Overview of 5G Security Challenges and Solutions

Article · March 2018

DOI: 10.1109/MCOMSTD.2018.1700063

Ijaz Ahmad
University of Oulu

Tanesh Kumar
University of Oulu

Madhusanka Liyanage
University College Dublin

Jude Okwuibe
University of Oulu

Overview of 5G Security Challenges and Solutions

Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov

Abstract

5G networks will use novel technological concepts to meet the requirements of broadband access everywhere, high user and device mobility, and connectivity of massive number of devices (e.g., the Internet of Things) in an ultra-reliable and affordable way. Software defined networking and network functions virtualization leveraging the advances in cloud computing such as mobile edge computing are the most sought out technologies to meet these requirements. However, securely using these technologies and providing user privacy in future wireless networks are the new concerns. Therefore, this article provides an overview of the security challenges in clouds, software defined networking, and network functions virtualization, and the challenges of user privacy. Henceforth, this article presents solutions to these challenges and future directions for secure 5G systems.

Introduction

According to the Fifth Generation Public Private Partnership (5G-PPP), 5G will connect about 7 trillion wireless devices or things, shrink the average service creation time from 90 hours to 90 minutes, and enable advanced user controlled privacy [1]. By connecting all aspects of life, 5G aims at a digital society that requires high service availability and security using a diverse set of technologies. Therefore, the concepts of cloud computing, software defined networking (SDN), and network functions virtualization (NFV) are sought out to meet the growing user and service demands within the constraints of capital expenditures (CapEx) and operational expenses (OpEx) through flexible network operation and management.

Cloud computing provides an efficient way for operators to maintain data, services, and applications by bringing technologically distinct systems into a single domain on which multiple services can be deployed to achieve a higher degree of flexibility and availability with less CapEx and OpEx. Mobile edge computing (MEC), using the concepts of cloud computing, will empower the network edge to process delay-sensitive and context-aware applications in close proximity of users or things. Softwarizing network functions will enable portability and flexibility of networking systems and services. SDN enables network function softwarization by separating the network control from the data forwarding planes, and enabling programmability of both planes. Hence, SDN brings innovation in networking through abstraction and programmability on one hand and simplifies network management through logically centralized control of the network on the other hand.

NFV provides the basis for placing various network functions in different network perimeters and eliminates the need for function or service-specific hardware. SDN and NFV, complementing each other, improve network elasticity, simplify network control and management, break the barriers of vendor- specific proprietary solutions, and thus are considered the core technologies in the transformation of networks for 5G by 5G-PPP. Network slicing, leveraging NFV and SDN, enables the 5G network infrastructure to share the same resources for multiple use cases such as the Internet of Things (IoT), enhanced broadband, and critical communication [1]. A generic 5G deployment scenario using these key technologies is depicted in Fig. 1.

However, recent research in these technologies reveals potential security challenges that must be addressed in order to ensure security of new 5G services and infrastructures, and users. For example, multi-tenant shared cloud infrastructures among multiple virtual network operators require strict isolation at multiple levels to avoid illegal resource consumption and maintain integrity of users' information of different operators [2]. According to the 5G-PPP Phase 1 Security Landscape [1], network slicing has several open security challenges such as security isolation of network slices and security of inter-slice communications [3]. Moreover, programmable network architectures like SDN require strong authentication and authorization for applications to avoid misuse of the network resources exposed to applications through the control plane. Similarly, misconfigurations of virtual network functions (VNFs) can lead to inter-federated conflicts creating jeopardy in the whole network [4]. Since 5G will connect every aspect of life to the network, having most users' information stored and shared online, maintaining user privacy, will be highly challenging.

Furthermore, wireless communication systems have been prone to security vulnerabilities from the very inception. In 1G wireless networks, mobile phones and wireless channels were targeted for illegal cloning and masquerading. In 2G

Digital Object Identifier: 10.1109/MCOMSTD.2018.1700063

Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, and Mika Ylianttila are with the University of Oulu; Andrei Gurtov is with Linköping University.

