Challenges for Evolving Large-Scale Security Architectures

Geir M. Køien

Institute of ICT
Faculty of Engineering and Science
University of Agder, Norway
Email: geir.koien@uia.no

***Abstract*—In this paper, we conduct an informal analysis of challenges that face evolving large-scale security architectures. The 3rd generation partner project (3GPP) mobile systems is our example case and we shall investigate how these systems have evolved and how the security architecture has evolved with the system(s). The 3GPP systems not only represent a truly long-lived system family, but are also a massively successful system family, serving billions of subscribers. What once was an auxiliary voice-based infrastructure has evolved to become a main (and thereby critical) information and communications technology (ICT) infrastructure for billions of people. The 25+ years of system evolution has not all been a linearly planned progression and the overall system is now clearly also a product of its history. Our ultimate goal is to capture some of the essence of security architecture evolution for critical ICT system.**

Keywords–Evolving Security; System Security; Security Architecture; Long-term security planning.

I. INTRODUCTION

In this paper, we carry out a case-study analysis of some of the challenges that evolving large-scale security architectures must meet. The object of our study, the 3GPP systems, has gradually become important, all-encompassing and pervasive on a global scale. The systems have emerged to become a critical ICT infrastructure and this makes the system robustness and security a concern for society-at-large.

A. The 3GPP System Context

The first 3GPP system is the second generation (2G) Global System for Mobile communications (GSM), developed in the mid/late 1980ies. Originally, GSM only featured circuit-switched (CS) services, but was later adapted to also include packet-switched (PS) services through the General Packet Radio Service (GPRS) extension. With the new millennium came the third generation (3G) Universal Mobile Telecommunications System (UMTS), which natively features both CS and PS services. From around 2010 we also have the fourth generation (4G) Long-Term Evolution (LTE) system, which is a broadband PS-only system. LTE is further developed into LTE-Advanced (LTE-A).

1) Principal Parties: From a subscriber perspective, the system can be described with three types of principal parties.

- The Home Public Land Mobile Network (HPLMN)
- The Visited Public Land Mobile Network (VPLMN)
- The subscriber/user (USER)

These parties are legal entities, and the relationships are determined by contractual agreements. A national telecom regulator will also be involved, in addition to external service providers. One may also add intruders to the list. The external service providers usually have little influence on how the networks operate and so we exclude those for further discussion. Likewise, in this context, we do not see a need for including virtual mobile network operators (VMNOs).

2) System Development: The 3GPP system specifications are developed by the 3GPP, but ratification is done by the organizational partners (formal standardization bodies). As with other such groups, the 3GPP is contribution driven. This has an important impact on what is actually being done. The impact is noticeable when it comes to priorities and efforts spent. Early on, when GSM/GPRS was specified, the operators took considerable responsibility and led many of the efforts. Subsequently, the vendors have taken over more and more of this work. The impetus to carry out work is clearly related to the business potential the work has. Unfortunately, investments in security functions seldom look like a good business proposition prior to an incident.

The 3GPP differentiates between *mandatory for implementation* and *mandatory for use*. That is, a feature may be mandatory to be implemented by the vendors if they want compliance with a system release. At the same time, the operators may freely disregard the feature if they want. Other functions may be mandatory both to develop and deploy.

3) License to Operation and Regulatory Requirements: Cellular systems operate in licensed bands and are subject to regulatory requirements. These requirements include support for lawful interception (LI) and emergency call (EC). The last decade we have also had anti-terrorist measures such the EU Data Retention Directive (DRD) [1].

B. Brief Introduction to 3GPP Systems

1) 2G – GSM and GPRS: The GSM and GPRS systems are the 2G systems. It is common to see monikers like 2.5G used for GPRS, and 2.9G used for GPRS with Enhanced Data rates for Global Evolution (EDGE). The main GSM features are mobility, speech and text messaging. GPRS is an overlay system to GSM. It features two additional core network nodes and provides PS support. With EDGE (new codecs) it provides up to 236 kbps data-rate. There is also an "Evolved EDGE" extension on the horizon, with yet higher data-rates. The 2G-based radio access network is called GSM EDGE Radio Access Network (GERAN).

