Journal of Convergence for Information Technology
Vol. 11. No. 10, pp. 144-150, 2021
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2021.11.10.144

Threat Diagnostic Checklists of Security Service in 5G Communication Network Virtualization Environment

Jin-Keun Hong
Professor, FCTech/Division of Smart IT Engineering, Baekseok University

5G 통신 네트워크 가상화 환경에서 보안 서비스의 위협 진단 체크리스트

홍진근
백석대학교 미래기술융합연구소/스마트IT공학부 교수

Abstract The purpose of this paper is to review the direction of the slicing security policy, which is a major consideration in the context of standardization in 5G communication network security, to derive security vulnerability diagnosis items, and to present about analyzing and presenting the issues of discussion for 5G communication network virtualization. As for the research method, the direction of virtualization security policy of 5G communication network of ENISA (European Union Agency for Cybersecurity), a European core security research institute, and research contents such as virtualization security policy and vulnerability analysis of 5G communication network from related journals were used for analysis. In the research result of this paper, the security structure in virtualization security of 5G communication network is arranged, and security threats and risk management factors are derived. In addition, vulnerability diagnosis items were derived for each security service in the risk management area. The contribution of this study is to summarize the security threat items in 5G communication network virtualization security that is still being discussed, to be able to gain insights of the direction of European 5G communication network cybersecurity, and to derive vulnerabilities diagnosis items to be considered for virtualization security of 5G communication network. In addition, the results of this study can be used as basic data to develop vulnerability diagnosis items for virtualization security of domestic 5G communication networks. In the future, it is necessary to study the detailed diagnosis process for the vulnerability diagnosis items of 5G communication network virtualization security.

Key Words : Communication, Network, Security, Risk, Virtualization

요 약 본 논문의 연구목적은 5G 통신네트워크 보안에서 표준화가 진행되고 있는 상황에서 주요 고려 사항인 슬라이싱 보안 정책에 대한 방향을 검토하고, 5G 통신 네트워크 가상화의 보안 취약점 진단 항목들을 도출하며, 위험관리에 대한 주요 논의 사항들을 분석하고 제시하는데 있다. 연구방법은 유럽 핵심보안 연구기관인 ENISA(European Union Agency for Cybersecurity)의 5G 통신네트워크의 가상화 보안 정책 방향과, 국외 주요 관련 저널로부터 5G 통신네트워크의 가상화 보안정책과 취약점 분석 등의 연구 내용을 분석에 활용하였다. 본 논문의 연구 결과에서는 5G 통신 네트워크의 가상화 보안에서 보안구조를 정리하였고, 보안 위협들과 위협관리 요소를 도출하였다. 또한 위험관리 영역에서 보안 서비스별로 취약점 진단 항목들을 도출하였다. 본 연구의 기여도는 여전히 논의 되고 있는 5G 통신 네트워크 가상화 보안에서 보안 위협 항목들을 요약하였다는 것과, 유럽의 5G 통신네트워크 사이버보안 방향을 파악 할 수 있었다는 것, 그리고 5G 통신 네트워크의 가상화 보안에 고려되어야 하는 취약점 진단 항목들을 도출하였다는 데 있다. 아울러 본 연구의 결과는 국내 5G 통신네트워크 가상화 보안을 위한 취약점 진단 항목들을 개발하는데 기초 자료로 활용 될 수 있다. 향후 5G 통신네트워크 가상화 보안의 취약점 진단 항목에 대한 상세한 진단 프로세스를 연구하는 것이 필요하다.

주제어 : 통신, 네트워크, 보안, 위험, 가상화

*This paper is supported of funding of Project of Baekseok University
*Corresponding Author : Jin-Keun Hong(jkhong@bu.ac.kr)
Received September 6, 2021
Revised September 29, 2021
Accepted October 20, 2021
Published October 28, 2021

1. Introduction

The 5G system has unique advantages for each frequency band. 5G In 5G communications, spectrum sharing is becoming more common as more devices compete for access to the same spectrum. However, in 5G communication, spectrum sharing can cause an attacker to interfere with less important communication paths or adversely affect important communication networks in terms of security. Of course, these discussions require a discussion on the characteristics of network slicing virtualization environment in 5G communication or risk management in security [1]. Therefore, it is essential to understand the intentions of attackers in terms of security threats in 5G communication networks. Therefore, in this paper, we will discuss security issues in slice virtualization of 5G communication network environment. In 5G communication, the slicing technique is used to take advantage of the strength of virtualization. And this gives security advantages. Research on the topic of network slicing in 5G communication networks is needed. So far, there has been no specific case of providing vulnerability diagnosis items for slicing security threats. This study is ongoing. Therefore, this study intends to study threat factors, risk assessment, and vulnerability diagnosis items for each security service, along with understanding of virtualization of 5G communication network from this point of view.

