Challenges of Security Assurance Standardization in ICT

Marcus Wong

Huawei Technologies (USA), Bridgewater, New Jersey, USA, mwong@huawei.com

Received: September 5, 2014;
Accepted: November 10, 2014

Abstract

The explosion of mobile broadband growth has created a greater demand on the operators and vendors working together to place more and more telecom gears into wireless networks at a record pace to satisfy the users' insatiable appetite for mobile data. The desire for undiminished security coupled with more sophisticated attacks in an ICT world where the traditionally closed telecom networks are going through a change of open architecture, open platform, and virtualization, the entire telecommunication community has taken a proactive approach to re-evaluate the security assurance process to ensure that the products are as secure as ever. The operators and the vendors have come together under the roof of 3GPP to create such a security assurance standards to be applied, recognized, and accepted in all areas for which 3GPP network products are sold and marketed. This paper will examine the many issues, hurdles, and challenges of the standardization of security assurance.

Keywords: Security Assurance, 3GPP, standards.

1 Introduction

The market needs and lacking of a security assurance for telecommunication sector coupled with the explosion of mobile broadband growth have made the condition ripe to start putting the focus on an industry-wide security

Journal of ICT, Vol. 2, 187–200.
doi: 10.13052/jicts2245-800X.226

assurance process for telecommunication products. Attacks have become more and more sophisticated; attackers have become more and more intelligent; and the attack tools have become more and more advanced. At the same time, the wireless networks have become more and more open in terms of architecture and visibility. The combination of these events has called upon the entire telecommunication community to re-evaluate the approach and the process to ensure that the products are more and more secure. This leads to an international security assurance standards for the wireless telecom product so that one process can be applied to every market, every product and for every stakeholder. As a result, expert members in the Third Generation Partnership Program (3GPP) security group have committed themselves to create such a security assurance process.

2 The Challenges

Riding the wave of 3G, 4G and the forthcoming 5G, operators have introduced a plethora of new services that not only rely on new products and features to be developed quicker than ever before but also that these products and features are rolled out to market place at a record pace. The users and the operators still demand and expect the same undiminished security values they have become accustomed to and offered by the vendors as the network security landscape and threat models are constantly evolving. The challenges are real. The interests are high for customers, governments, and vendors alike to ensure that the telecommunication products and the networks are more secure than ever.

2.1 Security Challenges

Today's telecommunication networks have become more open, and at the same time more sophisticated and more intelligent. We are relying on the communication networks and connectivity more than ever. Information, tools, and knowledge about networks and network security are readily available to anyone who has the desire and determination to learn about anything or gain a great deal from it, including those who attempt to seek financial gains or those who seek to create damage and disruption. When the information and knowledge are in the wrong hands, along with the more powerful machines and tools of today (e.g. PCs, tablets, smart phones, etc.), it is becoming increasingly evident that malicious misuse of the learned or gained knowledge can lead to serious disruption of communication networks and

network services. Being able to communicate anytime and anywhere also means that attackers are able to launch attacks anytime and anywhere. The potential losses can be great in terms of productivity losses, financial losses and information losses. It has become vitally important to keep the communication systems and network more secure than ever. Ensuring the security of systems and networks has become one of the toughest challenges for the entire telecom ecosystem in the foreseeable future. Some of these challenges include:

- Identity management
- Virus, malware and botnets
- Internet-based attacks
- Industrial espionage and sabotage
- Privacy laws and regulations
- Awareness, education, and training

These challenges also bring along an assortment of many potential threats and risks to the products, networks, and services:

Figure 1 Threat and attack model

- Physical tampering
- Denial of service and attacks on the networks
- Compromise of authentication credentials
- Man-in-the-middle attacks on the networks
- Intercepting and modification of user's data
- Rogue network equipment
- Mis-configuration
- Radio resource tampering
- Hackers