 ISBN: 978-1-61208-376-6

2) 3G – UMTS (incl. High-Speed Packet Access (HSPA)): The UMTS system was finalized in late 1999 and is a combined CS/PS system. It can readily achieve >10 Mbps data-rates (w/max. rates >100 Mbps downlink). The system is a mix of GSM/GPRS technology and protocols and, increasingly, IP-based protocols and technology. The radio access network is called the Universal Terrestrial Radio Access Network (UTRAN).

3) 4G – LTE and LTE-A: The LTE systems are designed as all-IP networks (AIPN) and features true mobile broadband. The core network is fully IP based and there are no CS components to be found. The radio system is highly advanced and provides true broadband services. The radio base-stations, called eNB, are logically mesh connected. There are no longer any controllers in the access network (E-UTRAN). The VPLMN mobility functions are carried out by the mobility management entity (MME) server.

C. Paper Layout

In Section II, we briefly outline the security of the 3GPP systems. In Section III, we attempt to capture some of the triggers for changing the security architecture. Then we proceed in Section IV, with observations regarding successful systems, and for security and cryptography in those systems. We also include observations regarding the typical intruders. In Section V, we try to learn from the lessons and provide some advice. Finally, we sum up our effort and provide some concluding remarks in Section VI.

II. Security in the 3GPP Systems

In this Section, we provide a (necessarily) short description of the main features of the 3GPP security provisions.

A. 2G Security

There is no well-defined security architecture per se in the 2G systems. The main security specification was technical specification (TS) 03.20 "Security-related network functions", which subsequently has been transposed into TS 43.020 [2]. It defines the identity- and location privacy scheme, the entity authentication protocol and the smart-card based security functions. It also outlines the over-the-air cipher function.

1) Background and Requirements: In the voice-only 1G systems one had experienced charging fraud and impersonation fraud. Two distinct types of attacks quickly came into focus: **a)** Eavesdropping was a big problem as the analogue voice channel was unprotected and easy to listen-in on. **b)** Faking the call setup signaling, which was digital, was quite easy and could in principle be done by simply recording a setup sequence and then later replay it. The main priority for a fully digital system a la GSM was therefore to **a)** protect the over-the-air channel against eavesdropping, such that it would no longer be the weakest link, and **b)** provide credible subscriber authentication to avoid impersonation attacks.

2) The 2G Security Architecture: GSM security is based on a physical subscriber identity module (SIM). For portability reasons it was decided to use a smart-card. The SIM comprises both hardware and software functionality, and it contains the authentication and key agreement (AKA) functions (symmetric crypto). The SIM also contains the security credentials, like the permanent subscriber identity (IMSI) and the corresponding 128-bit authentication secret, called K_I in the 2G SIM. Figure 1 outlines the GSM security procedures.

The AKA protocol used is called GSM AKA, and it is a single-pass challenge-response protocol with a signed response (SRES). The challenge is a pseudo-random 128-bit RAND bit-field and the response is the 32-bit SRES element. The challenge-response part is dependent on an "authentication set" forwarding stage, in which the HPLMN forwards the authentication credentials to the VPLMN network. The protocol is run between the SIM and the visited network. This scheme is efficient and allows for fast and simple authentication of the subscriber as well as deriving a session key (the 64-bit K_C). The SIM features the A3 and A8 AKA interfaces, which are only found in the SIM and the home subscriber database (HLR). The original example implementation, called COMP128, is cryptographically broken [3], but still seems to be in use in many markets.