Another research background lies in the relatively insufficient research on risk management in the 5G slicing virtualization environment, and the lack of research on the derivation of related vulnerability diagnosis items. Therefore, this study focused on the slicing security structure and security threats in the virtualized environment of 5G networks, which European cyber security organizations are focusing on, and vulnerability diagnosis items that should be considered in risk management.

5G communication is an infrastructure communication service that supports multi edge convergence computing. However, security threats in the 5G communication network's virtualization environment can affect the security of MEC convergence services. Therefore, in order to support secure MEC convergence service, it is necessary to diagnose security service threats in the 5G communication's virtualization environment and prepare countermeasures.

In this paper, in Chapter 2, we describes about the security structure in the virtualized slicing environment of 5G communication networks, and in Chapter 3, we analysis at risk assessment and security threats in this environment. And in Chapter 4, vulnerability diagnosis items to be considered in the security risk management of 5G communication network virtualization are derived and presented for each security service.

2. Related researches

In general, the risk assessment process consists of risk identification, risk analysis, risk assessment, and risk action. Hazard identification is the process of figuring out which risks are occurring and when, where, and how they occurred. However, the reason for performing this risk identification is to determine the cause, place, and method of potential loss or damage. Originally, risk management consists in identifying assets, identifying the risks that impair them, and predicting the damage that may arise from these risks.

Relevant research on risk management in 5G

is as follows. Abdullah et al. review the risks considered in the 5G application environment from the health impact and cyber security perspectives [2]. Young B et al. are interested in potential security issues in the 5G environment and introduce new security functions [3]. Yong Wu et al. studied information security decisions of companies considering the interdependence of security risks between companies. However, in this study, an effective security risk mechanism to be considered by companies is presented [4]. Miltiadis et al. emphasize the characteristic that vulnerability prediction can identify and mitigate security risks in software development life cycle, thus facilitating secure software development. In this study, the ability of a common technical debt indicator to indicate the security risk of software products is studied [5]. Michael et al. are researching risk analysis of software product development and marketing focusing on the application of fuzzy logic. In this study, the probability of occurrence of a major risk event is considered, and the threat level of the relevant risk factor is estimated based on fuzzy logic [6]. Jaspreet Singh et al. studied a software-defined boundary -based multi level security framework for network function virtualization (NFV), and claim that the proposed NFV software defined perimeter structure is resistant to denial of service(DoS) attacks [7]. Other related studies include modeling and tools for security threats, namely Process for attack simulation and threat analysis(PASTA) [8], Trika [9], attack tree [10], UMLSec [11], Operationally critical threat, asset and vulnerability evaluation(OCTAVE) [12], misuse cases [13], Common Criteria(CC) There are studies on [14], Damage Reproducibility Exploitability Affected-Use Discoverability(DREAD) which is a threat modeling program developed by Microsoft [15], Cyber operations rapid assessment security (CORAS) [16], and Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privileges(STRIDE) [17].

The focus of this paper is to derive a security service threat diagnosis list in the 5G communication's virtualization environment. However, as this topic is under research, it is necessary to derive a diagnostic list. Until now, there is no threat diagnosis list related to 5G communication's virtualization environment threats, so it was difficult to reference in research. In order to solve this problem, the European ENISA study judged to be highly relevant was referred to, and diagnostic items were developed based on the security principles considered to be valid from this study.

The related studies reviewed so far include research on risk management and evaluation, and threat modeling for software products including 5G.

3. 5G Network Virtualization Security

3.1 5G NFV Security Architecture

The 5G domain (TS 23.101) consists of a USIM domain, a mobile equipment domain, an access network domain, a core network domain, a transit network domain, and a service network domain. The infrastructure domain is composed of AN and CN domains, and the user equipment (ME) domain is composed of a USIM domain and an ME domain. The following Fig. 1 shows the security structure in the 5G NFV environment.