2471-2825/18/$25.00 © 2018 IEEE

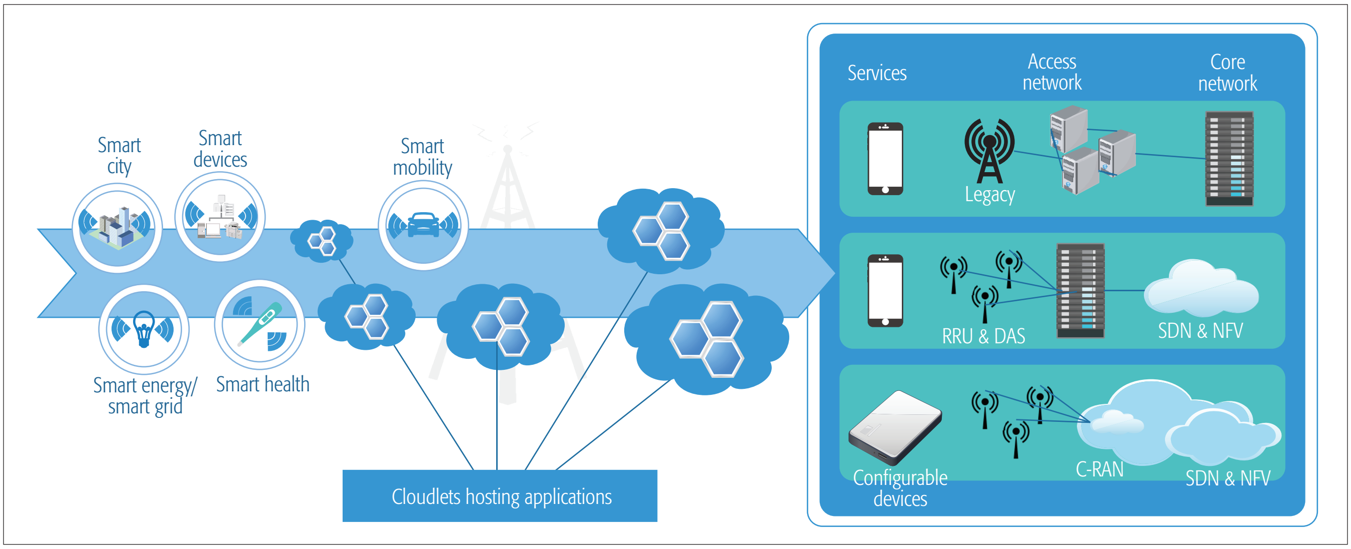

FIGURE 1. 5G deployment scenarios and key technologies.

wireless networks, message spamming became common for not only pervasive attacks but injecting false information or broadcasting unwanted marketing information. In 3G wireless networks, IP-based communication enabled the migration of Internet security vulnerabilities and challenges in the wireless domains. With the increased necessity of IP-based communication, 4G mobile networks enabled the proliferation of smart devices, multimedia traffic, and new services into the mobile domain [5]. This development led to a more complicated and dynamic threat landscape. With the advent of 5G wireless networks, the security threat vectors will be bigger than even before with greater concern for privacy.

Therefore, it is crucial to highlight the security challenges that not only are threatening due to the wireless nature of mobile networks, but also exist in the potential technologies that are highly important for 5G. The rest of the article is organized as follows. We describe the key security challenges, followed by security solutions for the highlighted security challenges. We highlight the 5G security standardization activities at the time of writing this article, and finally we conclude the article.

Key Security Challenges in 5G

5G needs robust security architectures and solutions since it will connect every aspect of life to communication networks. Therefore, we investigate and highlight the important security and privacy challenges in 5G networks (depicted in Fig. 2) and overview the potential solutions that could lead to secure 5G systems. The basic challenges in 5G highlighted by Next Generation Mobile Networks (NGMN) [6] and highly discussed in the literature are as follows:

- **Flash network traffic:** There will be a high number of end-user devices and new things (IoT).
- **Security of radio interfaces:** Radio interface encryption keys are sent over insecure channels
- **User plane integrity:** There is no cryptographic integrity protection for the user data plane
- **Mandated security in the network:** Service-driven constraints on the security architecture lead to the optional use of security measures.
- **Roaming security:** User-security parameters are not updated with roaming from one operator network to another, leading to security compromises with roaming.
- **Denial of service (DoS) attacks on the infrastructure:** There are visible etwork control elements and unencrypted control channels.
- **Signaling storms:** Distributed control systems require coordination, for example, non-access stratum (NAS) layer of Third Generation Partnership Project (3GPP) protocols.
- **DoS attacks on end-user devices:** There are no security measures for operating systems, applications, and configuration data on user devices.

The 5G design principles outlined by NGMN beyond radio efficiency include creating a common composable core and simplified operations and management by embracing new computing and networking technologies. Therefore, we focused on the security of those technologies that will fulfill the design principles outlined by NGMN (i.e., mobile clouds, SDN, and NFV). Table 1 provides a summary of different types of security threats and attacks, the targeted elements or services in a network, and the technologies that are most prone to the attacks or threats are ticked. These security challenges are briefly described in the following sections.