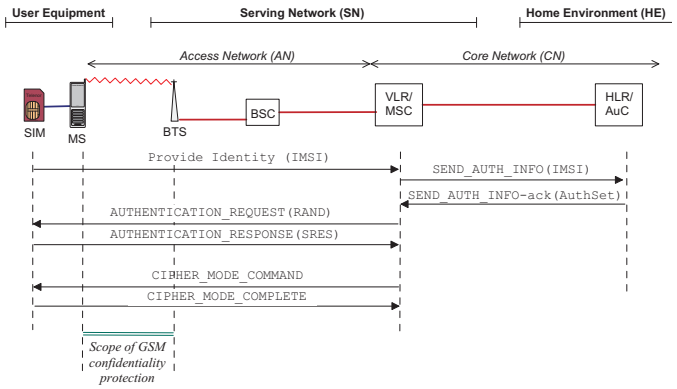

Figure 1: GSM security overview

Over-the-air encryption is by means of the A5 stream cipher family, which is located in the mobile phone and the base tranceiver station (BTS). There are several A5 versions available, but the original A5/1 is still the default and mandatory-to-deploy algorithm. It can easily be broken today by a dedicated attacker [4]. The A5/2 algorithm, which was explicitly designed to be weak (CoCom regulations), is officially deprecated. The A5/3 algorithm, which is based on the 3G KASUMI design, is the current best option for GSM, but rainbow table attacks still work since the algorithm is limited to 64-bit [5]. The A5 family is based around a 64-bit key, expect the new (and not deployed) A5/4 cipher, which is a 128-bit design based on the KASUMI algorithm. In GPRS one uses the GSM AKA protocol as-is, but here one uses the GPRS Encryption Algorithm (GEA) ciphers to protect the asynchronous packet transfers.

3) Omissions and Shortcomings: There are many obvious omissions and shortcomings to GSM security. This is not strange as the 2G systems do not have a security architecture as such; it is more akin to a collections or measures put together without well-defined requirements. The following list (derived in [6]) identifies some of the flaws. Even with all these flaws, the GSM/GPRS system has been a remarkably secure system. However, some 25 years down the line and the shortcomings have become serious liabilities. There are also a number of

 ISBN: 978-1-61208-376-6

implementations issues [7]. The list is not fair with regard to the threats found early on, but it is certainly valid now.

- One-way authentication is utterly inadequate
- Delegated authentication is naive trust-wise
- No inter-operator authentication
- No way to authenticate system nodes
- No uniqueness/freshness to challenges
- Unauthenticated plain-text transfer of security credentials
- Unprotected key transfer
- Missing key binding and too short keys
- Key refresh dependent of re-authentication
- Missing expiry condition on security context
- Weak A3/A8 functions and no key-deriving key structure
- Short A5 key stream cycle and key stream re-use
- Redundant and structured input to A5 (expand-then-encrypt)
- Highly redundant input to A5 (in signaling message)
- Protection coverage/range too short (only MS – BTS)
- Missing integrity protection
- Weak/inadequate identity/location privacy
- No core network control plane (signaling) security features
- No core network user plane protection
- No IP protection (GPRS)
- No mobile phone (MS) platform security

B. 3G Security

1) Background and Requirements: Security in the UMTS system is described briefly in [6, 8] and in considerable depth in [9]. The main security specification is TS 33.102 [10]. One also provided a "Security Objectives and Principles" [11] background document, as well as conducting a threats and requirements analysis [12]. One also introduced Network Domain Security (NDS), which includes IPsec profiles for use with 3GPP systems [13] and a standard set of public-key infrastructure (PKI) protocols and methods [14].

2) The 3G Security Architecture: The UMTS security architecture, depicted in Figure 2, is an important overhaul of the GSM security, yet the underlying system model remains much the same. Amongst the features are:

- New subscriber card (UICC) with security module (USIM)
- Introduction of 128-bit crypto primitives
- Improved two-way AKA algorithm (UMTS AKA)
- Introduction of core network protection (IP protocols)

Sadly, backwards compatibility concerns also dictated that the GSM SIM could still be used, which re-introduces many if not most of the 2G weaknesses.

3) The IP Multimedia Subsystem (IMS): IMS came with UMTS (Rel.5). We do not include IMS in our discussions as it is an optional service-level feature.

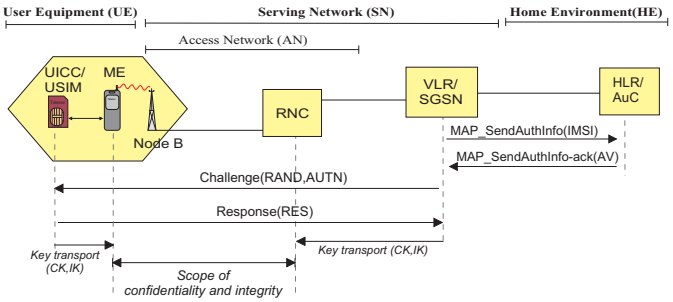

Figure 2: UMTS security

4) Omissions and Shortcomings: The 3G security is substantially better and more future proof than the 2G security, and one really has a security architecture. The architecture is by no means perfect or complete, but it does at least capture the main risks/threats and defines what one wants to protect. Completeness will always be an issue, but in the 3G systems we also have that there sometimes is a considerable mismatch between stated goal and what the mechanisms achieve. A case in point would be the identity/location privacy requirements, which does capture the problem well, but the mechanisms that should provide the necessary services are woefully inadequate. They are however *a)* exactly the same as for the 2G systems and *b)* they are intimately tied to the identity presentation scheme defined in the basic mobility management (MM) protocol machinery (discussed in [6, 15]). Making changes here would have been a major undertaking, and since there was considerable time pressure to complete the 3G standard, improvements to identity/location privacy simply did not happen (there were efforts investigating the possibilities during the Rel.99 design).