2.2 Market Place Challenges

In addition to building secure products, meeting these challenges also requires that a global security assurance process to be developed so that the security of the products can be demonstrated in a systematic approach. The needs for such security assurance are also driven by the market for such a transparent process, for instances in the Indian market and other markets around many parts of the world. Making claims that a particular product is either secure or insecure without substantiating the claims is simply irresponsible. From the operator's perspective, they demand that the products they place in their networks are secure and are developed with the highest integrity as they not only have their reputation to protect, the user's security and privacy to protect, but also the laws and regulations to comply with as there are numerous such regional and national laws and regulations regarding the protection of user data and user privacy. From the vendor's perspective, they want to ensure that not only the operator's requirements are met and that their products are secure, but also that they can keep up with the demand for faster feature and product development without compromise in security as they too, have a reputation to protect. At the same time, the vendors also want an environment to ensure that their products can be used in all markets of the globe without the need to customize and certify the products for each market. To reach this goal, the operators and the vendors have come together in the telecommunication industry create such a security assurance standards to be applied, recognized, and accepted in all areas for which network products are sold and marketed. Bottom line is that the telecommunication industry needs such a security assurance process so that every stakeholder can benefit from it. Products built to the security assurance specification and having gone through the security assurance process will be able to withstand any unsubstantiated claims about the security of the products.

2.3 Regulatory Challenges

Regulators have spoken loudly and clearly with laws regulations put in place in various regions around the world covering data security, user privacy, and with strict requirements for telecommunication products when the systems and networks provide vital services to serve the government and regulator communities in addition to serve the general public. Some examples of these regulations and directives include EU's Data Protection Directive, UK's Data Protection Act, Canada's Privacy Act, Japan's Personal Information Privacy, China's Provisions for Administration of Information Service, so on and so forth. The list goes on and on. It should be noted that the varying regulators should not overly burden the industry with unnecessary and impractical rules and regulations that are difficult to harmonize and thereby creating a barrier to inhibit innovation.

3 Requirements of Security Assurance

Meeting the challenges head-on requires that the security assurance process must be transparent, collaborative, global, standards-based, and practical to be effective. Requirements from operators, vendors, and regulators need to be taken into account fully to build up the security assurance process. Market needs drive products and services, which in turn drive requirements on the vendors, operators and regulators. The market place is unyieldingly unwilling to compromise even in the face of increased threats and risks presented. Regulatory requirements are also an important and necessary component of the security assurance process. All and all, it requires the best of vendors, operators, and regulators to come together to define ways of ensuring the security of products, systems, networks, and the users. The network operators also have requirements and demand the best of vendors and suppliers not only to build the best and most secure products, but also to provide indisputable evidence, in the form of assurance and certification. The operators have moral, legal, and financial requirements and obligations to ensure the security and privacy of its customers – the very users who contribute to the growth and success of the operators. Besides building the most secure product, vendors and suppliers are also required to ensure that not only they follow the most strict industry security best practices, but also receive the necessary accreditation to ensure that they are held to the highest standards.

4 Security Assurance Process

The security assurance process is certainly not new. The process already exists for many reasons for IT products. The process can be used for networking products to a certain extent but with some degree of limitations. The most notable of these developments is the Common Criteria (CC) and the Common Criteria Recognition Arrangement (CCRA) which combined three standards: Information Technology Security Evaluation Criteria (ITSEC), Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), and Trusted Computer Security Evaluation Criteria (TCSEC) originally developed by the governments of European countries, Canada, and US respectively.

4.1 Goals of Security Assurance

In recent years, some of the legal requirements have put the vendors and operators in a dilemma as they risk the possibility of financial losses in terms of fines originating from government enforced penalties and lost business opportunities as result of negative publicity when these requirements are not met. Vendors have to show not only that they have followed the strict operator requirements and legal requirements, but also industry best practices that they have built the products to the highest degree of standards, but also with highest degree of security and integrity. Furthermore, vendors may have to repeat the process in every market and region where their products are deployed.

There should be a globally standardized process in demonstrating the security of products, systems, and networks. This process has to be systematic that every stakeholder can work with and rely upon. The stakeholders include vendors, suppliers, network operators, regulators, government agencies, etc. With so much at stake, it is easy to understand the goal of this approach – to specify the network product security assurance requirements that are necessary to protect against unwanted access to the product, its operating systems, and running applications. The security assurance requirements to be developed and specified should be based on threat and attacker models that are applicable to the functions the products are designed to perform, including generic IT and communication functions. The security assurance requirements are of course in addition to any basic functional requirements and feature requirements of the products to be developed. For instance, a base station will be developed with set of required core functions (e.g. RF, communication, etc.) with the security assurance requirements in mind as these security assurance requirements

are taken as baseline for building products that are not only functional, but also demonstrably secure. This systemic approach becomes the "Security Assurance Process".

4.2 Challenges of Security Assurance

Although CC and CCRA have existed for many years and have gained international acceptance with more than twenty member countries around the world, but the framework and infrastructure were developed mainly to focus on IT products as well as computer products, and were originally developed to serve the government and intelligence markets.

