Security Challenges of Small Cell as a Service in Virtualized Mobile Edge Computing Environments

Vassilios Vassilakis, Emmanouil Panaousis, Haralambos Mouratidis

Security Challenges of Small Cell as a Service in Virtualized Mobile Edge Computing Environments

Vassilios Vassilakis[1], Emmanouil Panaousis[2], and Haralambos Mouratidis[2]

[1] School of Computing and Engineering, University of West London, UK
{vasileios.vasilakis@uwl.ac.uk}
[2] Secure and Dependable Software Systems Research Cluster
School of Computing, Engineering, and Mathematics, University of Brighton, UK
{e.panaousis,h.mouratidis}@brighton.ac.uk

Abstract. Research on next-generation 5G wireless networks is currently attracting a lot of attention in both academia and industry. While 5G development and standardization activities are still at their early stage, it is widely acknowledged that 5G systems are going to extensively rely on *dense small cell deployments*, which would exploit *infrastructure* and *network functions virtualization* (NFV), and push the network intelligence towards network edges by embracing the concept of *mobile edge computing* (MEC). As security will be a fundamental enabling factor of *small cell as a service* (SCaaS) in 5G networks, we present the most prominent *threats* and *vulnerabilities* against a broad range of *targets*. As far as the related work is concerned, to the best of our knowledge, this paper is the first to investigate security challenges at the intersection of SCaaS, NFV, and MEC. It is also the first paper that proposes a set of criteria to facilitate a clear and effective taxonomy of security challenges of main elements of 5G networks. Our analysis can serve as a staring point towards the development of appropriate 5G security solutions. These will have crucial effect on legal and regulatory frameworks as well as on decisions of businesses, governments, and end-users.

Keywords: Security, small cell as a service, network functions virtualization, mobile edge computing, 5G.

1 Introduction

Rapid advances in the industry of handheld devices and mobile applications has fuelled the penetration of interactive and ubiquitous web-based services into almost every aspect of our lives. At the same time, users expect almost *zero-delay* and *infinite-capacity* experience. However, current 4G technologies reveal their inherent limitations, as discussed in [1]. This is true, for both human-to-human and machine-to-machine (M2M) communications [2, 3]. Both will require radically different architectural design, network protocols, and business models. To achieve that, researchers are working towards the next-generation 5G wireless

networks aiming to offer high-speed and personalized services to both humans and machines, when and where needed [4].

To support highly dense areas where a vast number of users want to access the network infrastructure, deployment of *small cells* (SCs) is envisioned. These can co-operate with traditional macro cells, to provide high levels of user experience [5, 6]. SCs will play a significant role in 5G networks, which are expected to be highly heterogeneous. That is, future 5G networks will comprise a variety of *collocated resources*, such as indoor and outdoor SCs, macro cell sites, and WiFi access points. Another driving force in 5G will be the advances in *hardware virtualization* technologies, which can facilitate the realization of the *small cell as a service* (SCaaS) concept [7].

The primary benefit that comes with SCaaS is that independent actors own and lease their cellular infrastructure to multiple *mobile network operators* (MNOs); therefore SCaaS provides a natural *multi-tenant* support, by allowing each MNO to be a tenant of the infrastructure and getting a "slice" of the physical SC infrastructure [8]. This is not the only advantage that SCaaS can offer to 5G. We can leverage SCaaS to provide high-speed, low-latency communications, and to offload the mobile core network traffic and computation to the network edge, giving life to the concept of *mobile edge computing* (MEC) and *fog computing*, which has recently attained attention [9–11].

Finally, another important technology of 5G is *network function virtualization* (NFV), which: decouples network functions from their physical location; offers flexible function migration; and distributes functions across different network components [12, 13]. It is worth mentioning that NFV can be further enhanced with the concept of *software-defined networking* (SDN) decoupling the control plane from the data plane [14, 15].

Although 5G network technologies are still taking shape, and standardization activities are still ongoing, it is expected that SCaaS, MEC, NFV, and SDN are going to be *integral parts* of 5G networks. For example, the recently started EU 5G-PPP project SESAME (Small cEllS coordinAtion for Multi-tenancy and Edge services) aims to provide solutions in the field [16]. Another, EU 5G-PPP project called 5G-ENSURE aims at defining the security architecture and developing security enablers for 5G [17].

1.1 Contribution

In order to investigate the security challenges of 5G networks, one must look into the security issues of its elements and their interaction. In this paper, we identify the security *threats* and *vulnerabilities* of SCaaS, NFV, and MEC, as a first step towards a more comprehensive 5G security analysis that we intend to undertake in future work. Our analysis is focused on SC infrastructure, whose security is a very crucial issue because SCs are expected to support both MNOs and end-users, who cannot tolerate financial losses or data privacy violations, and therefore they seek the highest possible security guarantees. Having a comprehensive view and taxonomy of security threats and vulnerabilities in SCs, is prerequisite for architecting optimal security solutions.