Many of the items on the 2G list of omissions and shortcomings are mitigated and resolved, but suffice to say that many of the 2G weaknesses were inherited or permitted through backwards compatibility requirements. Another main problem with 3G security is the limited scope.

C. 4G Security

1) Background and Requirements: The book "LTE Security" [16] is good and thorough introduction. The main security standard for LTE is TS 33.401 [17]. LTE and LTE-A are very similar with respect to the security architecture, which for historical reasons is called the "System Architecture Evolution (SAE)" security architecture. The term Evolved Packet System (EPS) is also used.

The radio access architecture changed significantly with LTE and this triggered large-scale changes to the whole system, including the security architecture. The security requirements were retained more or less as-is. For compatibility reasons and due to time constraints during the design phase, the UMTS AKA protocol was retained as a component of the EPS AKA protocol.

2) The 4G Security Architecture: The LTE security architecture has a lot in common with 3G security, but with some important changes. Amongst the LTE features are:

- UICC/USIM is retained and required

 ISBN: 978-1-61208-376-6

- Introduction of full key-deriving key hierarchy
- Session keys not dependent on re-authentication
- Auth. master key (K_{ASME}) bounded to VPLMN id.
- New session keys for every handover
- Separation of user plane and control plane protection
- Introduction of improved AKA algorithm (EPS AKA)

A welcome change is that backwards compatibility with GSM SIM is prohibited for access to E-UTRAN. UMTS AKA derived security contexts can be used (mapped) to LTE contexts. Figure 3 depicts the EPS key hierarchy, which is very different from the 2G/3G schemes. The new key derivations take place exclusively outside the UICC/USIM. This makes for a significant departure from previous practices.

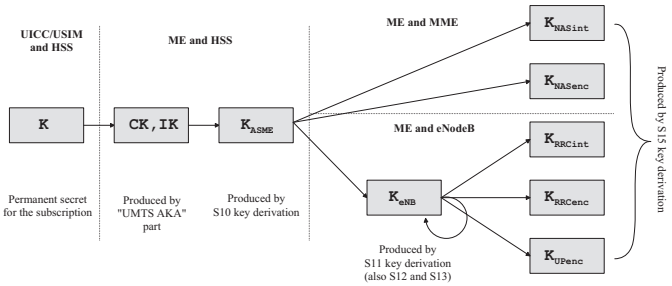

Figure 3: The EPS key hierarchy

3) Omissions and Shortcomings: The list of omissions and shortcoming is shorter for LTE, but there are also new threats. In a world of smart phones, it is obvious that 128-bit crypto on the access link may count for nothing if the mobile phone is infested with malicious Apps. Likewise, the networks are often hybrid systems, and it is common to have base stations that are 2G/3G/4G compliant. With different security levels and common hardware/software, it is clear that strong 4G protection may easily be offset with weak 2G/3G protection. For 4G this is quite important, as the mesh architecture means that all eNBs will be able to reach all other eNBs. Thus, one compromised eNB can reach all other eNBs in the network segment (which may span the entire operator network). It is also clear that many of the nodes, including the base station (BTS/NB/eNB) may be running commodity operating systems (OS). The chosen OS, likely a Linux variant, may be reasonably secure, but even a high-security OS will have weaknesses and must be properly managed to remain secure. Also, introduction of firewalls and intrusion detection systems will be required for these systems now. Server hardening is a must, and even so it is clear that not all attacks can be prevented. This means that prevention alone cannot be a viable future strategy.

The EPS security architecture does require the eNB to be secure, but the specification is not very specific [17]. It also has recommendations on use of firewalls, but the specification is quite vague on this subject too. For a greenfield 4G system, the security may be quite good at what the system provides, but the standard system does not do all it needs to do. Also, it is obvious that even though the user equipment (UE) normally is not owned or controlled by the network operator, the mobile devices must have a minimal level of protection. This is not only to protect the user, which a HPLMN should be interested in anyhow, but also to protect the network as a population of broadband devices could disrupt the access network. Distributed Denial-of-Service (DDoS) attacks would be but one possibility.

