OIC-CERT Journal of Cyber Security
Volume 3, Issue 1 (April 2021)
55 - 64

Achieving 5G Security through Open Standards

A. Cheang[1], X. Gong[2], and M. Yang[3]
[1]Huawei, Dubai, UAE
[2]Huawei, Shenzhen, China
[3]Huawei, Manama, Bahrain
[1]aloysius.cheang@huawei.com, [2]gongxiaoxin@huawei.com, [3]yang.ming@huawei.com

ARTICLE INFO

Article History
Received 04 Feb 2020
Received in revised form 10 Feb 2020
Accepted 08 Mar 2021

Keywords:
5G, Cybersecurity, Privacy, Standards, NESAS

ABSTRACT

In telecommunications, 5G is the fifth generation technology standard for broadband cellular networks. The substantial increase in speed, coupled with reduced latency that allows instant communication and ability to connect more devices at the same time are critical game changers when it comes to building a foundation infrastructure that will support future smart applications and solutions in any digital transformation projects that attempt to create new outcomes that will benefit people and businesses. However, how do we ensure that a deployment of 5G is secure? How can experts ensure that 5G security risks can be effectively managed in terms of security protocols and standards as well as security assurance mechanisms? How to continuously improve 5G security level from the perspectives of different stakeholders in order to address future? This white paper will describe industry initiatives, joint efforts of industry partners and our proposal on how to build an open and transparent framework under OIC-CERT that will define a common baseline for 5G security across OIC member states.

I. INTRODUCTION

5G is a digital revolution, not just a speed-boost. 5G and the broadband bandwidth that it brings about allows for the realization of a real-time cloud, and the creation of applications and solutions that will enable the development of the next digital economy, enabling the smart city of the future and bridging the social divide leveraging on digital transformation that mines data as the new oil.

However, before 5G can takes flight the industry needs to resolve the security challenges and opportunities brought by new services, architectures, and technologies [1], as well as higher user privacy and protection requirements. The industry

ISSN 2636-9680
eISSN 2682-9266

needs to understand the requirements of diversified scenarios and better define 5G security standards and technologies to address the associated risks. Globally, the 3rd Generation Partnership Project (3GPP) SA Working Group (SA3) is tasked to look into security and privacy security issues in 5G. 3GPP SA3 quickly becomes the world's leader in defining 5G security standards. SA3 held seven meetings. 74 companies (including their subsidiaries) sent technical experts to attend the meetings [2], with the key objective of formulating 5G security standards. The 3GPP SA3 has comprehensively analyzed 5G threats and risks in 17 security areas [3]: Security architecture, authentication, security context and key management, radio access network (RAN) security, security within NG-UE, authorization, subscription privacy, network slicing security, relay security, network domain security, security visibility and configurability, credential provisioning, interworking and migration, small data, broadcast/multicast security, management security, and cryptographic algorithms.

However, on top of the 3GPP security standards endorsement, operators need to develop a consistent end-to-end security framework that addresses both their network equipment and their network management. It should encompass more than just an operator's backhaul and core networks and base stations. Other network elements, such as interconnection gateways, firewalls, and IT servers (such as DHCP, DNS, and RADIUS servers) must also be considered in the overall security framework. By taking a holistic approach in designing such a framework, operators can ensure that there are no single points of failure within the network or at the border with other networks.

Besides operator's overall design framework, there is also an imperative need to evaluate and benchmark the equipment such as mobile network equipment used in 5G deployment to meet the following requirement to achieve an impartial and high-quality standard in 5G deployment in any part of the world. This will be critical to ensure supply chain security though:

- Providing accreditation from the world's leading mobile industry representative body
- Delivering a world-class security review of security related processes
- Offering a uniform approach to security audits
- Avoiding fragmentation and potentially conflicting security assurance requirements in different markets

II. RELATED WORK

Several organisations have been working on designing architectures for telecommunication networks. Besides the heavily referenced 3GPP work in this paper, these are related work done by other projects such as:

- The NGMN (Next Generation Mobile Networks) Alliance's 5G working programme [4], [5]. NFMN has identified new threats and security issues that may arise with 5G. In particular, the NGMN Alliance provides 5G security recommendations

for network slicing, access network, and low-latency use cases. For example, for network slicing, these recommendations express security needs of the infrastructure and virtualisation security realm.