Security Challenges in SDN

SDN facilitates innovation in communication networks and simplifies network management by enabling programmability and logically centralizing the network control planes. These two features are significantly important for future networks; however, they also open the network to security challenges. For example, the SDN controller updates or modifies flow rules in the data forwarding elements. This control information traffic can easily be identified, making it a visible entity in the network and rendering it a favorite choice for DoS attacks. Similarly, the centraliza-

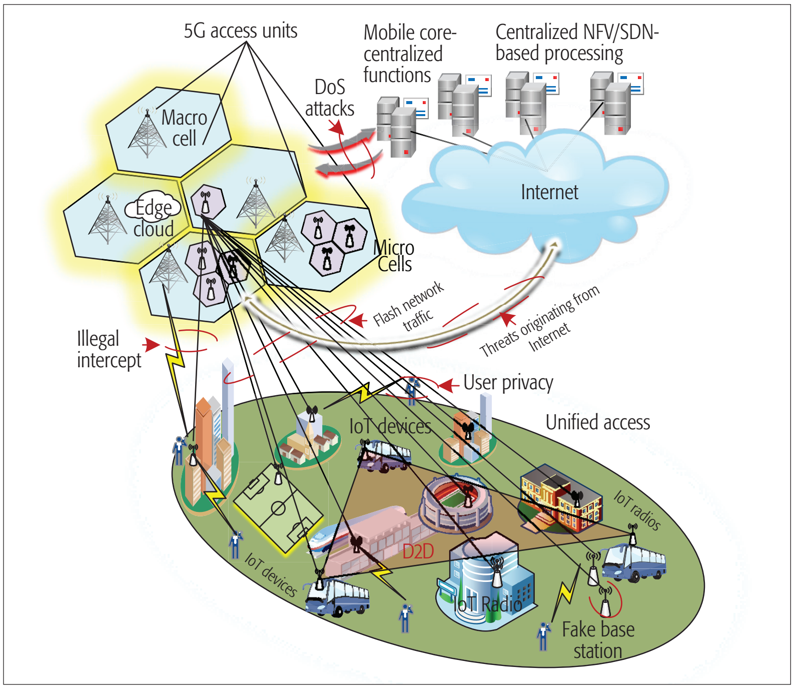

FIGURE 2. 5G network and the threat landscape.

tion of network control can also make the controller a bottleneck for the whole network in the case of saturation attacks. By enabling programmability, most network functions can be implemented as SDN applications. If malicious applications are granted access, or critical application programming interfaces (APIs) are exposed to unintended software, a havoc can be spread across the network [7].

The current SDN architecture (i.e., OpenFlow) requires the data forwarding elements to store traffic flow requests until the controller updates the flow forwarding rules. Hence, the data plane elements can also be prone to saturation attacks since the forwarding elements, such as OpenFlow switches, have limited resources to buffer unsolicited (TCP/UDP) flows. Furthermore, this dependence on the controller requires the control-data planes channel to be resilient to security attacks unlike the current optional use of security protocols and long restoration delays in large networks. Redundant or multiple controllers may solve the challenge of controller availability or increase resilience to security attacks. However, misconfiguration of forwarding elements or inter-federated conflicts due to multiple controllers will hinder network-wide security policy enforcement [4].

Security Challenges in NFV

Even though NFV is highly important for future communication networks, it has basic security challenges such as confidentiality, integrity, authenticity, and non-repudiation [7]. From the point of view of its use in mobile networks, it is presented in [7] that the current NFV platforms do not provide proper security and isolation to virtualized telecommunication services. One of the main challenges persistent in the use of NFV in mobile networks is the dynamic nature of VNFs that leads to configuration errors and thus security lapses [8]. Moreover, VNFs are vulnerable to typical cyber-attacks such as spoofing, sniffing, and DoS. NFV is also vulnerable to a special set of virtualization threats, such as side-channel attacks, flooding attacks, hypervisor hijacking [9], malware injection, and virtual machine (VM) migration related attacks, as well as cloud-specific attacks. Moreover, private deployments of NFV are vulnerable only to malicious insiders (e.g., a malicious administrator), since remote access to the system is prevented. Due to the common accessibility of the infrastructure, a malicious user or a compromised provider of VNF can interfere with the operations of the infrastructure by inserting malware or manipulating network traffic.

Operational interference and misuse of shared resources are considered as infrastructure-level attacks on NFV. Due to the common accessibility of physical infrastructure resources, an attacker can interfere with operations of the infrastructure by inserting malware or manipulating network traffic. In these kinds of resource misuse attacks, the victim can have no benefit of shared or dedicated resources. The maintenance of trust in virtualized NFV systems is also a big challenge. Usually, physical network devices are installed and configured by a trusted employee, and there is established trust of the device. However, because VNFs fetch dynamically from the cloud, some level of trust mechanism is needed to prevent malicious VNFs. Further challenges are highlighted in Table 1.