D. Architectural Oddities

One puzzling aspect of the 3GPP security architectures is that while identity presentation and entity authentication is fully standardized, there is no authorization mechanisms present. There are of course mechanisms to discriminate subscriber based on the type of subscription, but these schemes are not a feature of the security architecture.

Another aspect to be noted is that the subscriber identity that actually is authenticated, the IMSI, is basically a link layer identifier. Since there is only basic connectivity present at the link layer it may help explain why there never was any built-in authorization scheme in the 3GPP security architecture.

III. Evolving Security Architecture

A. Why Change the Security Architecture?

The short answer is that we need to change the security architecture because some of the premises for the original security architecture have changed. A slightly longer answer would revolve around the following aspects.

B. High-level change triggers

There are many high-level change triggers, amongst others:

- *Changes to the assets of the system*
  This could include changes to the value of the existing assets, inclusion of new assets or removal of assets.
- *Changes in the threats towards the assets*
  This includes assets exposure, new intruders, new intruder capabilities. For new assets it could also include missing or mismatched protection.
- *Changes to the system context*
  The system may initially have played a limited role, but may have evolved into something more.

C. Evolution aspects

Large-scale long-lived systems cannot remain as static objects for long. Instead, they must be dynamic and adapt to changing environments.

- *Evolving Target System*
  If the target system changes, then this will likely affect the security architecture. Still, the nature of the change may be such that it does not trigger a need for updating the security architecture.
- *Evolving Security Architecture - Externally triggered*
  The security architecture may need updates and modifications due to external circumstances, or even completion of planned features that were not initially fully specified. Changes in the threats towards the assets, the exposure of the assets, and the number of users will

 ISBN: 978-1-61208-376-6

also affect the system. It could also involve changing trust-relationships and changes to value of the assets.

- *Evolving Security Architecture - Internally triggered*
  Change in use. The internal circumstances would encompass altered or increased use, which would include changes to the assets of the system.
- *Security Evolution History*
  An evolving system is obviously a product of its history. Decisions taken during the design of GSM still have an impact on LTE. For instance, the basic identity presentation scheme essentially remains the same for LTE as for GSM [18, 19].
- *Societal Impact*
  When a system reaches certain thresholds it will take on a new role. It enters a state of criticality to society and will become an object of regulatory interest. The critical infrastructure (CI) requirements, will focus on system survival and service availability rather than security and privacy for the individual.
- *Privacy*
  Privacy requirements may not have mattered too much for a small system with few users back in the early 1990ties. Today privacy requirements are often mandated by laws and regulations.

IV. Assumptions Regarding Systems, Security and Cryptographic Characteristics

The following set of assumptions not all be true for all systems, but we advocate assuming that they are true.

A. Assumptions about Successful Systems

We assume that when people start to design a system they intend it to be successful. Thus, they must therefore take the above into account in their design. Our high-level assumptions about a successful system:

1) It will outlive its intended lifetime (and design)
2) It will have many more users then originally intended
3) It will need to scale its services cost-effectively
4) It will become highly valuable (many/valuable assets)
5) It will outlive its base technologies
6) It may become a critical system (company, organization)
7) It may become a critical infrastructure (society-at-large)
8) It will spawn unsuccessful branches/features
9) It will have to deal with multi-vendor cases
10) It will need to operate with multiple releases in place
11) It must encompass all of operations & maintenance too
12) It will be subject to regulatory interventions

B. Assumptions about System Security

Our assumptions about a long-lived security architecture:

1) The assets will change (value/number/types)
2) The principal parties will change and multiply
3) The threats will change
4) Trust models will fail (and/or become outdated)
5) Trust will be betrayed
6) Risk evaluations will be outdated
7) The weaknesses, vulnerabilities and exposure will change
8) The intruders will become more powerful and proliferate
9) Attacks will only be better over time
10) There will be security incidents
11) Scalability in security mechanisms will be decisive
12) No single security scheme or approach will be sufficient
13) Effective and efficient defense-in-depth will be needed
14) Pro-active security protection will not be sufficient
15) Re-active security will be very important (detect & respond)
16) Ability to handle large incidents will be required
17) Mitigation and recovery must be supported
18) Pervasive resilience and robustness is required
19) Autonomous sub-system response will become important
20) There will be security architecture omissions
21) There will be security compatibility issues (multi-vendor)
22) There will be security compatibility issues (multi-release)
23) Fixing minor security wholes can take a very long time
24) Fixing the security architecture take years (next generation)
25) Security management will be crucial
26) Security configuration management is crucial
27) Security migration methods should be built-in
28) Privacy will become ever more important