Many attempts to apply the CC and the CCRA framework for certain telecommunication products have shown the process to be both intensive and time consuming and may not meet the need for products to reach market timely with many of the features and products that are required to offer value added services to the users. Obtaining CC certification for products, even at particular levels acceptable to private communication networks (e.g. EAL 3) would mean thousands of dollars and many more man-hours spent with one of the CC-accredited laboratories around the world before certification can be obtained. Obtaining certification for higher level of assurance requires even greater efforts, more time and more money. To that effect, CC has been around many years and has served a good purpose. Many members within the telecommunication community felt that it does not address the constant changing needs and requirements of the telecommunication industry since it was designed for a different class of products and it may prove difficult to adopt it to accommodate the security assurance requirements of telecommunication products without substantial modifications. Trying to fit the networking products into the CC framework for the purpose of security assurance and accreditation has proven to be awkward, time-consuming, and expensive even though CC is not without its merits. The lessons learned and experience gained through CC and the CCRA framework will serve as a solid basis for developing security assurance process in the telecommunication environment.

Another challenge is having the stakeholders to endorse the process once it is completed. For CC and CCRA, it took quite some time for it to be recognized in twenty-plus countries, mostly through governmental efforts. Without these efforts and relying on the industry leverage alone may prove difficult even though 3GPP is an internationally recongnized standards body which produces de facto specification for wireless systems around the world. Recognition of

3GPP standards is often quite different than recognition of security assurance standards such as interoperability aspects.

Yet another challenge is choosing the right threat model and security framework in the process. There are various threat models and security framework created for different purposes, such as STIX, short for Structured Threat Information Expression, STRIDE, short for Spoofing, Tampering, Reputation, Information Disclosure, Denial of Service, Elevation of Privilege, or ITU's X.805 Security Architecture for systems providing end-to-end communications. Though there are similarities among them, but like CC, they were developed for specific cases making adaptation in telecommunication difficult. There is no right or wrong threat model and everyone has its own merits.

4.3 3GPP Security Assurance

A good example of putting the lessons learned through CC and the CCRA framework to use is shown by 3GPP in its Security Assurance Methodology (SECAM) and Security Assurance Specifications (SCAS) activities. This work is also done in conjunction with GSMA's Network Equipment Security Assurance Group (NESAG) where as 3GPP defines the security baseline specifications including test cases for evaluating the results while NESAG defines the framework for accrediting evaluation laboratories (including vendor evaluation laboratories and third-party evaluation laboratories) and resolution in case of disputes between the vendors and operators.

SECAM and SCAS are seen as a positive development of such a security assurance methodology specifically for the 3GPP products, as the first attempt to evolve into an international standards purely from the industry perspective. SECAM and SCAS are intended to be a comprehensive process for which all network product and network product when the process is fully implemented. It starts with identification of the threats and risks associated with each product. Although there may be many functions within each product (e.g. encryption, authentication, etc.), the focus is to perform the threat and risk analysis on the entire product as a whole so that the security requirements along with security assurance specification can be developed. Next, the security requirements will be developed for that product, which may be done in modular fashion, for example based on functional components, to afford the flexibility of applying these modules of requirements to different products with same or similar functions without duplicating efforts needed to develop security assurance requirements for the same function in another product.