Security Challenges in Mobile Clouds and MEC

Since cloud computing systems comprise various resources, which are shared among users, it is possible that a user spreads malicious traffic to tear down the performance of the whole system, consume more resources, or stealthily access resource of other users. MEC, on the other hand, comprises different complementary technologies interoperating in an open ecosystem where virtualization and distributed computing are harnessed by service providers to deploy and serve applications to end users. Given that MEC is relatively in its infancy, coupled with the diversity of MEC technologies, there is potential for malicious attacks and privacy issues. Since MEC extends cloud computing capabilities to the edge of mobile networks, the level of protection that can be offered to the edge hosts is low compared to what is obtainable in traditional large data centers. Similarly, in multi-tenant cloud networks where tenants run their own control logic, interactions can cause conflicts in network configurations. Mobile cloud computing (MCC) migrates the concepts of cloud computing into the 5G ecosystems. This creates a number of security vulnerabilities that mostly arise with the architectural and infrastructural modifications in 5G. Therefore, the open architecture of MCC and the versatility of mobile terminals create vulnerabilities through which adversaries could launch threats and breach privacy in mobile clouds [10].

In this work, we categorize MCC threats according to targeted cloud segments into front-end, back-end, and network-based mobile security threats. Detailed descriptions of each cloud segment and their threat landscapes are contained in [7]. The threat landscape at the front-end range from physical threats to application-based threats. On the back-end platform, threats are mainly tar-

Security threat	Target point/network element	Effected technology			Links	Privacy
		SDN	NFV	Cloud		
DoS attack	Centralized control elements	✓	✓	✓		
Hijacking attacks	SDN controller, hypervisor	✓	✓			
Signaling storms	5G core network elements			?	✓	
Resource (slice) theft	Hypervisor, shared cloud resources		✓	✓		
Configuration attacks	SDN (virtual) switches, routers	✓	✓			
Saturation attacks	SDN controller and switches	✓				
Penetration attacks	Virtual resources, clouds	✓		✓		
User identity theft	User information data bases			✓		✓
TCP level attacks	SDN controller-switch communication	✓			✓	
Man-in-the-middle attack	SDN controller-communication	✓			✓	✓
Reset and IP spoofing	Control channels				✓	
Scanning attacks	Open air interfaces				✓	✓
Security keys exposure	Unencrypted channels				✓	
Semantic information attacks	Subscriber location				✓	✓
Timing attacks	Subscriber location			✓		✓
Boundary attacks	Subscriber location					✓
IMSI catching attacks	Base station, identity registers				✓	✓

Table 1. Security challenges in 5G technologies [7].

Redundant or multiple controllers may solve the challenge of controller availability or increase resilience to security attacks. However, misconfiguration of forwarding elements or inter-federated conflicts due to multiple controllers will hinder network-wide security policy enforcement.

geted toward the mobile cloud servers. The scope of these threats may range from data replication to HTTP and XML DoS (HX-DoS) attacks. For the network- based mobile security threats, potential attacks include Wi- Fi sniffing, DoS attacks, address impersonation, and session hijacking.

On the side of MEC, the main security concerns are in the context of cloud-enabled IoT environment as well as the open APIs through which developers and creators serve contents to MEC applications and end users. The need for open APIs in MEC is mainly to provide support for federated services and interactions with different providers and content creators. However, the adoption of open APIs often create vulnerabilities through which adversaries in the form of third parties can launch various attacks on the MEC environment. This has triggered research on relevant security technologies channeled toward the security of the MEC nodes, which include the MEC server and other IoT nodes. Popular threats in this landscape are DoS attack, man-in-the-middle (MitM) attack, malicious mode problems, privacy leakages, and VM manipulation. A broad description of the threat landscape in MEC is presented in [11], in which the authors cover a wide array of potential security threats for the MEC system and also why security is one of the greatest challenges of MEC.