1.2 State-of-the-art

The state-of-the-art within the field of 5G security is in its infancy. Mantas *et al.* [18] investigated some of the potential threats and attacks against the main components of 5G systems. The authors mainly focus on security issues related to the user equipment, and although they briefly go beyond that, they do not present security issues that open up as a result of SCaaS, NFV, and MEC. Apart from this, they lack a clear list of criteria that facilitate the creation of a taxonomy of threats and vulnerabilities. In an even less depth, in terms of threats and vulnerabilities investigation, Fang *et al.* [19] propose a high level security framework for 5G networks, without paying particular attention in the technologies we consider in our paper, here.

Within the realm of physical layer security for 5G networks, Yang *et al.* [20] investigate the security challenges that open up when considering the technologies of heterogeneous networks, massive multiple-input multiple-output (MIMO), and millimeter wave, which are likely to be important parts of 5G networks. Furthermore, Duan and Wang [21] investigated the security challenges, focusing mainly on authentication handover and privacy protection in 5G. The contribution of these papers is not directly comparable to ours, here, and we only referred to them for completeness.

1.3 Outline

This paper is structured as follows. In Section 2, we describe a generic, high-level architecture for SCaaS. We also present our assumptions regarding the SCaaS security and the adversarial model. Section 3 discusses the security challenges of SCaaS and reveals major security threats that arise due to (i) network resources and functions being virtualized, (ii) the adoption of MEC, and (iii) the incorporation of NFV and SDN concepts. We also present a set of criteria to facilitate the taxonomy of security challenges and discuss their mutual dependencies. Finally, Section 4 concludes this paper by summarizing its contributions and presenting our plans for future work.

2 Prerequisites

2.1 System Architecture

Our considered high-level system architecture for SCaaS is in line with [22] and has been illustrated in Fig. 1. The main elements of this architecture include: infrastructure virtualization; NFV; SDN, and MEC. According to the SC infrastructure virtualization principle, the *physical SC* is sliced into a number of *virtual SCs* (VSCs). To enable MEC services, each VSC is equipped with a MEC server, which has the ability to communicate with the Cloud and to execute some of the functions that are traditionally hosted in the Cloud. Furthermore, multiple MEC servers can be clustered to provide enhanced services in the form of a *light data centre* (Light DC) and managed by the *virtual resources manager*

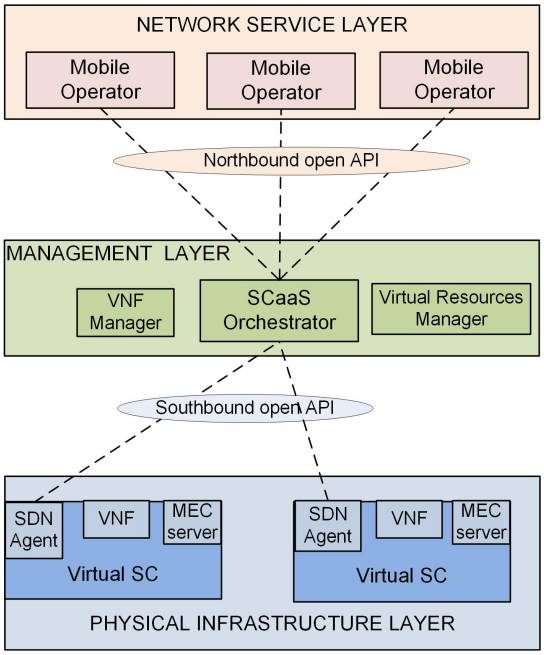

Fig. 1. High-level system architecture for Small Cell as a Service.

(VRM). Each VSC also accommodates a number of *virtual network functions* (VNFs) and it is managed by the *SCaaS Orchestrator* via an SDN agent. Above the *management layer* there is the *service layer*, in which multiple tenants (i.e., MNOs) are accommodated.

The network service layer accommodates MNOs who are benefited from having *on-demand access* to SC resources without owing the physical infrastructure. MNOs communicate with the SCaaS Orchestrator, located in the management layer, who orchestrates the allocation of virtual resources to MNOs. The SCaaS Orchestrator closely collaborates with the VRM, which is responsible for the management of virtual resources of MEC servers in the physical infrastructure layer. The control of VSCs is performed via SDN agents using some appropriate SDN protocol, such as the MobileFlow [23]. Finally, various network functions, such as *firewalling* and *deep packet inspection* (DPI), are virtualized using the NFV technology and managed by the VNF Manager. A specific realization of the architecture of Fig. 1 could be, for example, the SESAME architecture [16], [24]. However, in this work we intentionally keep our considered system architecture as generic as possible in order to accommodate a wide range of implementation choices of the SCaaS concept.