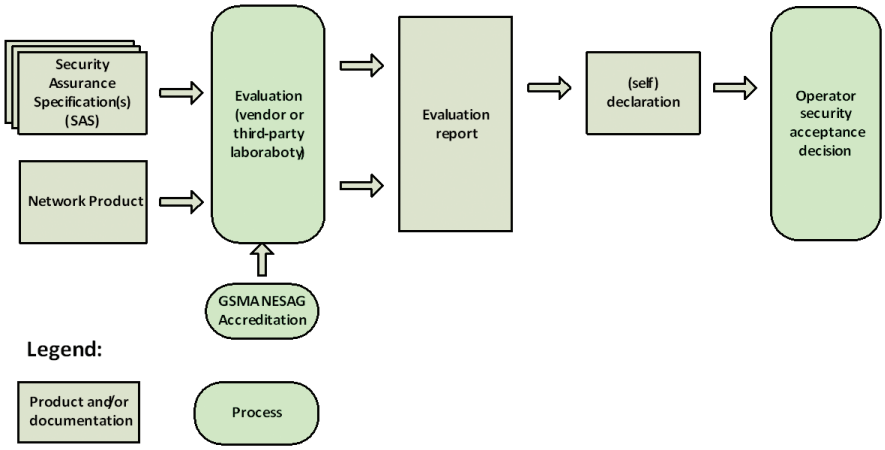

Figure 2 3GPP Security Assurance Process

The security requirements take into account threat model and risk analysis, attacker potentials and capabilities, environmental variations, etc. to resist all known attacks (both current and anticipated). A testing process (e.g. evaluation by an accredited laboratory that can be either a vendor or a third-party independent laboratory) then follows with test cases and testing methodology that will be able to produce verifiable and repeatable results from the security testing of the product. All product will be tested vigorously and comprehensively to ensure that that the product being built and tested will conform to the security requirements. This is the same philosophy of assuming nothing, believing in no one, but checking everything with a multi-layered "many hands" and "many eyes" approach to independent verification in order to reduce the risk of insecure products being distributed.

The final step in the security assurance process is for the operator to gain confidence after the product has clearly demonstrated meeting all of the defined security requirements and passing all of the verifications. Acceptance is also backed by rigorous and yet robust audit mechanism where verifiability, traceability, and disputes can be resolved.

More than ever, the operators demand greater uniformity in terms of requiring the same security assurance from all vendors, especially in a multi-vendor deployment environment. The users demand unequivocal guarantee in terms of security and privacy. And finally the governments have placed stringent requirements on the service providers to deploy secure network equipments and networks in the name of national security as more and more governments

are relying less on dedicated networks and more on private networks to carry their traffic. Greater emphases are placed on the security assurance of telecom products, as the entire industry has experienced an evolution of migrating to open architecture and open platform from a traditionally considered closed environment. This, in turn will drive the telecommunication community to create the standards necessary to achieve the desired security assurance for the products developed to comply with specifications.

4.4 3GPP Security Assurance Approach

In order for the security assurance process to work, a multi-layered approach needs to be taken where the security assurance process is to be developed as an open and transparent process where all stakeholders with their vast expertise and experience from aspects of telecommunication, information technology, networking, and security contribute toward a common goal. The ultimate goal is not only to give the operators assurance that the products built are secure, but also to give assurance to all stakeholders that the products built are secure against the known attacks at the time of deployment.

Every stakeholder across all regions also needs to sign on to and agree to the process. Working with other standardization bodies, such as ETSI, IETF, ITU, 3GPP, etc and with regulators will ensure mutual acceptance once a particular product has successfully gone through the security assurance process is not alone in perfecting the security assurance process. Other organizations' expertise is also very helpful as those have gone through similar efforts such as National Institute of Standards and Technology (NIST) Security Content Automation Program (SCAP), the Security Automation and Continuous Monitoring (SACM) in IETF, and SECAM and SCAS in 3GPP even though sometimes the efforts by disjoint organizations would appear in random. Mutual recognition and mutual acceptance equate to a single and fair process for all and goes a long way to ensure the success of the entire process.

Though the aim is for the operators to gain confidence about the security of the products, but since the process is open and every step within the process can be documented and substantiated, it should make it very easy for all stakeholders, whether they are vendors, system operators, regulators or the like to realize the transparency within the process and to accept the products with a great deal of confidence that the products are secure, once the rigorous security assurance process has been followed. It is important to emphasize once again that such a security assurance must be transparent, collaborative, global, standards-based and practical to be effective. It is noted that as a

Figure 3 International Security Assurance Collaboration

standards-developing organization (SDO), 3GPP has made great strides to achieving the goal of security assurance through the study items and work items that have produced various technical reports such as 3GPP Study on Security Assurance Methodology for 3GPP Network Products Technical Report, 3GPP Pilot development of Security Assurance Specification (SCAS) for MME network product class Technical Report, and 3GPP Security Assurance Methodology for 3GPP network products Technical Report. Once the work is done, 3GPP will have produced security assurance specification for all 3GPP products, starting with the Mobility Management Entity and extending to other network product class such as evolved NodeBs (eNB), Serving Gateways (SGW), etc.

In summary, here is the approach and process taken in 3GPP to develop a security assurance specification:

1. Establish and methodology for 3GPP security assurance
2. Create testable requirements and test cases
3. Develop specification on security assurance for a particular 3GPP product (e.g. MME)
4. Test the process
5. Extend the process for all all 3GPP products.