Privacy Challenges in 5G

From the user's perspective, the major privacy concerns could arise from data, location, and identity. Most smartphone applications require details of subscribers' personal information before the installation. The application developers and companies rarely mention how the data is stored and for what purposes it is going to be used. Threats such as semantic information attacks, timing attacks, and boundary attacks mainly target the location privacy of subscribers. At the physical layer level, location privacy can be leaked by access point selection algorithms in 5G mobile networks. International Mobile Subscriber Identity (IMSI) catching attacks can be used to reveal the identity of a subscriber by catching the IMSI of the subscriber's user equipment (UE). Such attacks can also be caused by setting up a fake base station that is considered as the preferred base station by UE which has lost access to a Temporary Mobile Subscribers Identity (TMSI); thus, the subscriber will respond with their IMSI [12]. Moreover, 5G networks have different actors such as virtual mobile network operators (VMNOs), communication service providers (CSPs), and network infrastructure providers. All of these actors have different priorities for security and privacy. The synchronization of mismatching privacy policies among these actors will be a challenge in the 5G network. In the previous generations, mobile operators had direct access and control of all the system components. However, 5G mobile operators are losing full control of the systems as they will rely on new actors such as CSPs. Thus, 5G operators will lose full governance of security and privacy. User and data privacy are seriously challenged in shared environments where the same infrastructure is shared among various actors (e.g., VMNOs and other competitors). Moreover, there are no physical boundaries of 5G networks as measures in MCC revolve around the strategic use of virtualization technologies, the redesign of encryption methods and dynamic allocation of data processing points. Hence, virtualization comes as a natural option for securing cloud services since each end-node connects to a specific virtual instance in the cloud via a Virtual Machine.

Security solutions	Primary focus	Target technology			Links	Privacy
		SDN	NFV	Cloud		
DoS, DDoS detection	Security of centralized control points	✓	✓			
Configuration verification	Flow rules verification in SDN switches	✓				
Access control	Control access to SDN and core network elements	✓	✓	✓		
Traffic isolation	Ensures isolation for VNFs and virtual slices		✓			
Link security	Provide security to control channels	✓			✓	
Identity verification	User identity verification for roaming and clouds services					✓
Identity security	Ensure identity security of users					✓
Location security	Ensure security of user location					✓
IMSI security	Secure the subscriber identity through encryption					✓
Mobile terminal security	Anti-malware technologies to secure mobile terminals					✓
Integrity verification	Security of data and storage systems in clouds			✓		
HX-DoS mitigation	Security for cloud web services			✓		
Service access Control	Service-based access control security for clouds			✓		

Table 2. Potential security solutions for targeted threats [7].

they use cloud-based data storage and NFV features. Hence, the 5G operators have no direct control of the data storage place in cloud environments. As different countries have different levels of data privacy mechanisms depending on their preferred context, the privacy is challenged if the user data is stored in a cloud in a different country.

Potential Security Solutions

In this section, we highlight security solutions for the security challenges outlined in the previous section. The challenges of flash network traffic can be solved by either adding new resources or increasing the utility of existing systems with novel technologies. We believe that new technologies such as SDN and NFV can solve these challenges more cost effectively. SDN has the capability to enable runtime resource (e.g., bandwidth)assignment to particular parts of the network as the need arises. The SDN controller can gather network stats through the southbound API from network equipment to see if the traffic levels increase. Using NFV, services from the core network cloud can be transferred toward the edge to meet the user requirements. Similarly, NFV enables the provision of virtual slices or resources at runtime to meet the growing traffic demands or surges in traffic at different network locations.

The security of the radio interface keys is still a challenge, as it needs secure exchange of keys encrypted like the proposed Host Identity Protocol (HIP)-based schemes in [7]. The same end-to-end encryption protocol can be used for user plane integrity. Roaming security and network-wide mandated security policies can be achieved using centralized systems that have global visibility of the users' activities and network traffic behavior (e.g., SDN). Signaling storms will be more challenging due to the excessive connectivity of UEs, small base stations, and high user mobility. The cloud radio access network (C-RAN) and edge computing are the potential problem solvers for these challenges, but the design of these technologies must consider the increase in signaling traffic as an important aspect of the future networks as described by NGMN. Solutions for DoS and saturation attacks, and other security challenges described in the previous section, are listed in Table 2, and the methodologies are described below.

Security Solutions for SDN

Once the basic security challenges inherent in SDN are addressed, SDN can be a potential problem solver in terms of security in communication networks. Having a global view of the network, centralized control, and programmability in network elements, SDN enables network-wide consistent security policies and facilitates quick threat identification through a cycle of harvesting intelligence from the network resources, states, and flows. Therefore, the SDN architecture supports highly reactive and proactive security monitoring, traffic analysis, and response systems to facilitate network forensics, the alteration of security policies, and security service insertion [13].

One of the basic features of SDN is flow- or packet-level granularity that provides transparency in terms of packet origin or source, the route it takes, and even the content. Security applications can gather samples of flows or packets through the control plane from any network perimeter to check their content regardless of the network ingress or egress ports, unlike traditional networks in which the security appliances normally reside in the entry points. This capability of SDN lays the foundation for network-wide consistent security policies, early threat identification at any network location, and quick response by updating the flow tables to route traffic to intrusion detection systems (IDSs) or firewalls at runtime. Since most of the security functionalities will be deployed in the application plane in software, security leveraging SDN can be referred to as *software defined security* [4].