2.2 Security Assumptions

To identify the *security challenges* of the investigated system architecture, we first introduce our *security assumptions*, regarding the baseline security of the system. One of main assumptions is the *physical security* of SC infrastructure and *hardware integrity*. More specifically, we assume that *hardware tampering* is prevented by appropriate security controls deployed by the SC infrastructure owner [25], and that the Cloud provider has ensured the physical security of the Cloud infrastructure and of the data centres (e.g., according to the recommendations from the Cloud Security Alliance [26]). The existence of physical attacks will be considered in our future works. Note that due to space limitations, in this paper, we do not consider attacks that are initiated from the Cloud side. Instead, we focus on attacks originated either from *user equipment* (UE) or from the SC infrastructure itself (e.g., from a malicious tenant or a compromised system component). Besides, modern literature has investigated Cloud-originated attacks and identified the main Cloud security challenges [27,28]; developed adequate security solutions [29]; and proposed methods for Cloud provider selection based on security and privacy requirements [30].

2.3 Adversarial Model

Our analysis adopts the widely-used Dolev-Yao adversarial model [31]. According to this model, the cellular network is represented as a *set of abstract entities* that exchange messages and the adversary is capable of overhearing, intercepting, and synthesizing any message and they are only limited by the constraints of the deployed cryptographic methods. For example, the adversary neither is able to forge the message authentication code (MAC) nor has the means to obtain the plaintext of encrypted messages.

Apart from the above, we enrich the adversarial model by considering *compromised nodes*. The adversary per se could be a *legitimate tenant* interacting with network entities by using valid credentials and having *privileged access* to virtualized resources. Yet the adversary might run any management application in their VSC or specify various policies within its virtual domain, which is defined as a cluster of VSCs allocated to the same tenant.

3 Security Challenges

In this section we discuss the security challenges that emerge from the adoption of the SCaaS concept, using as a reference the architecture of Fig. 1. We adopt the widely-used threat taxonomy proposed in [32] and identify the security challenges that arise due to specific architectural characteristics and interaction of various components and layers of SCaaS. The different security challenges can be classified according to five categories.

– **Precondition**: What are the necessary conditions to be met before the adversary is able to launch the attack? For example, if the attack requires

a particular service running on the victim side, the existence of an open interface is a precondition; another case is when the adversary has some particular access rights.
- **Vulnerability**: What are the vulnerabilities of the system components or the network interfaces, which can be exploited by the adversary? For example, some components could be implemented in software with flaws or non-adequate cryptographic mechanisms could be in place [33].
- **Target**: Which components or interfaces are the potential attack targets? Other considerations include the communication layer the adversary targets and whether he aims to compromise the control or the data plane or both.
- **Method**: What are the various attack methods, tools and techniques that the adversary might use? In the same category we examine whether the adversary follows an active (e.g., replay attack) or passive strategy (e.g., passive reconnaissance).
- **Effect**: What is the impact of a successful attack on the victimized system component or network interface? Impact might be, for instance, unavailability of some services, financial costs, and leakage of sensitive data.

Below, we identify specific security challenges for each of the aforementioned five categories.

3.1 Precondition

Regarding precondition, the following types of requirements might be valid for the adversary.

Specific configuration: In some cases, to launch an attack against a component, the adversary requires that this component has specific exploitable configuration or runs a specific software. For example, a precondition for a *denial-of-service* (DoS) attack [34, 35] can be specific configuration of the VRM with regard to the allocation of resources to tenants. Yet, some flaws in the resource allocation algorithm can allow the adversary to prevent a tenant from accessing its portion of virtual resources. Also, other types of DoS attacks may exploit the broadband nature of the wireless medium. For example, malicious interference at the physical layer, even using off-the-shelf hardware, can cause packet collisions at the media access control (MAC) layer [36].

Ubiquitous connectivity: If a network component or function can be accessed via the public Internet, this may be exploited by a *remote adversary*. The adversary will require a way of discovering the vulnerable component and sending messages via control or data plane. By moving the network intelligence to the network edge, as with the Light DC, a pool of MEC servers is usually available for UEs to be connected via the Internet using conventional methods. Also, the *physical location* and *distributed or centralised nature* of the SCaaS Orchestrator could be an important factor influencing its security. For example, one way to realise the SCaaS Orchestrator is as a distributed function with its instances located across multiple SCs (e.g., in the form of a VNF). In such case, if public Internet is used to remotely configure various SCaaS policies, this can be exploited by the adversary.