C. Assumptions about Cryptographic Solutions

Our assumptions related to cryptographic solutions:

1) The cryptographic base functions must be future-proof
2) Cryptographic primitives will be broken (or too weak)
3) Key sizes will be changed
4) Security protocols will be broken (or too weak)
5) Cryptographic parameters will need to be negotiated (securely)
6) Cryptographic primitives will need to be revoked
7) Implementations will contain weaknesses
8) Management of cryptographic elements will be crucial

It is clear that the basic boot-strapping fundament must be very solid. This minimal base is what you will depend on if you need to boot-strap new security solution and new cryptographic primitives in the rest of the security architecture. It needs to contain enough to support boot-strapping and it needs to be future-proof. Efficiency is *not* a main priority here.

D. The Scalability War

The classical Dolev-Yao Intruder (DYI) is not the most realistic intruder [20]. Real intruder will use any available means (subversion, physical intrusion, tricking the principals), ultimately being as powerful as a DYI. There is a reasonably body of papers detailing various intruder model, but suffice to say that a modern CI system must be able to handle **all** types of intruders. And many of them! This essentially means that the system *must* have efficient as well as effective protection, and that mechanisms that do not scale well, compared to intruder capabilities, will be doomed to fail in the long run.

Our assumptions related to scalability and efficiency:

1) Security scalability will be a major concern
2) Efficiency is highly important
3) Effectiveness is imperative for core mechanism
4) Auxiliary defense-in-depth solution are needed
5) Avoid specific-attack measures if at all possible
6) Security management must scale well

Assumption three and four are apparently somewhat at odds, but in the end assumption three can be supported given that these means are complementary and cost-effective. See

 ISBN: 978-1-61208-376-6

also considerations about the economy of attacks and defenses outlined in [21], This indicates that for broad sweeping attacks, even quite weak mechanisms may successfully thwart the attacks. Measures that are only effective for one specific attack should be avoided.

E. Other Concerns

1) Passive Regulatory Authorities: One main concern is that the regulatory authorities generally are quite passive with regard to security requirements. This is apparent for the cellular system and regulations concerning the operators. The 3GPP standards are by no means perfect or complete, but it is still the case that many of the standardized and recommended security mechanisms are not deployed in the networks. The regulatory authorities are generally more reactive than proactive, unless they have a clear political mandate to be stringent. One should also be concerned about regulations just subsequent to a major public incident, since it is likely that the urge to "do something" is strong while it is also likely that one focuses narrowly on details. One may end up with *security theater*, as coined by Schneier [22].

Part of this problem is a that one sometimes ends up with a lot of attention to correct and strengthen unimportant features. To do something right is not enough, one must also do the right thing.

2) False Security: Security theater may over time develop into the more elaborate *cargo cult security* type of deception. Then the main functions and mechanisms may all be there (or mimicked closely), but with some vital part missing or done completely wrong. Cargo cultism is defined by "perfect form", but it simply does not work as intended. Feynman has an amusing description of "cargo cult science" that nicely illustrates the principles [23]. Since security can be very difficult to get right and to verify, cargo cult security may look like the real deal.

3) Security Testing and Security Configuration: In [7] the authors clearly also demonstrate that not only is not all security options exercises, but that, unsurprisingly, there are implementation weaknesses and vulnerabilities. The ASMONIA project provides many more examples of weakness, vulnerabilities and risks facing a mobile system [24]. The ASMONIA project published a lot of useful documents for operators wanting to improve their security level. The documents also include advice and methods for how to test the security. The EU body ENISA provides a lot of useful security-related input, but generally have no mandate to impose security [25]. When it comes to IP network security and server security there is a large body of standards and methods for how to design and test security hardening [26–29]. There are also various checklists available [30].

V. Lessons Learned

A. Verify Assumptions

One must verify assumption about the system and the security periodically or when there are substantial changes to the system. That is, an audit is called for to verify assumptions about the assets, the principal entities, trust relationships etc. Security policies will be affected by changes to these assumptions. This is a process oriented task that must take place both for the design phase and for the deployed system(s).

