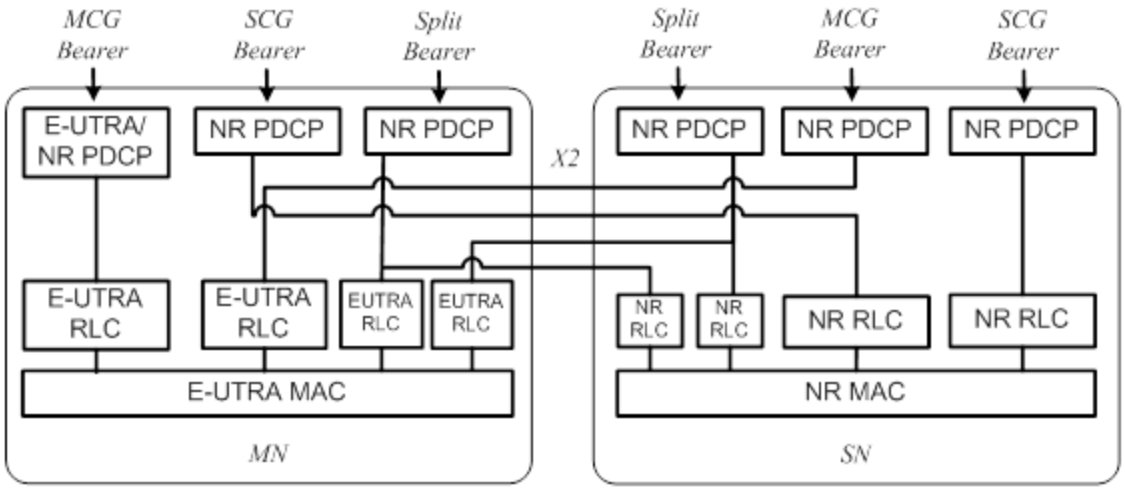
3. **5G Network Threat Model extension:** This host VNF's which are source or sunk of user workload like DNS , AAA ,IPAM is east use case but introducing middle Box VNF like AS , Control plan and Media boxes means we need to introduce Telco Concepts like multihoming , A/S architectures , CSLB and on top of it complex dependence on IT Network redundancy like Bonds ,bridges and it makes the Security a big issue of concern . Obviously introducing a disparate solution means security threat boundary will extend than it is originally supposed to be

4. **5G Security Frame work for 5G SA System:** Well I will not go in to the details here because an expert buddy has just done it perfectly watch Hitchhikers guide here https://www.linkedin.com/pulse/hitchhikers-guide-5g-security-special-edition-junny-song/

   However I do want summarize a bit as follows the 5G Rel15 specifications consider EN-DC (E-UTRAN New Radio Dual Connectivity) as the defacto standard for 5G security at least in 2018 or let's say till H1 2019 reason is obvious because the final Standalone Security specification TS33.501 will freezed in Dec ,2018 http://www.tech-invite.com/3m33/tinv-3gpp-33-501.html#toc . Why EN-DC security is important but same time not very difficult to embrace is that The EN-DC security is based on the existing LTE security specification, TS 33.401 with EN-DC enhancement as shown below



The Good news about EN-DC is that it works almost the same way the LTE-DC runs the concepts of Key Generation, Key Management, Ciphering and Integrity Protection are re-used from LTE – DC concept TS23.501 while the DRB <Data Radio Bearer Security> context is added with regard to 5G Core Network. For EN-DC security, new X2 Information Elements, "SgNB security Key" and "UE Security Capabilities" is newly defined.