Privileged access: The adversary has privileged access to some parts of the network components or functions. The privileged access can be either at the administrator level or at the user level. For example, the adversary may be a legitimate UE receiving service from its MNO, with the latter being a legitimate tenant of the SC network infrastructure. Also, the emerging *bring your own device* (BYOD) trend in modern enterprises, constitutes many conventional security solutions incapable of protecting the private network [37]. For example, a Trojan horse that infected an employee's device, can bypass the security of the corporate firewall.

3.2 Vulnerabilitiy

SDN controller weaknesses: Some vulnerabilities are caused by flaws in software and programming errors. This may lead, for example, to control flow attacks [38] and buffer overflow attacks [39]. This issue is particularly important in the context of next-generation wireless networks, where the trend is to implement the control plane in software and to virtualize network functions [40, 41]

Flaws of NFV platforms: The virtualised environment itself could introduce many potential security problems [42]. In particular, flaws of the virtualisation platform in place, may constitute the guest operating system (OS) vulnerable to side-channel attacks. For example, weak isolation between host and guest OSs may lead to a side-channel attack based on cache leakage [43].

Cloud based management: Some vulnerabilities stem from the Cloud based management nature of certain network components. The Cloud based interface used for configuration and updates could be used as a potential attack channel.

Weak access control and authentication: Use of weak or default passwords could be easily exploited by an adversary and should be avoided. Also, some components may have hard-coded passwords, which can be exploited by the adversary towards the establishment of backdoor access; stealthy or not.

Weak cryptographic mechanisms: Weaknesses or improper use of cryptographic mechanisms may lead to security breaches in authentication processes and data confidentiality. Also, the generation of cryptographic keys shouldn't rely on weak random number generators. Other security problems may arise due to communication protocols that use weak cryptographic primitives. Hence, it should be ensured that the cryptographic security controls are in place [44]. This is to say that any adopted public-key scheme that enables the encryption of the communications among SC, UE, and the Cloud, should be sufficiently secure.

3.3 Target

Physical small cell infrastructure: Attacks on the specific piece of hardware that is used in the cellular network [45]. For example the physical SC infrastructure can be a target of hardware attacks. While it is a common practice for the users to authenticate themselves to mobile devices before using them, the devices usually do not do the same to users. This means that there is a risk for the authentication secret to be revealed to a non-authenticated device. Hence, an

attacker may try to obtain the secret, by replacing the device with a malicious one [46].

NFV-based management system: Some attacks initiated inside virtualised environments may aim at taking control of the Hypervisor [47]. Also, the SCaaS Orchestrator is an attractive attack target due to being in the "‘middle" of the system model architecture, as well as other components of the *management layer*, such as the VNF Manager. Finally, impersonation by the adversary of one of the VNFs or the MEC server when communicating with the management layer could be a potential threat.

VM-hosted operating system: Both host and guest OS may be targeted [48], and to alleviate the impact of such an attack, adequate isolation must be enforced between guest virtual machines (VMs), as well as between the host and guest VMs. The adversary could attempt to break the isolation by exploiting, e.g., some flaws of the virtualisation platform in use [49].

Mobility management entity: In some cases, the attack does not target a specific layer in the system architecture, but it rather aims to *take control* of a specific network entity, either physical or virtual, such as the mobility management entity (MME). Protecting against such kind of attacks will be even more difficult when a distributed MME is introduced in 5G networks [50].

MEC-based application: A certain application that runs, for instance, on a MEC server is a potential attack target. This does not affect only the SC that hosts the compromised MEC server. Due to clustering of MEC servers into the Light DC, as discussed in Section 2, and their communication with the Cloud, a compromised MEC server can be used as a door to attack other network entities and components. Also, the adversary may attempt to attack the network service isolation. This may result in the violations of limits for virtual resources or unauthorized use of other tenants' resources. We assume that the adversary can attempt to impersonate another tenant or another network entity. Also, it may attempt to decrypt the intercepted messages.

MobileFlow protocol: A usual attack target is the protocol used for communication, management or control purposes, such as the MobileFlow protocol [23]. For example, the southbound and northbound interfaces, shown in Fig. 1, are potential attack targets when attempting to hijack the communication of the SCaaS Orchestrator with VSCs and MNOs. Also, the communication within the SC infrastructure could be targeted; for example, between the management and the physical infrastructure layer. This may enable an adversary to alter the network policies and create attack channels. In particular, possible attack targets are (i) communication of the VNF Manager with VNFs in a SC; and (ii) communication of the VRM with MEC servers. Hence, the adversary may try to alter or disable legitimate policies and cause attacks such as DoS and privilege escalation or to violate the privacy of other tenants data.