B. Rock Solid Bootstrapping Security

There needs to be a rock solid fundament that will be secure for the foreseeable future. The smart-card has served this purpose in the 3GPP systems on the subscriber side. The smart-card is not tamper-proof, but it has successfully served as a high-trust platform.

C. Planned Deprecations

A scalable and evolving system must be able to handle deprecation of almost all cryptographic algorithm, security protocols and security services. The deprecation, needless to say, must be conducted in a secure manner. Backwards compatibility requirements and fallback solutions must be handled in a secure way.

D. Negotiable and Adaptable

Given that one must plan for deprecation of security features/services, one must also plan how to negotiate new features/services. This feature must be built-in and have high assurance. Adaptation may be necessary to account for local requirements, but is vital that adaptations must be fully compliant with a well-defined security policy.

E. Proactive & Reactive Security

Basic security functionality to identify and authenticate principals and entities is necessary, but not sufficient. Adding authorization, protected storage and protect communication is also necessary, but still not sufficient. More may be added, but in the end it is impossible to fully secure the system. This means that one must handle and deal with incidents. There is therefore a clear need for intrusion detection and response systems, to deploy firewalls, anti-virus protection, secure backups, secure audit trails etc. The reactive measures must be included in the overall system security plans and subject to revisions as need be.

F. Stability, Resilience and Recovery

System integrity is imperative to ensure a stable and resilient system. System integrity is a system-level characteristic and does not preclude partial or local failures. What is imperative is to prevent the failures to scale. Failures, whether man-made intentional or unintentional, cannot entirely be prevented. Procedures that support mitigation and recovery must be an integral part of the overall system security plan.

G. Configuration Management

Proper planned configuration management, which must include security functionality, is an absolute necessity.

H. Privacy Matters

Privacy is one feature that must be accounted for in all systems that include human users or any kind of data pertaining to humans. This must be planned for from the design phase and handled in all phases of system deployment.

 ISBN: 978-1-61208-376-6

VI. Concluding Remarks

The results in this paper cannot be said to be fully supported by the evidence provided in this paper (or in the referenced papers). They are neither rigorous nor complete. This is to be expected for such a complex issue. Thus, while the results may be valid and true, they will hardly be complete and not always necessary either. That is, the usual "necessary and sufficient" conditions are not really there. Still, experience and empirical evidence should not be discounted, and we advocate that the lessons learned are taken into account, not as mathematical axioms, but inputs to be considered. We therefore recommend that scalable evolving security architectures should be designed with these assumption as background.

In this paper, we have outlined the 3GPP security architecture as it has evolved over more than 25 years. From being an auxiliary service for the few, it has grown to literally cater to billions of subscribers, and the number and types of services provided has changed dramatically over the years. The use-patterns of these systems has changed as well. All in all, there has been a complete transformation of almost all aspects of these systems. During this process, the security architecture has evolved with the system and the changing system context, though not without some noticeable failures and a growing number of security problems.

We have argued that to achieve scalable security architectures that are able to evolve over time, one needs to take into account the fact that almost all assumption one initially had will become false or moot. This means that adaptability and ability to support changes is crucial. This is important in a world where the internet-of-things (IoT) landslide is about to happen and where the systems will be ever more important.

In the wake of the Snowdon revelations, it is also clear that cyber-security is under constant pressure, and while we do not want to over-state the Snowdon case per se, it should be clear that the cyber-war methods will (over time) become available to many organizations and individuals. So we need to learn how to cope with this and do so fast.

References

[1] European Parliament/European Council, "Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC," EU, Directive 24/EC, 2006.

[2] 3GPP, TS 43.020, "Security related network functions," 3GPP, France, TS 43.020 (2G), 2014.

[3] J. R. Rao, P. Rohatgi, H. Scherzer, and S. Tinguely, "Partitioning attacks: or how to rapidly clone some gsm cards," in Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on. IEEE, 2002, pp. 31–41.

[4] M. Kalenderi, D. Pnevmatikatos, I. Papaefstathiou, and C. Manifavas, "Breaking the gsm a5/1 cryptography algorithm with rainbow tables and high-end fpgas," in Field Programmable Logic and Applications (FPL), 2012 22nd International Conference on. IEEE, 2012, pp. 747–753.