4.5 Security Assurance Around the Globe

Recognizing the importance of security assurance in ICT, many other SDOs have accelerated their pace in bringing more awareness through the development and work on security assurances. Work in CC is continuing in terms of making it more "user-friendly" by considering the different levels of assurance. IETF has taken on the work of creating use cases for Endpoint Security Posture Assessment and has gone through several iterations of internet drafts. GISFI is working closely with 3GPP in addressing the security assurance requirements originating from the Indian telecom market. CESG, though not a SDO, has also development a commercial product scheme or CPA for short for the UK market to provide assured commercial security products for users who have a need for information assurance. With network virtualization and SDN on everyone's mind, the European Union Agency for Network and Information Security has also developed a set of assurance criteria to assess the risks of adopting cloud services, obtain assurance from the cloud providers, and reduce the assurance burden on the cloud providers. Similar activites in ITU produced Entity Authentication Assurance Framework in ITU-T's X.1254. The list goes on and on, but none bigger than the challenges taken up in 3GPP.

5 Conclusion

Now is the time to step up and address future global security challenges today. The team of security experts representing the operators, vendors, and regulators in 3GPP have come together in unison to focus on the security assurance process by leveraging the expertise and knowledge gained from years of creating standards. Making claims one way or another about the security of the products, systems, or networks based on misconstrued or misinformed belief without any concrete evidence is not only irresponsible but they are also not valid reasons to accept or reject a particular product. The network of tomorrow starts today. Getting away from the cycles of break-and-fix to drive the security assurance message home will ensure the success of verified and certifiable security claims. Security begins with a commitment coupled with a solid foundation of understanding the threats, defining a security assurance process, and going through vigorous testing leading to verification. It is also important for the market that a successful verification as a result of the security assurance process should be internationally recognized and accepted as the process itself is an open process. Following the security assurance process will not be beneficial for the telecommunication industry, but a win-win proposition for the entire ecosystem.

References

[1] 3GPP TR 33.805, Study on Security Assurance Methodology for 3GPP Network Products
[2] 3GPP TR 33.806, Pilot development of Security Assurance Specification (SCAS) for MME network product class
[3] 3GPP TR 33.916, Security Assurance Methodology for 3GPP network products
[4] Canada's Privacy Act, http://www.priv.gc.ca/leg_c/leg_c_a_e.asp
[5] Common Criteria for Information Technology Security Evaluation, Version 3.1 Release 4, September 2012
[6] The CC and CEM documents: http://www.commoncriteriaportal.org/cc/
[7] The CCRA introduction: http://www.commoncriteriaportal.org/ccra
[8] CCRA Licensed Laboratories: http://www.commoncriteriaportal.org/labs/
[9] EU Directive 95/46/EC, The Data Protection Directive
[10] CESG Commercial Product Assurance (CPA) Scheme: http://www.cesg.gov.uk/servicecatalogue/Product-Assurance/CPA/Pages/CPA.aspx
[11] IETF Internet Draft: "Endpoint Security Posture Assessment – Enterprise Use Cases"
[12] Cloud Computing Information Assurance Framework: http://www.enisa.europa.eu
[13] ITU-T X.1254: Entity Authentication Assurance Framework

Biography

Marcus Wong Wireless Security Research and Standardization, Huawei Technologies (USA).

Marcus received his Master of Arts Degree in Computer Science from Queens College of City University of New York (USA). He has over 20 years

of experience in the wireless network security field with AT&T Bell Laboratories, AT&T Laboratories, Lucent Technologies, and Samsung's Advanced Institute of Technology. He holds Certification of Information System Security Professional (CISSP) from the prestigious International Information Systems Security Certification Consortium (ISC2).

Marcus has concentrated his research and work in many aspects of security in wireless communication systems, including 2G/3G/4G mobile networks, Personal Area Networks, and satellite communication systems. Marcus joined Huawei Technologies (USA) in 2007 and continued his focus on research and standardization in 3GPP, WiMAX Forum, IEEE, and IETF security areas. As an active contributor in the Wireless World Research Forum (WWRF), he has shared his security research on a variety of projects contributing toward whitepapers, book chapters, and speaking engagements.

In the past, Marcus has held elected official positions in both WWRF and 3GPP, serving as the vice-Chairman of WWRF Working Group 7 (Security and Trust working group) from 2007 to 2012 and as the vice-Chairman of 3GPP SA3 (Service & System Aspect, Security Group) from 2009 to 2011 respectively. He also served as guest editor in the IEEE Vehicular Technology magazine. He also has published a number of journal papers and whitepapers in leading publications, including that of the Journal of Cyber Security and Mobility. In addition, he has numerous patents granted and/or pending.