3.4 Method

Reverse engineering: The adversary collects and analyses sensitive information about the network and its functionality. She may also try to decompile the soft-

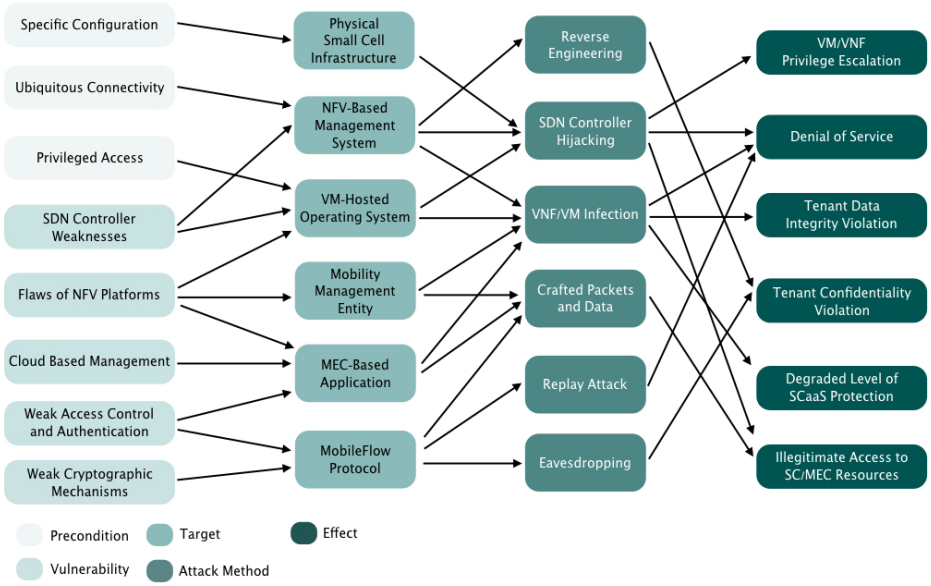

Fig. 2. Dependencies among security challenges of Small Cell as a Service in virtualised MEC environments.

ware to retrieve the source code. This may enable the adversary to identify vulnerabilities in the software or network interfaces. In some cases, the adversary may exploit weaknesses in the implemented access control mechanisms and exploit a device through normal usage, i.e., as a legitimate user. Other reverse-engineering techniques may target users' sensitive personal information. For example, the increasing popularity of mobile crowdsourcing and mobile sensing projects [51] may enable an attacker to exploit various personal data such as the user location, mobility patterns or web browsing habits [52].

SDN controller hijacking: By exploiting the SDN controller implementation weaknesses, the adversary tries to divert the control flows to a controlled device [53]. Then the captured messages can be *discarded* preventing the data plane entities from proper operation. In a more advanced case, the captured messages may be manipulated with a special purpose code and sent into the network.

VNF/VM infection: The adversary infects a virtual network component, such as a VM or a VNF, with a malicious code. In this way, an unwanted and potentially harmful functionality can be added to the affected system and can modify its behaviour. The future trends in *network softwarization* and *programmability* [54, 55] make this attack method particularly important. Furthermore, in a typical virtualised environment, guest VMs are expected to run in complete isolation. This means that a VM is not able to interact with the host and other

VMs nor is able to monitor or control them in any way. This isolation is typically enforced by the Hypervisor. However, such virtualised environments may be vulnerable to the so-called *VM escape attack* [56], which is a process of breaking out the aforementioned VM isolation. This can be achieved for example by installing malware on the Hypervisor [57].

Crafted packets and data: The adversary can attack communication and control protocols by injecting crafted packets or crafted input data. These actions may exploit, for example, the parsing vulnerabilities of protocol implementations [58].

Replay attack: The adversary captures packets or packet fragments and replays them at appropriate times aiming to cause protocol failures or other types of disruption and confusion.

Eavesdropping: The adversary observes messages exchanged between various network components or functions. In this way, sensitive information can be obtained, especially if this information is weakly protected by cryptographic mechanisms or not protected at all.

3.5 Effect

VM/VNF privilege escalation: The adversary, who has already some level of limited access privilege (e.g., to a VM or a VNF), manages to gain more privilege. This may have very serious negative effects for SDN-based mobile networks [59] as well as for the emerging *Internet of things* (IoT) technologies [60].

Denial of service: A potential outcome of attacks can be DoS leading to switched off or malfunctioning SC, or unavailable MEC servers. Also, a DoS attack against the SCaaS Orchestrator can cause service disruption and data loss. Yet, in a multi-tenant environment, security implications that may arise due weak isolation between tenants may allow adversaries to compromise more than one tenants upon compromising one of the other tenants. Furthermore, a DoS attack may be launched from within the SC [11].

Tenant data integrity violation: Some data or code, including various configuration settings and security policies, can be altered. This is a particularly important issue in a virtualised multi-tenant environment. It must be taken into account that some tenants could be malicious. Hence, adequate data isolation for different tenants must be ensured. This could be done, for example at the database level or at the hardware level.