Security Solutions for NFV

The security of VNFs through a security orchestrator in correspondence with the European Telecommunications Standards Institute (ETSI) NFV architecture is presented in [14]. The proposed architecture provides security not only to the virtual functions in a multi-tenant environment, but also to the physical entities of a telecommunication network. Using trusted computing, remote verification and integrity checking of virtual systems and hypervisors is proposed in [15] to provide hardware-based protection to private information and detect corrupt software in virtualized environments. In NFV systems, sophisticated security protection solutions such as firewalls and IDSs can be used to prevent outside attacks. Moreover, identity and access management mechanisms (e.g., role-based access control) can be used to mitigate the impact of insider attacks. Infrastructure-level attacks can be prevented by continuous monitoring of the resource consumption of each user and preventing malicious requests according to a blacklist of IP addresses.

In order to increase the trust between different entities, a chain of trust relationships needs to be created and maintained in NFV environments throughout its life cycle. Solutions based on cryptographic techniques, such as message stream encryption, can be used to guarantee the confidentiality of VNFs. Furthermore, the accountability and trust management can be utilized by a VNF provider to know whether its software is running without any modification in the infrastructure provider's network. Secure outsourcing is another viable solution in NFV to transfer the sensitive information to external networks. It will not only protect sensitive information but also validate the integrity of data. Moreover, security-preserving migration mechanisms establishing secure interfaces with the authorized source and destination parties, and detection and reporting of any malicious activities during migrations are needed to enable secure VM migration.

Security Solutions for Mobile Clouds and MEC

Most proposed security measures in MCC revolve around the strategic use of virtualization technologies, the redesign of encryption methods, and dynamic allocation of data processing points. Hence, virtualization comes as a natural option for securing cloud services since each end node connects to a specific virtual instance in the cloud via a virtual machine (VM). Security is provided through the isolation of each user's virtual connection from other users. Virtualized in-cloud security is one such virtualization solution to secure MCC.

For specific security threats such as HX-DoS, specific solutions such as learning-based systems (e.g., [16]) are more useful than generic approaches. For example, learning-based systems take a certain number of samples of packets and analyze them for various known attributes to detect and mitigate threats.

To secure the mobile terminals, anti-malware solutions are installed on the mobile terminal or hosted and served directly from the cloud. In MCC data and storage, the security framework will consist of energy-efficient mechanisms for the integrity verification of data and storage services in conjunction with a public provable data possession scheme and some lightweight compromise-resilient storage outsourcing. For application security, some proposed frameworks are based on securing elastic applications on mobile devices for cloud computing, a lightweight dynamic credential generation mechanism for user identity protection, an in-device spatial cloaking mechanism for privacy protection, as well as MobiCloud, which is a secure cloud framework for mobile computing and communication.

On the side of MEC, there are limited works on the topic of security; however, the use of gateways at strategic points on the networks is highly recommended. An IoT gateway is a typical example of such deployments. Other recommended security strategies include ensuring that the application hosted at the edge server authenticates any user attempting to access the application resources. The MEC server should be configured to protect applications and data storagee at the edge server from intrusion. Also, mobile devices should be required to authenticate the edge application accessing from the edge server, and the MEC platform should give assurance of data integrity [17].

Security Solutions for Privacy in 5G

5G must embody privacy-by-design and service-oriented privacy-preserving approaches. To preserve the user privacy in 5G systems, there should be mutual agreements and trust models among various stakeholders involved in the process such as user, network operator, service provider, application developer, and manufacturer on data usage and storage. Therefore, 5G will require better mechanisms for accountability, data minimization, transparency, openness, and access control [7]. A hybrid cloud-based approach is also required where mobile operators are able to store and process highly sensitive data locally and less sensitive data in public clouds. In this way, operators will have more access and control over data and can decide where to share it.

For location privacy, anonymity-based techniques must be applied where the subscriber's real identity could be hidden and replaced with pseudonyms. Encryption-based practices are useful in this case; for instance, a message can be encrypted before sending to a location-based services (LBS) provider. Techniques such as obfuscation are also crucial, where the quality of location information is reduced in order to protect location privacy. Moreover, location-cloaking-based algorithms are quite useful to handle some major location privacy attacks such as timing and boundary attacks [7]. For IMSI catching attacks, one ongoing solution for protecting subscribers' identities is to use TMSI, which is generated randomly and assigned to the UE at regular intervals. The long-term IMSI is utilized only in the case of fault recovery and when a TMSI is not yet allocated. Another way might be to adopt a passive method that will allow detection of fake base stations that capture the subscriber's IMSI. The authors in [12]

To preserve the user privacy in 5G systems, there should be mutual agreements and trust models among various stakeholders involved in the process such as user, network operator, service provider, application developer, and manufacturer on data usage and storage. Therefore, 5G will require better mechanisms for accountability, data minimization, transparency, openness, and access control.