- Resilient Communication Services Protecting End-user Applications from Disaster-based Failures or COST-RECORDIS [6], a European level consortium with scientific scope focusing on resilience of communication networks under disaster-induced failures. Such events can seriously disrupt a communication network, making its services unavailable. They follow from natural disasters, weather-induced disruptions, technology-related failures, or malicious attacks, and they are observably increasing in number, intensity and scale. When network services that are part of a critical infrastructure become unavailable, commercial and/or societal problems are the inevitable result. This COST Action, driven by researchers from academia and industry in strong cooperation with governmental bodies, aims to fill the gap by developing appropriate solutions to provide resilient communications in the presence of disaster-based disruptions of all types for existing and future communication network architectures.
- ETSI TC CYBER working group is recognized as a major trusted centre of expertise offering market-driven cyber security standardization solutions, advice and guidance to users, manufacturers, network, infrastructure and service operators and regulators. ETSI TC CYBER [7] works closely with stakeholders to develop standards that increase privacy and security for organizations and citizens across Europe and worldwide. They provide standards that are applicable across different domains, for the security of infrastructures, devices, services, protocols, and to create security tools and techniques. Specifically, on 5G security and 5G applications, these are their key research questions:
    - Mobile/Wireless systems (5G, TETRA, DECT, RRS, RFID...)
    - IoT and Machine-to-Machine (M2M)
    - Network Functions Virtualisation
    - Intelligent Transport Systems, Maritime
    - Broadcasting
    - Securing Artificial Intelligence
    - Privacy-preserving pandemic protection

III. METHODOLOGY

The following approach is adopted in our research methodology that is based on qualitative analysis methodologies, mainly Action Research [8] supported by Case Study and Narrative Models [9].

ISSN 2636-9680
eISSN 2682-9266

Action Research, or Participatory Action Research, is a reflective process of progressive problem solving led by individuals working with others in teams or as part of a "community of practice" to improve the way they address issues and solve problems. Whereas the narrative model occurs over extended periods of time and compiles information as it happens. Like a story narrative, it takes subjects at a starting point and reviews situations as obstacles or opportunities occur, although the final narrative does not always remain in chronological order. Businesses use the narrative method to define buyer personas and use them to identify innovations that appeal to a target market. Lastly, the case study model provides an in-depth look at one test subject. The subject can be a person or family, business or organization, or a town or city. Data is collected from various sources and compiled using the details to create a bigger conclusion. Businesses often use case studies when marketing to new clients to show how their business solutions solve a problem for the subject.

Thus, our research is performed according to the following time-based schedule:

A. Systematic literature review

To arrive at a key research focal direction based on the following research questions:

Question 1: What is the current 5G security controls in terms of baseline control sets and advanced control sets? How are they being developed into cyber security hygiene requirements?

Question 2: What are the efforts in establishing a common baseline for 5G security vis-à-vis various regulatory requirements and supporting deep tech applications?

Questions 3: What is the work currently to engage all the stakeholders in the 5G ecosystem and how can that be improved?

B. Identify gaps or areas for performing Action Research

Arriving from an analysis based on literature survey, to build a systemic approach to ensure that a common baseline of key 5G security controls can be developed that will be adopted globally while reduce the gap (barriers of entry) and cost (reduce cost of entry) and harmonising regulatory requirement while matching technical capabilities.

C. Design Case Study / Reference Use Cases

As per required by Cast Study model, to develop use cases and reference models that can provide reassurance of the proposed solution framework effectiveness.

D. Continuous review of other 5G security research initiatives and progress

At the same time, to continue to scan the environment and review work done by other groups to ensure that any major security issues that are brought up can be addressed by this research

framework or that the risks can be mitigated by existing security controls proposed.

IV. KEY FEATURES OF 5G SECURITY STANDARDS

3GPP 5G security and 4G security share the same purpose, which is to ensure the confidentiality, integrity, and availability of networks and data. 5G Security Architecture inherits 4G Security Architecture, however provides Security Enhancement of 5G Standards over 4G Standards:

- Stronger air interface security: In addition to user data encryption on 2G, 3G, and 4G networks, 5G standards provide user data integrity protection to prevent user data from being tampered with.
- Enhanced user privacy protection: In 2G, 3G, and 4G networks, users' permanent IDs (international mobile subscriber identities — IMSIs), are transmitted in plain text over the air interface. Attackers can exploit this vulnerability using IMSI catcher attacks to track users. In 5G networks, users' permanent IDs (in this case, SUPIs) are transmitted in ciphertext to defend against such attacks.
- Better roaming security: Operators usually need to set up connections via third-party operators. Attackers can forge legitimate core network nodes to initiate Signaling System 7 and other attacks by manipulating third-party operators' devices. 5G Service-Based Architecture (SBA) defines Security Edge Protection Proxy (SEPP) to implement E2E security protection for inter-operator signaling at the transport and application strata. This prevents third party operators' devices from tampering with sensitive data (e.g. key, user ID, and SMS) exchanged between core networks.
- Enhanced cryptographic algorithms: 5G R15 standards currently define security mechanisms such as 256-bit key transmission. Future 5G standards will support 256-bit cryptographic algorithms to ensure that such algorithms used on 5G networks are sufficiently resistant to attacks by quantum computers.