Tenant confidentiality violation: In some cases sensitive information of a tenant may be leaked and made available to the adversary or to a malicious tenant.

Degraded level of SCaaS protection: A possible effect can be the degradation of SCaaS infrastructure protection. This can be achieved, for example, by altering the security policies or switching to weaker cryptographic mechanisms.

Illegitimate access to SC/MEC resources: The adversary gains illegitimate access to the SC resources (physical or virtual) or MEC environment. Given the increasing trend of outsourcing data and applications, an adequate security solution must ensure that only authorised entities gain access. Also, the insider

threat should be considered and appropriate mechanisms must be put in place for preventing service providers form misusing tenants' data.

In Fig. 2, we show, in the form of a directed graph, an example of possible dependencies of these categories. For instance, to cause DoS, the adversary could select VM/VNF infection as an attack method. To achieve that, malware could be injected in the management system (e.g., to the VRM or the VNF Manager in Fig. 1), a VM-hosted OS, or a MEC-based application (i.e., by compromising a MEC server), which constitute the potential attack targets. To target, e.g., the VM-hosted OS, the adversary could possibly exploit the SDN controller weaknesses or flaws of NFV platforms, and take advantage of any privileged access rights.

4 Conclusion

In this paper, we have identified the most important security challenges of SCaaS in virtualized environments of 5G networks. We envision that novel technologies, such as NFV, SDN, and MEC will be adopted in the future and will play an important role in the SCaaS realization. We have summarized the main security challenges that (i) open up with these technologies and (ii) arise due to the interoperability among them, which enables SCaaS. We have highlighted the necessary conditions for the adversary to be able to launch an attack; the vulnerabilities of various system components and network interfaces that can be exploited by the adversary; potential targets of attacks, such as management systems and applications; various methods and techniques that can be used by the adversary; and finally, the impact of the attacks on an SCaaS provider and its tenants. In future work, we intend to study and evaluate prominent security solutions developed for protecting virtualized SC networks and systems per se, focusing on NFV, SDN, and MEC. This security assessment will use this paper, here, as a basis.

Acknowledgements. The present work has been performed in the scope of the SESAME ("*Small cEllS coordinAtion for Multi-tenancy and Edge services*") European Research Project and has been supported by the Commission of the European Communities (*5G-PPP/H2020, Grant Agreement No. 671596*).

References

1. Boccardi, F., Heath, R.W., Lozano, A., Marzetta, T.L., Popovski, P.: Five disruptive technology directions for 5G. IEEE Commun. Mag. 52 (2), 74-80 (2014).
2. Andreev, S. *et al.*: Understanding the IoT connectivity landscape: A contemporary M2M radio technology roadmap. IEEE Commun. Mag. 53 (9), 32-40 (2015).
3. Vardakas, J.S., Zorba, N., Skianis, C., Verikoukis, C.V.: Performance analysis of M2M communication networks for QoS-differentiated smart grid applications. In: IEEE Globecom Workshops (GC Wkshps), 1-6 (2015).