Standardization bodies	Work groups	Major security areas in focus	Milestones
3GPP	Service and System Aspects Security Group (SA3)	Security architecture, RAN security, authentication mechanism, subscriber privacy, network slicing	TR 33.899 Study on the security aspects of the next generation system, TS 33.501: Security architecture and procedures for 5G system
5GPPP	5GPPP Security WG	Security architecture, subscriber privacy, authentication mechanism	5G PPP Security Landscape (White Paper) June 2017.
IETF	I2NSF, DICE WG, ACE WG, DetNet WG	Security solutions for massive IoT devices in 5G, user privacy, network security functions (NSFs)	RFC 8192, RFC 7744, Deterministic Networking (DetNet) Security Considerations
NGMN	NGMN 5G security group (NGMN P1 WS1 5G security group)	Subscriber privacy, network slicing, MEC security	5G security recommendations: Package 1 and 2, and 5G security: Package 3
ETSI	ETSI TC CYBER, ETSI NFV SEC WG	Security architecture, NFV security, MEC security, privacy	ETSI GS NFV-SEC 010, ETSI GS NFV- SEC 013 ETSI GS NFV-SEC 006 and ETSI GS MEC 009

TABLE 3. Security activities of various standardization bodies.

have proposed one potential solution to protect subscribers from IMSI catching attacks in 5G networks.

During the standardization of 5G, strong privacy regulations and legislation should be taken into account. The regulatory approach can be classified into three types. First is government-level regulation, where governments mainly make country-specific privacy regulations and through multi-national organizations such as the United Nations (UN) and European Union (EU). Second is the industry level, where various industries and groups such as 3GPP and ETSI collaboratively draft the best principles and practices to protect privacy. Third is the consumer-level regulations, where desired privacy is ensured by considering consumers' requirements [7].

5G Security Standardization

5G security standardization is still in the drafting phase, and various key organizations are providing immense contributions toward its rapid development, as highlighted in Table 3. In March 2015, 3GPP set the deadline for defining 5G standards around 2020. The same year, NGMN published a white paper on 5G [6] that covered a wide range of topics including virtualization, privacy, radio architecture, availability, and IoT, among others. For 5G security standardization, the NGMN P1 WS1 5G security group is mainly gathering requirements and providing their suggestions. In January 2016, the SA3 group [3] of 3GPP started working to standardize the 5G security aspects and provide contributions to 5G-PPP initiated projects. The major task was to propose 5G security architecture by analyzing threats and requirements. The SA3 group of 3GPP covers all security aspects including RAN security, authentication mechanisms, and network slicing, among others [1].

The Open Networking Foundation (ONF) is dedicated to accelerating the adoption of SDN and NFV, and publishes technical specifications including specifications for security of these technologies [4]. Also, the ETSI Industry Specification Group (ISG) for NFV Security (ISG NFV SEC) is responsible for security specifications of NFV platforms. ISG NFV SEC has highlighted the need for a standard interface in ETSI NFV architecture for adding security functions that can react to potential security threats in real time. In 2014, ESTI MEC ISG was formed to look after MEC security standards and empower NFV capabilities within the RAN to deliver security and robustness. The NGMN 5G security group is working on identifying the security requirements for MEC and proposing corresponding recommendations. Regarding privacy, subscription privacy is one of the core security areas focused in 3GPP SA3. For example, privacy enhanced identity protection deals with safeguarding the IMSI from adversaries on the air interface. SA3 is also taking valuable input from the FSAG group GSMA to identify subscriber privacy challenges [1]. Furthermore, the standards suggested by the Internet Engineering Task Force (IETF) will be critical because 5G will use various Internet protocols. The International Telecommunication Union (ITU) continuously gathers contributions from regional organizations like ETSI and ARIB, and proposes recommendations for the standardization organizations.

Conclusion

5G will use mobile clouds, SDN, and NFV to meet the challenges of massive connectivity, flexibility, and costs. With all their benefits, these technologies also have inherent security challenges. Therefore, in this article we have highlighted the main security challenges that can become more threatening in 5G unless they are properly addressed. We have also presented the potential security mechanisms and solutions for those challenges. 5G still has to be deployed; thus, the security challenges in these technologies and their solutions will become more vivid. However, the integration of IoT seems to raise more security concerns, specifically in terms of privacy. Therefore, novel security solutions need to be sought out that use the development in, for example, artificial intelligence and context awareness to enable proactive network forensics and response leveraging the programmability enabled by SDN and runtime, but need-based security service insertion in various network perimeters using NFV.