5G cyber security standards put more security features into standard to tackle potential security challenges and lead to security enhancements in the future 5G lifecycle.

V. THE NEED TO ENSURE CONSISTENCY OF EFFECTIVE 5G SECURITY CONTROLS IN DEPLOYMENTS BY ANY OPERATOR

Governments can be part of these efforts in controlling risks to operate 5G services in line with country regulations. A recommended win-win strategy to address 5G security is to deliver a plan described as follows:

ISSN 2636-9680
eISSN 2682-9266

- Formulation of regulations and laws, involving cross-discussion with all public and private partners, to guarantee a consistent security framework. Governments should take a key role here to define the requirements of their respective countries in terms of security and encourage the development of new technologies with risk control mechanisms to address both their economic objectives and security needs. This can be achieved through collaboration with all stakeholders, based on a common goal to define world standards. Governments play a major role in providing incentives to deliver a positive economic output for their respective countries, in terms of both leveraging innovations (5G in the context of this report) and guaranteeing that regulations are available for defining key aspects such as the security agenda, security assurance mechanism, certification program, and policies.
- Operators should be the major responsible body for the operation of network infrastructure and implementation of risk management according to the country's security regulations and official standards bodies. In addition to this, governments can implement specific policies to obtain oversight on the security level of each network operating in the country.

Towards this end, the Network Equipment Security Assurance Scheme/Security Assurance Specifications (NESAS/SCAS), jointly defined by GSMA and 3GPP, establishes a framework to facilitate improvements in security levels across the mobile industry [10].

VI. BUILDING SECURITY THROUGH INDUSTRY COLLABORATION TO TACKLE REAL WORLD PROBLEMS AND FUTURE SECURITY CHALLENGES

To truly control risks in the 5G lifecycle, besides continuously enhancing security solutions through technological innovation, efforts need to be expended to bring all stakeholders, from end users, government regulator, operators, technology providers and standardization or cyber security professional bodies together to build an industry-led open and transparent ecosystem cooperation so as to ensure that there is a common baseline of security control set and supply chain security.

Specifically,

- Technology providers: Technology providers should contribute industry security standard work, comply with standards, and integrate security technologies to build secure equipment. Together with customers and other stakeholders, vendors should provide capability to support the operators to assure secure operation and cyber

resilience. Thus, the security of the technology provided should be able to meet stringent certification requirements that are 3rd party, meet government regulator's procurement requirement and recognized by different jurisdiction where you only need to be certified once, but accepted and usable by many.

- Operators: Operators are responsible for the secure operations and cyber resilience of their own networks. 5G networks are private networks. The boundaries between different networks are clear. Operators should build their own security defences based on zero trust architecture. For internal threats, operators can manage, monitor, and audit all vendors and partners to make sure their network elements are secure. Hence, through a zero trust approach to prevent against supply chain attack, operators need to have a defence in depth strategy that will heavily rely on a supply chain that has a common security baseline that is referenceable and can be relied upon through ecosystem cooperation.
- Industry and government regulators: As an industry, we all need to work together on standards. This is our shared responsibility. In terms of technologies, we need to continuously contextualize 5G security risks (in slicing, Mobile Edge Computing (MEC), massive Machine-Type Communications (mMTC) and other scenarios) and enhance protocol-based security. In terms of security assurance, we need to standardize cyber security requirements and ensure that these standards are applicable to and verifiable for all vendors and operators both locally and globally as part of a global ecosystem.
- End users: The end users should define key requirements that will be taken into account during standards development. They should be able to provide valuable inputs on actual 5G deployments security requirements especially in 5G to business applications.
- Cyber security professional bodies: The Cyber security professional bodies provide a platform for the ecosystem to leverage, that all stakeholders can come together in an industry-led effort to lead 5G security deployment in the locality that the bodies have a presence in. In fact, such a body like the OIC-CERT can play an important role to harmonise and enjoy economies of scale when it comes to pushing standards and certifications that are required to build the trust in any 5G business model, whether it is 5G to Consumers or 5G to Business.

ISSN 2636-9680
eISSN 2682-9266

As such, to build a system that we can trust, we need aligned responsibilities, unified standards, and clear regulation.