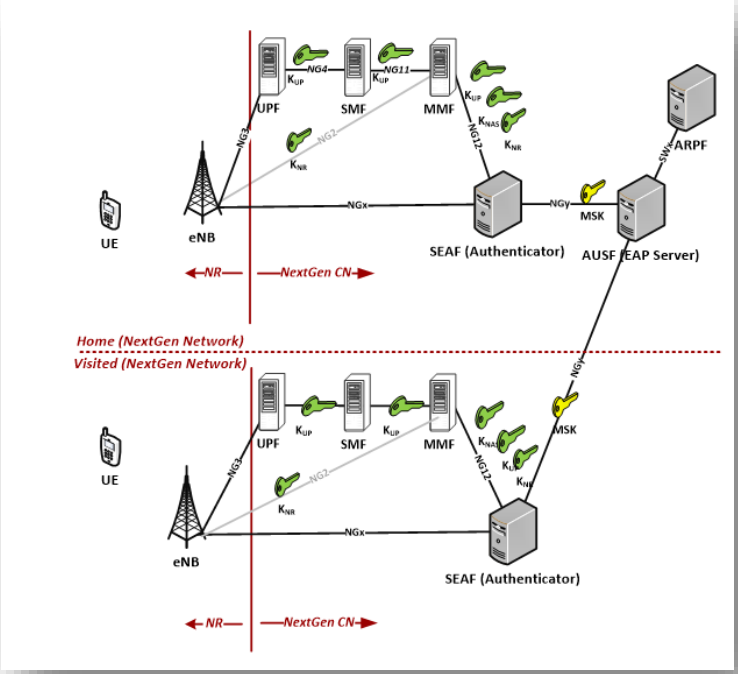


Here shows EN-DC bearers and PDCP termination points from Network side. MN is the master eNB and SN is the secondary gNB. If the PDCP/NR-PDCP is terminated in the MN, LTE security works, on the other hand, if the NR-PDCP is terminated in the SgNB, NR security covers. EEA is redefined as NEA, EIA is also

now called NIA. As you can guess NEA, NIA stands for NR Encryption Algorithm and NR Integrity Algorithm

A good analysis of 5G security protocol can be seen in below

https://www.ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/information-security-group-dam/research/software/5G_lanzenberger.pdf



- In 2018 implement EN-DC architecture almost same as LTE DC
- Use existing USIM but program USIM/UICC it need USIM vendor support
- 5G Success depend on e-SIM trial special for IoT

5. **Assuring NFV/SDN security for 5G:** 5G Network is not about a network but about a system. It involves a plethora of NFV, SDN and Network automation in context of Enablers for 5G to support the future SBA based architecture. These days biggest question we have been talking in the ETSI ISG Security group and in TMforum is actually do Network automation a bliss or curse for security assurance.

6. **Scalable Security solution :** Historically the Telco companies and 3GPP must be credited of building a robust security architecture , it can be reflected in 2G/3G/4G and same is expected in 5G with only problem that scale of 5G devices is billions not millions and a solution to expand only Core network and related Authentication servers is not enough . It require inclusion of distributed security architectures and above all IAM solutions which best use network API exposure to guarantee security. It means in future Security as a service can be possible and that an operator can open the network to guarantee whole system security using best offering from the third party. Anyways it will not change **5G Security Frame work for 5G SA System** as I explained in Point5 of this paper.

   The scalable solution also means that security can be provisioned for each use case in an orchestrated manner something very similar like VNF OLM management where security policy, test criteria all can be customizable as per required use case and SLA.

7. **Security assessment and Verification:** The 5G system is complex and include plethora of many technologies. The security context of IT , Cyber , Information security all are added along with the Telco security but till now even ETSI SA3 have not finalized the detailed scnerio

Sheikh is the Chief Architect Consultant for NFV, SDN and Telco Cloud in Saudi Telecom Company which is the Biggest ICT Operator in Middle East, Always interested in those disruptive technology driving the industry transformation, Author hails from Telco CSP background and since 2013 working on Telco Cloud domain including Amazon, Huawei, Mirantis, VMware, RedHat etc. The comments in my writings are my own and shall not be considered as any relation/binding with those of my employer.

National Security Agency review of Emerging Technologies

3GPP TR.501