4. Patel, S., Malhar, C., Kapadiya, K.: 5G: Future mobile technology - vision 2020. Int. J. of Comp. Applicat. 54 (17), 6-10 (2012).
5. Andrews, J.G.: Seven ways that HetNets are a cellular paradigm shift. IEEE Commun. Mag. 51 (3), 136-144 (2013).
6. Osseiran, A. *et al.*: Scenarios for 5G mobile and wireless communications: The vision of the METIS project. IEEE Commun. Mag. 52 (5), 26-35 (2014).
7. Trakas, P., Adelantado, F., Verikoukis, C.: A novel learning mechanism for traffic offloading with small cell as a service. In: IEEE Int. Conf. on Commun. (ICC), London, U.K. (2015).
8. Giannoulakis, I. *et al.*: System architecture and aspects of SESAME: Small cEllS coordinAtion for Multi-tenancy and Edge services. In: 2nd IEEE Conference on Network Softwarization (NetSoft), Workshop on Software Defined 5G Networks (Soft5G), Seoul, Korea (2016).
9. Soldani, D., Manzalini, A.: A 5G infrastructure for anything-as-a-service. J. of Telecommun. Syst. & Manag. 3 (2), 1-10 (2014).
10. Vaquero, L.M., Rodero-Merino, L.: Finding your way in the fog: Towards a comprehensive definition of fog computing. ACM SIGCOMM Comput. Commun. Review 44 (5), 27-32 (2014).
11. Roman, R., Lopez, J. and Mambo, M.: Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. arXiv preprint arXiv:1602.00484 (2016).
12. Han, B., Gopalakrishnan, V., Ji, L., Lee, S.: Network function virtualization: Challenges and opportunities for innovations. IEEE Commun. Mag. 53 (2), 90-97 (2015).
13. Yu, R., Xue, G., Kilari, V., Zhang, X.: Network function virtualization in the multi-tenant cloud. IEEE Netw. 29 (3), 42-47 (2015).
14. Ameigeiras, P.*et al.*: Link-level access cloud architecture design based on SDN for 5G networks. IEEE Netw. 29 (2), 24-31 (2015).
15. Sun, S., Kadoch, M., Gong, L., Rong, B.: Integrating network function virtualization with SDR and SDN for 4G/5G networks. IEEE Netw. 29 (3), 54-59 (2015).
16. EC H2020 Small sElls coordinAtion for Multi-tenancy and Edge services (SESAME) Project, https://5g-ppp.eu/sesame/ [July 2016].
17. EC H2020 5G-ENSURE, https://5g-ppp.eu/5g-ensure/ [July 2016].
18. Mantas, G. *et al.*: Security for 5G Communications. Fundamentals of 5G Mobile Netw., John Wiley & Sons, Ltd, 2015.
19. Fang, Q., Weijie, Z., Guojun, W., Hui, F.: Unified security architecture research for 5G wireless system. In: 11th Web Information System and Application Conference, Tianjin, China (2014).
20. Yang, N. *et al.*: Safeguarding 5G wireless communication networks using physical layer security. IEEE Commun. Mag. 53 (4), 20-27 (2015).
21. Duan, X., Wang, X.: Authentication handover and privacy protection in 5G HetNets using software-defined networking. IEEE Commun. Mag. 53 (4), 28-35 (2015).
22. Vassilakis, V.G., Moscholios, I.D., Alzahrani, B.A., Logothetis, M.D.: A software-defined architecture for next-generation cellular networks. In: IEEE Int. Conf. on Commun. (ICC), Kuala Lumpur, Malaysia (2016).
23. Pentikousis, K., Wang, Y., Hu, W.: Mobileflow: Toward software-defined mobile networks. IEEE Commun. Mag. 51 (7), 44-53 (2013).
24. Fajardo, J.O. *et al.*: Introducing mobile edge computing capabilities through distributed 5G cloud enabled small cells. Mobile Networks and Applications, Springer US, 1-11 (2016).
25. Skorobogatov, S.: Physical attacks and tamper resistance. Introduction to Hardware Security and Trust, Springer, New York, 143-173 (2012).

26. Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, Dec. (2009).
27. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. J. of Netw. and Comput. Applicat. 34 (1), 1-11 (2011).
28. Ryan, M.D.: Cloud computing security: The scientific challenge, and a survey of solutions. J. of Syst. and Sotw. 86 (9), 2263-2268 (2013).
29. Zissis, D., Lekkas, D.: Addressing cloud computing security issues. Future Generation Comput. Syst. 28 (3), 583-592 (2012).
30. Mouratidis, H., Islam, S., Kalloniatis, C., Gritzalis, S.: A framework to support selection of cloud providers based on security and privacy requirements. J. of Syst. and Softw. 86 (9), 2276-2293 (2013).
31. Dolev, D., Yao, A.C., On the security of public key protocols. IEEE Trans. Inf. Theory 29 (2), 198-208 (1983).
32. Papp, D., Ma, Z., Buttyan, L.: Embedded systems security: Threats, vulnerabilities, and attack taxonomy. In: 13th Annu. Conf. on Priv., Secur. and Trust, Izmir, Turkey (2015).
33. Mihaljevic, M.J., Gangopadhyay, S., Paul, G., Imai, H.: Generic cryptographic weakness of k-normal Boolean functions in certain stream ciphers and cryptanalysis of grain-128. Periodica Mathematica Hungarica 65 (2), 205-227 (2012).
34. Gobbo, N., Merlo, A., Migliardi, M.: A denial of service attack to GSM networks via attach procedure. In: International Conference on Availability, Reliability, and Security, 361-376. Springer, Heidelberg (2013).
35. Merlo, A., Migliardi, M., Gobbo, N., Palmieri, F., Castiglione, A.: A denial of service attack to UMTS networks using SIM-less devices. IEEE Transactions on Dependable and Secure Computing, 11(3), 280-291 (2014).
36. Fragkiadakis, A., Askoxylakis, I., Chatziadam, P.: Denial-of-service attacks in wireless networks using off-the-shelf hardware. In: Distributed, Ambient, and Pervasive Interactions, Springer International Publishing, 427-438 (2014).
37. Armando, A., Costa, G., Merlo, A.: Bring your own device, securely. In: 28th ACM Symp. on Appl. Comp., Coimbra, Portugal (2013).
38. Davi. L. *et al.*: MoCFI: A framework to mitigate control-flow attacks on smartphones. In: 19th Annu. Netw. & Distr. Syst. Secur. Symp., San Diego, USA (2012).
39. Wang, L.B., Wei, G.H., Li, Z.: Research of defense scheme against buffer overflow attack in embedded system. J. of Comput. Appl 12 (2012).
40. Wang, H., Chen, S., Xu, H., Ai, M., Shi, Y.: SoftNet: A software defined decentralized mobile network architecture toward 5G. IEEE Netw. 29 (2), 16-22 (2015).
41. Vassilakis, V.G., Moscholios, I.D., Alzahrani, B.A., Logothetis, M.D.: On the security of software-defined next-generation cellular networks. In: IEICE Inf. and Commun. Tech. Forum (ICTF), Patras, Greece (2016).
42. Kotsovinos, E.: Virtualization: Blessing or curse? Commun. of the ACM 54 (1), 61-65 (2011).
43. Barthe, G., Betarte, G, Campo, J.D., Luna, C.: Cache-leakage resilient OS isolation in an idealized model of virtualization. In: 25th IEEE Comp. Secur. Foundations Symp., Cambridge, USA (2012).
44. Bhargavan, K., Fournet, C., Kohlweiss, M., Pironti, A., Strub, P.: Implementing TLS with verified cryptographic security. In: 34th IEEE Symp. Secur. Privacy, San Francisco, USA (2013).
45. Rostami, M., Koushanfar, F., Rajendran, J., Karri, R.: Hardware security: Threat models and metrics. In: 32nd IEEE/ACM Int. Conf. on Comput.-Aided Design, San Jose, CA (2013).