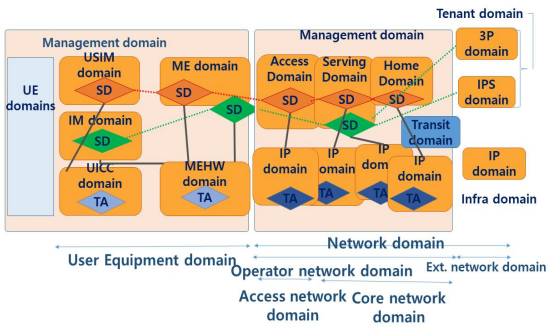

Fig. 1. 5G NFV architecture

In this domain structure, a functional and logical mapping relationship is indicated. In the management domain, the slice domain is connected to (user device domain) (UICC domain) - USIM domain - ME domain - (network domain) access domain - service domain - home domain. Also it is connected between node to node as follows: (user device domain) (MEHW domain) - IM domain - ME domain - (network domain) service domain - (IP domain) - 3P or IPS domain. Upper-lower domains are internetworked according to characteristics, and slice domains perform unique functions according to services for each slice. However, distinct slices must consider their own security breach factors. Here, SD is a slice domain, TA is a trust anchor, and IP is an infrastructure provider. Chapter 3 analysis the risk management process in 5G NFV/SDN and classifies security threats.

3.2 5G NFV/SDN security threats

ENISA classifies 5G NFV/SDN security threats as security threats in detail as follows.

- Security threats, which is caused by malicious and abnormal use, include information manipulation/data deception, SW/firmware exploits, DoS, remote SDN application exploits, SDN API exploits, malicious software, illegal activities, and illegal virtualization operations.

- Disaster threats include natural disasters and environmental disasters.

- Law and business threats include violations of SLAs, violations of the law, judicial decisions/court orders, improper use of personal information, and illegal competition.

- Physical attack threats include fraud, sabotage, vandalism, theft, information disclosure, illegal access, and terrorism.

- Threats of downtime include loss of resources, loss of support services, and loss of network connectivity.

- Eavesdropping/ interception/ hijacking threats include traffic diversion, side channel attacks, identity spoofing, software/firmware exploits, memory scraping, virtualized illegal operations, traffic sniffing, mobile user hijacking, man-in-the-middle attacks, and information interception.

- Device failure/malfunction threats include device or system failure, communication link failure or interruption, main power supply failure or interruption, service provider failure or interruption, and device malfunction threats.

- Threats of damage or loss of devices include human error, misuse by administrators, inconsistent and confusing maintenance, data loss, and threats of damage by second parties.

3.3 Risk Management Process of 5G Environment

1) 5G Assets

ENISA classifies assets into seven categories. The categories are data plane (network element, communication medium), control plane (SW/ HW/ Data), application plane (SW/ HW), service provider's IT infrastructure (IT infrastructure, billing system, operator data, end-user data), Network service provider's physical infrastructure (facility, power), SDN users (end

user data, SLA), and humans (SDN administrator/ application developer, network service operator, end-user application developer/ administrator, end service provider, end user) is done

2) Evaluation and Mitigation of Risk

Risk analysis is a process of predicting risk levels by determining probabilities, etc. Risk assessment is the process of comparing criteria and setting priorities. Finally, risk action is the process of establishing an action plan from identification and assessment.

The risk mitigation for each item should be derived integrally for each slice, and assuming that the risk index has an arbitrary graph for each time period, it can be represented as shown in Fig. 2.

Security integration risk mitigation (f) per slice is determined by individual risk factors (cost, schedule (time), performance, security).

Therefore, it can be expressed like Equation 1, as follows; the integrated risk index f is sum of the cost risk index f1 (max~min), the risk index for a certain period f2 (max~min), the performance risk index f3 (max~min), and the security risk index f4(max~min), etc.

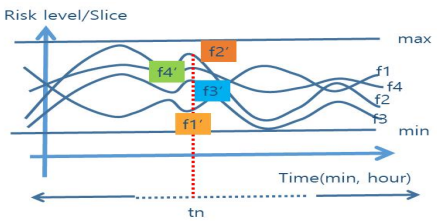

Fig. 2. Risk level vs. threats(f1~f4) in a Slice

$$f_T = f1 + f2 + f3 + f4 \quad (1)$$

Here, assuming that the individual risk index is determined between max and min, the risk index fT at time tn is determined as the sum of f1' + f2' + f3' + f4'. Of course, the functions f1, f2, f3, and f4 can be any step value between max and min. In addition, depending on the service, the risk index that can occur in the entire slice appears as a result of adding the risk index of individual fS1 to fSn for S1 to Sn. Therefore, the risk index that can occur in the entire slice (eg, n = 1 to 4) at time tn can be expressed as in Equation 2 and Fig. 2.