[5] P. Papantonakis, D. Pnevmatikatos, I. Papaefstathiou, and C. Manifavas, "Fast, fpga-based rainbow table creation for attacking encrypted mobile communications," in Field Programmable Logic and Applications (FPL), 2013 23rd International Conference on. IEEE, 2013, pp. 1–6.

[6] G. M. Køien, Entity authentication and personal privacy in future cellular systems. River Publishers, 2009, vol. 2.

[7] F. van den Broek, B. Hond, and A. Cedillo Torres, "Security Testing of GSM Implementations," in Engineering Secure Software and Systems, ser. Lecture Notes in Computer Science, J. Jürjens, F. Piessens, and N. Bielova, Eds. Springer International Publishing, 2014, vol. 8364, pp. 179–195.

[8] G. M. Køien, "An introduction to access security in UMTS," Wireless Communications, IEEE, vol. 11, no. 1, Feb 2004, pp. 8–18.

[9] V. Niemi and K. Nyberg, UMTS Security. John Wiley & Sons, 2003.

[10] 3GPP, TS 33.102, "3G Security; Security architecture," 3GPP, France, TS 33.102 (3G), 2014.

[11] 3GPP, TS 33.120, "Security Objectives and Principles," 3GPP, France, TS 33.120 (3G), 2001.

[12] 3GPP, TS 21.133, "3G security; Security threats and requirements," 3GPP, France, TS 21.133 (3G), 2001.

[13] 3GPP, TS 33.210, "3G security; Network Domain Security (NDS); IP network layer security," 3GPP, France, TS 33.210 (NDS/IP), 2012.

[14] 3GPP, TS 33.310, "Network Domain Security (NDS); Authentication Framework (AF)," 3GPP, France, TS 33.310 (NDS/AF), 2014.

[15] G. M. Køien, "Privacy enhanced cellular access security," in Proceedings of the 4th ACM workshop on Wireless security. ACM, 2005, pp. 57–66.

[16] D. Forsberg, G. Horn, W.-D. Moeller, and V. Niemi, LTE security. John Wiley & Sons, 2012, vol. 1.

[17] 3GPP, TS 33.401, "3GPP System Architecture Evolution (SAE); Security architecture," 3GPP, France, TS 33.401 (3G), 2014.

[18] G. M. Køien, "Privacy enhanced mutual authentication in LTE," in Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on. IEEE, 2013, pp. 614–621.

[19] G. Køien, "Mutual entity authentication for LTE," in Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International. IEEE, 2011, pp. 689–694.

[20] D. Dolev and A. C. Yao, "On the Security of Public-Key Protocols," IEEE Transactions on Information Theory, vol. 29, no. 2, 3 1983, pp. 198–208.

[21] D. Florêncio and C. Herley, "Where do all the attacks go?" in Economics of Information Security and Privacy III. Springer, 2013, pp. 13–33.

[22] B. Schneier, "Beyond fear," Copernicus Book, New York, 2003.

[23] R. P. Feynman, "Cargo cult science," in Surely You're Joking, Mr. Feynman, 1st ed. W. W. Norton, 1985, Originally a 1974 Caltech commencement address.

[24] "The ASMONIA project," See www.asmonia.de, 2014.

[25] "ENISA - European Union Agency for Network and Information Security," See www.enisa.europa.eu/, 2014.

[26] K. Scarfone, W. Jansen, and M. Tracy, "Guide to General Server Security," NIST, Gaithersburg, MD 20899-8930, Special Publication 800-123, 2008.

[27] Z. Anwar, M. Montanari, A. Gutierrez, and R. H. Campbell, "Budget constrained optimal security hardening of control networks for critical cyber-infrastructures," International Journal of Critical Infrastructure Protection, vol. 2, no. 1, 2009, pp. 13–25.

[28] R. Dewri, I. Ray, N. Poolsappasit, and D. Whitley, "Optimal security hardening on attack tree models of networks: a cost-benefit analysis," International Journal of Information Security, vol. 11, no. 3, 2012, pp. 167–188.

[29] R. Dewri, N. Poolsappasit, I. Ray, and D. Whitley, "Optimal security hardening using multi-objective optimization on attack tree models of networks," in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 204–213.

[30] NIST, "Security configuration checklists program," See http://csrc.nist.gov/groups/SNS/checklists/, 2014.

 ISBN: 978-1-61208-376-6