VII. FUTURE WORK

Leading from the previous Section, we propose OIC-CERT to set up a working group to look into 5G security for OIC member states to form a global trusted ecosystem for 5G. The working group shall aim at achieving the following:

- Identifying 5G cyber security risks taking in account different perspectives from the stakeholders and maintaining a risk register.
- Developing recommendations for our members, a 5G cyber security framework that be a reference model for member states to develop their own National 5G cyber security standards.
- Developing recommendations for developing an OIC-level 5G cyber security framework that harmonise the requirements that allow for cross-recognition among OIC member states.
- Subsequently to explore kick-starting another working group to develop an ISAC (Information Sharing and Analysis Centre) capability for CERT response in the era of 5G and Cloud for OIC member states under OIC-CERT.

On the other hand, we shall constantly scan the environment for any new 5G security updates, for example updates from 3GPP and update the 5G risk register in the proposed working group. For instance, 3GPP release 16 was completed on July 3, 2020. Looking ahead, SA3 are working on some exciting studies in release 17 [11], such as:

- Enhanced security support for Non-Public Networks.
- Security aspects of Unmanned Aerial Systems(UAS)
- Security for enhanced support of Industrial IoT
- Security Enhancements for 5G Multicast-Broadcast Services
- Security Enhancement of Support of Edge Computing in 5GC
- Security impacts of Virtualisation
- Authentication enhancements in 5GS
- Enhancements to User Plane Integrity Protection
- Security enhancement against false base stations
- Mission Critical Services Security Enhancement

Final release 17 was due 2021 has been shifted to 2022 due to the Covid-19 pandemic impact.

VIII. CONCLUSION

As more and more OIC member states embraces digital transformation, assumptions that need to be addressed such as unlimited bandwidth and unlimited storage will be the key addressable issues that

enable the realization of the vision to build a trusted digital oasis that will elevate the entire industry to the next level. 5G will provide that broadband connectivity that will address the need to provide unlimited bandwidth to bring us into Industrial 4.0 and support any Smart City, Smart Nation vision and it will be imperative that a common security baseline is defined for adoption of 5G such that minimum efforts are required for ensuring that any 5G deployment by any vendor or operator will meet the minimum security requirement for 5G regardless of which OIC member state or industry vertical that the 5G deployment is addressing where the outcome can be managed and measured with consistency without extensive time, effort and cost to go into assessing and certifying from scratch. This can be achieved through industry collaboration between different stakeholders in an industry-led open and transparent ecosystem cooperation that will build a secured and trusted supply chain for provisioning of broadband and any applications and solutions sitting on top of the broadband.

IX. REFERENCES

[1] 3GPP TR 33.899: "Study on the security aspects of the next generation system" [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3045

[2] 5G Security Transparency [Online]. Available: http://www.circleid.com/posts/20181209_5g_security_transparency/

[3] 3GPP TR 33.899: "Study on the security aspects of the next generation system" [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3045

[4] NGMN Alliance, 5G Security Recommendations—Package #2: Network Slicing, 2016, [Online]. Available: https://www.ngmn.org/uploads/media/160429_NGMN_5G_Security_Network_Slicing_v1_0.pdf

[5] NGMN Alliance, 5G Security—Package 3: Mobile Edge Computing/Low Latency/Consistent User Experience, 2016 [Online]. Available: https://www.ngmn.org/uploads/media/161028_NGMN-5G_Security_MEC_ConsistentUExp_v1.3_final.pdf

[6] J. Rak et al., "RECODIS: Resilient Communication Services Protecting End-user Applications from Disaster-based Failures," 2016 18th International Conference on Transparent Optical Networks (ICTON), Trento, pp. 1-4, 2016, doi: 10.1109/ICTON.2016.7550596. Available: http://www.cost-recodis.eu/images/Publications/1.pdf

[7] ETSI TC CYBER Available: https://www.etsi.org/technologies/cyber-security

[8] A. Bryman and E. Bell, "Business Research Methods" 3rd edition, Oxford University Press, 2011.

[9] Qualitative research methods [Online]. Available: https://measuringu.com/qual-methods/

[10] Network Equipment Security Assurance Scheme [Online].

ISSN 2636-9680
eISSN 2682-9266

Available: https://www.gsma.com/aboutus/workinggroups/working-groups/fraud-security-group/network-equipmentsecurity-assurance-scheme

[11] 3GPP Work Items for TSG/SA3 [Online]. Available: https://www.3gpp.org/DynaReport/TSG-WG--s3--wis.htm