Acknowledgment

This work was supported by TEKES Finland and the Academy of Finland under projects The Naked Approach, Towards Digital Paradise, and SecureConnect. Andrei Gurtov was supported by

the Center for Industrial Information Technology (CENIIT).

References

[1] 5G-PPP Security WG, "5G-PPP Phase1 Security Landscape," white paper, 2017.

[2] P. Mishra *et al.*, "Out-VM Monitoring for Malicious Network Packet Detection in Cloud," *2017 ISEA Asia Security and Privacy*, Jan. 2017, pp. 1–10.

[3] 3GPP (May 2017) SA3-Security; http://www.3gpp. org/Specifications-groups/sa-plenary/54-sa3-security.

[4] I. Ahmad *et al.*, "Security in Software Defined Networks: A Survey," *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 4, 2015, pp. 2317–46.

[5] A. Shaik *et al.*, "Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems," *CoRR*, vol. abs/1510.07563, 2015; http://arxiv.org/abs/1510.07563

[6] NGMN Alliance, NGMN 5G white paper, 2015.

[7] I. Ahmad *et al.*, "5G security: Analysis of Threats and Solutions," *2017 IEEE Conf. Standards for Commun. and Networking*, Sept 2017, pp. 193–99.

[8] W. Yang and C. Fung, "A Survey on Security in Network Functions Virtualization," *2016 IEEE NetSoft Conf. and Wksps.*, June 2016, pp. 15–19.

[9] A. van Cleeff, W. Pieters, and R. J. Wieringa, "Security Implications of Virtualization: A Literature Study," *2009 Int'l. Conf. Computational Science and Engineering*, vol. 3, Aug 2009, pp. 353–58.

[10] P. Kulkarni, R. Khanai, and G. Bindagi, "Security Frameworks for Mobile Cloud Computing: A Survey," *2016 Int'l. Conf. Electrical, Electronics, and Optimization Techniques*, Mar. 2016, pp. 2507–11.

[11] R. Roman, J. Lopez, and M. Mambo, "Mobile Edge Computing, Fog: A Survey and Analysis of Security Threats and Challenges," *Future Generation Computer Systems*, 2016.

[12] K. Norrman, M. Näslund, and E. Dubrova, "Protecting IMSI and User Privacy in 5G Networks," *Proc. 9th EAI Int'l. Conf. Mobile Multimedia Communications*. Inst. for Comp. Sci., Social-Informatics, and Telecommun. Engineering, 2016, pp. 159–66.

[13] S. Sezer *et al.*, "Are We Ready for SDN? Implementation Challenges for Software-Defined Networks," *IEEE Commun. Mag.*, vol. 51, no. 7, July 2013, pp. 36–43.

[14] B. Jaeger, "Security Orchestrator: Introducing a Security Orchestrator in the Context of the ETSI NFV Reference Architecture," *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug. 2015, pp. 1255–60.

[15] H. Lauer and N. Kuntze, "Hypervisor-Based Attestation of Virtual Environments," *2016 Int'l. IEEE Conf. Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress*, July 2016, pp. 333–40.

[16] A. Chonka and J. Abawajy, "Detecting and Mitigating HX-DoS Attacks Against Cloud Web Services," *2012 15th Int'l. Conf. Network-Based Info. Systems*, Sept 2012, pp. 429–34.

[17] A. Ahmed and E. Ahmed, "A Survey on Mobile Edge Computing," *2016 10th Int'l. Conf. IEEE Intelligent Systems and Control*, 2016, pp. 1–8.

Biographies

IJAZ AHMAD (ijaz.ahmad@oulu.fi) is a Ph.D. student at the Centre for Wireless Communications, University of Oulu.

TANESH KUMAR (tanesh.kumar@oulu.fi) is a Ph.D. student at the Centre for Wireless Communications, University of Oulu.

MADHUSANKA LIYANAGE (madhusanka.liyanage@oulu.fi) is a project manager at the Centre for Wireless Communications, University of Oulu.

JUDE OKWUIBE (jude.okwuibe@oulu.fi) is a Ph.D. student at the Centre for Wireless Communications, University of Oulu.

MIKA YLIANTTILA (mika.ylianttila@oulu.fi) is a professor at the Centre for Wireless Communications, University of Oulu.

ANDREI GURTOV (gurtov@acm.org) is a professor at Linköping University, Sweden.

Novel security solutions need to be sought out that use the development in, for example, artificial intelligence and context awareness, to enable proactive network forensics and response leveraging the programmability enabled by SDN and runtime, yet, need-based security service insertion in various network perimeters using NFV.