$$fS_T = fS1' + fS2' + fS3' + fS4' \quad (\text{in tn interval}) \quad (2)$$

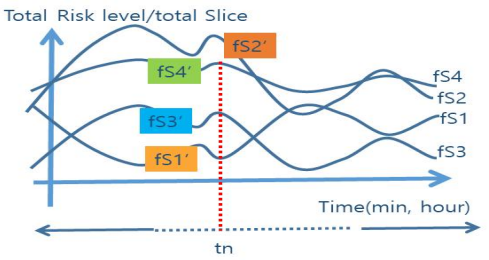

Fig. 3. Risk level vs. threats(fS1~fS4) in Total Slice(n=1~4)

The topic of the checklist for threat diagnosis in the 5G communication's virtualization environment derived from this study, is an item currently being researched. The proposed threat diagnosis checklist is presented to be suitable for the 5G communication's virtualization environment by referring to various guides including standard proposals, and since it refers to the guide presented by the European accredited ENISA research institute, it can be said that the proposed list has validity.

4. Proposed Vulnerability Diagnostic Checklists of 5G Network Virtualization Environment

In this study, we propose vulnerability diagnosis items for threats by 5 types of security services as follows: access control, authentication, non reputation, confidentiality, communication in Fig. 4.

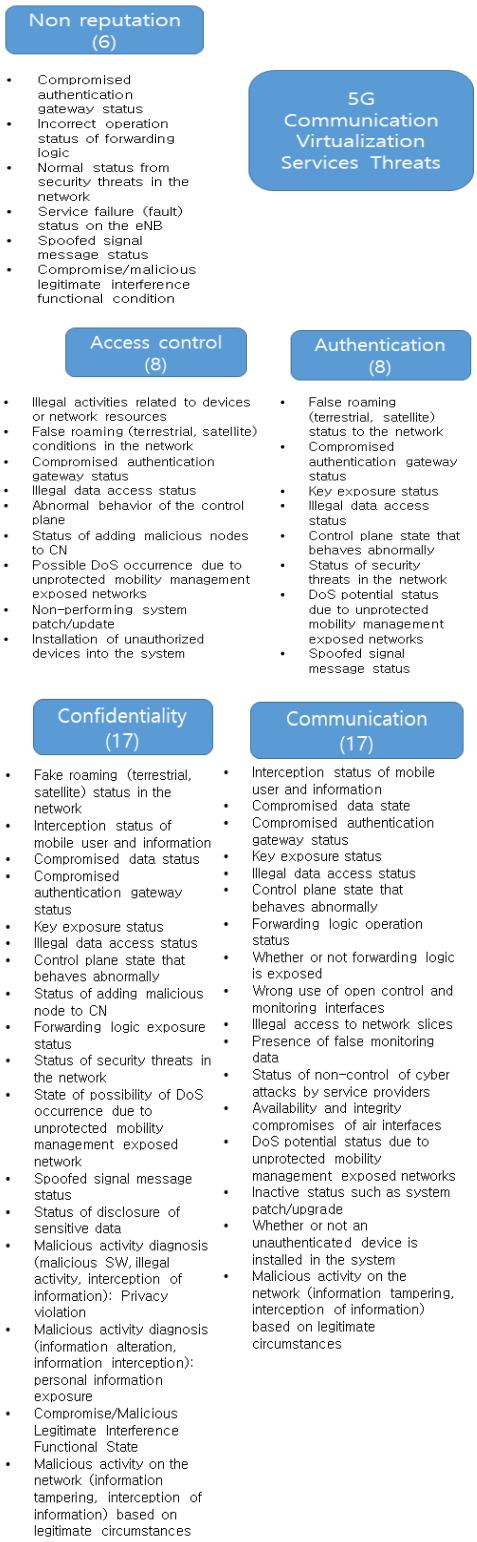

Fig. 4. 5G Communication Virtualization Services Threats

5. Conclusion

This paper has focused on the risk management and vulnerability diagnosis items to be considered in the 5G communication network virtualization environment. In this paper, the main focus is on the understanding of the slicing security structure, security threats, and risk management factors in 5G network virtualization that ENISA emphasizes. In the risk management element, risk assessment and security threat elements were examined, and vulnerability diagnosis items to be considered for each security service were derived and presented. Therefore, in order to support secure MEC convergence service, it is necessary to diagnose security service threats in the 5G communication's virtualization environment and prepare countermeasures.

REFERENCES

[1] R. Khondoker. (2018). *SDN and NFV Security: Security Analysis of Software-Defined Networking and Network Function Virtualization* (Vol. 30). Springer LNCS Publishing.