46. Findling, R.D., Mayrhofer, R.: Towards device-to-user authentication: Protecting against phishing hardware by ensuring mobile device authenticity using vibration patterns. In: 14th ACM Int. Conf. on Mobile and Ubiquitous Multimedia, 131-135 (2015).
47. Perez-Botero, D., Szefer, J., Lee, R.B.: Characterizing hypervisor vulnerabilities in cloud computing servers. In: 8th ACM Int. Workshop on Security in Cloud Computing, Hangzhou, China, 3-10 (2013).
48. Suzaki, K., Iijima, K., Yagi, T., Artho, C.: Memory deduplication as a threat to the guest OS. In: 4th ACM Europ. Workshop on System Security, Salzburg, Austria (2011).
49. Hoesing, M.T.: Virtualization security assessment. Inf. Secur. J.: A Global Perspective 18 (3), 124-130 (2009).
50. Giust, F., Cominardi, L., Bernardos, C.: Distributed mobility management for future 5G networks: Overview and analysis of existing approaches. IEEE Commun. Mag. 53 (1), 142-149 (2015).
51. Chen, P.Y., Cheng, S.M., Ting, P.S., Lien, C.W., Chu, F.J.: When crowdsourcing meets mobile sensing: A social network perspective. IEEE Commun. Mag. 53 (10), 157-163 (2015).
52. Han, Q., Liang, S., Zhang, H.: Mobile cloud sensing, big data, and 5G networks make an intelligent and smart world. IEEE Netw. 29 (2), 40-45 (2015).
53. Goktas, E., Athanasopoulos, E., Bos, H., Portokalidis, G.: Out of control: Overcoming control-flow integrity. In: 35th IEEE Symp. Secur. Privacy, San Jose, CA (2014).
54. Nikaein, N. *et al.*: Network store: exploring slicing in future 5G networks. In: 10th Int. ACM Workshop on Mobility in the Evolving Internet Architecture, Paris, France (2015).
55. Chin, W.H., Fan, Z., Haines, R.: Emerging technologies and research challenges for 5G wireless networks. IEEE Wireless Commun. 21 (2), 106-112 (2014).
56. Luo, S., Lin, Z., Chen, X., Yang, Z., Chen, J.: Virtualization security for cloud computing service. In: 4th Int. Conf. on Cloud and Service Computing (CSC), 174-179 (2011).
57. Oyama, Y., Giang, T.T., Chubachi, Y., Shinagawa, T., Kato, K.: Detecting malware signatures in a thin hypervisor. In: 27th Annu. ACM Symp. on Appl. Comput., Trento, Italy (2012).
58. Hu, C., Li, Z., Ma, J., Guo, T., Shi, Z.: File parsing vulnerability detection with symbolic execution. In: IEEE 6th Int. Symp. on Theoretical Aspects of Softw. Eng., Beijing, China (2012).
59. Chen, M., Qian, Y., Mao, S., Tang, W., Yang, X.: Software-defined mobile networks security. Mobile Networks and Applications, 1-15 (2015).
60. Roy, S., Manoj, B.S.: IoT enablers and their security and privacy issues. In: Internet of Things (IoT) in 5G Mobile Technologies, Springer International Publishing, 449-482 (2016).