[2] Abdullah Jameel Rowaished, Mohammed Mubarak Ghefaily (2021). An Overview into Applications and Risks in 5G NR Technology. Journal of IJECE, 8(3), 1-2.
DOI : 10.14445/23488549/IJECE-V8I3P103

[3] B. Young & E. B. ChoiMatthew. (2021). The Security Risks and Challenges of 5G Communications. *International Journal of Cyber Research and Education, 3(2),* 36-53.
DOI : 10.4018/IJCRE.2021070104

[4] Y. Wu, L. Wang, D. Cheng & T. Dai (2021). Information security decisions of firms considering security risk interdependency. *Journal of Expert Systems with Applications, 178,* 1-15.
DOI : 10.1016/j.eswa.2021.114990

[5] M. Siavvas, D. Tsoukalas, M. Jankovic & D. Kehagias & D. Tzovaras. (2020). Technical debt as an indicator of software security risk: a machine learning approach for software development enterprises. *Enterprise Information Systems,* 1-43.
DOI : 10.1080/17517575.2020.1824017

[6] M. Kataev, L. Bulysheva, L. Xu, Y. Ekhlakov, N. Permyakova & V. Jovanovic. (2020). Fuzzy model estimation of the risk factors impact on the target of promotion of the software product. *Enterprise Information Systems, 14(6),* 797-81. DOI : 10.1080/17517575.2020.1713407

[7] J. Singh, A. Refaey & A. Shami. (2020). Multilevel Security Framework for NFV Based on Software Defined Perimeter. *Journal of IEEE Network, 34(5),* 114-119. DOI : 10.1109/MNET.011.1900563

[8] T. UcedaVelez. (2012). Real World Threat Modeling Using the PASTA Methodology. *OWASP. Technical report.* https://www.owasp.org/images/a/aa/AppSecEU2012_PASTA.pdf.

[9] P. Saitta, B. Larcom & M. Eddington. (2005) Trike v1 methodology document. *Draft, work in progress.* http:// dymaxion.org/trike/Trike_v1_Methodology_Documentdraft.pdf.

[10] B. Schneier. (1999). *Attack trees.* Dr. Dobb's J. Technical report(Online). https://www.schneier.com/academic/archives/1999/12/attack_trees.html.

[11] J. Jurjens. (2002). UMLsec: Extending UML for secure systems development. *In International Conference on The Unified Modeling Language* (pp. 412-425). Springer, Berlin, Heidelberg. DOI : 10.1007/3-540-45800-X_32

[12] C. Alberts et al. (2003). *Introduction to the OCTAVE approach.* Carnegie Mellon University, Pittsburgh, PA

[13] I. Alexander. (2003). Misuse cases: use cases with hostile intent. *IEEE Software, 20(1),* 58-66. DOI : 10.1109/MS.2003.1159030

[14] H. Lohr et al. (2009). *Modeling trusted computing support in a protection profile for high assurance security kernels. In International conference on trusted computing* (pp. 45-62). Springer, Berlin, Heidelberg.

[15] D. Czagan. (2014). *Qualitative Risk Analysis with the DREAD Model.* Technical report(Online). http://resources.infosecinstitute.com/qualitative-risk-analysis-dread-model.

[16] M. S. Lund, B. Solhaug & K. Stolen. (2010). *Model-driven risk analysis: the CORAS approach.* Springer Science & Business Media.

[17] Cyral. (n.d.). *Threat Modeling With STRIDE*(Online). https://cyral.com/glossary/threat-modeling-with-stride/

[18] H. J. Mun & G. H. Choi & Y. C. Hwang. (2016). Countermeasure to underlying security threats in IoT communication. *Journal of Convergence for Information, 6(2),* 37-43. DOI : 10.22156/CS4SMB.2016.6.2.037

[19] J. H. Won, J. W. Hong & Y. Y. You. (2018). A study on the improvement of security threat analysis and response technology by IoT layer. *Journal of Convergence for information, 8(6),* 149-157. DOI : 10.22156/ CS4SMB.2018.8.6.149

[20] J. K. Cho. (2019). Study on improvement of vulnerability diagnosis items for PC security enhancement. *Journal of Covergence for Information, 9(3),* 1-7. DOI : 10.22156/ CS4SMB.2019.9.3.001

홍 진 근(Hong, Jin Keun) **[정회원]**

- 2000년 2월 : 경북대학교 정보통신공학(공학박사)
- 2004년 2월 : 국가보안기술연구소 근무
- 2004년 3월 ~ 현재 : 백석대학교 스마트IT공학부 교수

- 관심분야 : 미래융합기술, 미래보안기술
- E-Mail : jkhong@bu.ac.kr