Security Threat Analysis and Treatment Strategy for ORAN

C.T. Shen[1], Y.Y. Xiao[1], Y.W. Ma[1], J.L. Chen[1],
Cheng-Mou Chiang[2], S.J. Chen[2] and Y. C. Pan[2]
[1] Department of Electrical Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan
[2] Telecom Technology Center, Taipei, Taiwan

***Abstract*— Owing to the rapid development of networks and their gradual evolution from a closed architecture to an open architecture, the open radio access network (O-RAN) has been developed and offers new possibilities. However, because the O-RAN contains many new open interfaces, new information security issues may emerge. In this study, information security is discussed and a case analysis is performed based on vulnerability, exposed assets, threat models, security strategies, and test case modules. Missing authentication and authorization vulnerabilities are emphasized in this study. Affected assets such as O-RAN's Service Management and Orchestration(SMO), Near-RT RIC, and the O1 interface are discussed, and the threat model and security solution strategy are analyzed. Test cases are implemented to verify the effectiveness of the solution strategy. It is envisioned that the case analysis and development of missing authentication and authorization performed in this study will aid future mobile communication operators in addressing information security issues.**

***Keywords*— O-RAN, Security, Threat, Strategy, Test Case**

I. INTRODUCTION

The rapid development of the industry has resulted in the development of various innovative technologies and diversified application services, such as automated manufacturing and augmentation, as well as virtual reality. All types of new application services require a fast and stable network connection to enable the implementation of application services in various fields. As the fifth-generation (5G) technology continues to popularize, high speeds and high device connection capabilities will be afforded; however, it entails new information security threats to mobile communication networks. The beyond 5th Generation(B5G)/6th Genration(6G) network affords new business types, information technology-oriented network architectures and heterogeneous access networks, as well as other innovative technologies. The open radio access network (O-RAN) architecture designed by OSC affords open interfaces, software, and hardware. Although the system offers greater flexibility and application possibilities than other systems, various issues and challenges must be considered to ensure high information security. Therefore, B5G/6G must demonstrate more complete security protection capabilities to mitigate attacks and threats from new fields and technologies.

In an O-RAN network environment involving multiple security protection mechanisms, failure to verify or revise various vulnerabilities will result in threats and challenges to the network environment. Attackers can use various attack methods to attack and expose the system to threats. These organizations or individuals, who intend to exploit the vulnerabilities or trigger the vulnerabilities and methods, are known as threat agents. Threat actors in the O-RAN environment include cyber-criminals, insiders, hacktivists, cyber-terrorists, script kiddies, and the nation state.

This study focuses on the vulnerability and security of the O-RAN interface. The contributions of this study are as follows: First, a security threat analysis and processing strategy system architecture is proposed, and case studies are performed. Authentication and authorization vulnerabilities are defined, assets affected are considered, and five primary aspects for describing the protection level are introduced: confidentiality, integrity, availability, replay, and authentication. In addition, a threat model is designed to address vulnerability, identify treats, as well as analyze the threat description, threat actor, threat assets, and affected components. A security strategy for addressing vulnerability is proposed, in which a public key infrastructure is introduced to issue certificates and verify the identity via mutual authentication. A test case is designed to verify the security of nodes.

II. BACKGROUND KNOWLEDGE

The network architecture of the O-RAN differs from that of the 3GPP RAN. The 3GPP RAN architecture focuses on the components, interfaces, and technologies of the network environment. Meanwhile, the O-RAN architecture focuses on designing new specific network interfaces and service components to support software virtualization and containerization technologies, open-source strategies, artificial intelligence, and machine learning. Therefore, a literature review pertaining to the architecture security of 5G and O-RAN should be conducted. Table 1 shows the research documents relevant to 5G technologies and the O-RAN for ensuring information security.

TABLE 1. RESEARCH DOCUMENTS RELATED TO 5G AND O-RAN IN INFORMATION SECURITY

Topic of 5G	Contents
Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class (Release	This technical specification focuses on goals, requirements, and test case planning of security assurance specifications under the gNB network product category. The report describes the specific security function requirements of gNB and security requirements from specific threats. This report only focuses on the discussion of safety requirements between gNB and its

17) [1]	related devices.
Security for 5G Mobile Wireless Networks [2]	The study proposes a new 5G wireless network security architecture for identity management and authentication, as well as analyzes the handover process and signal load to demonstrate the advantages of the proposed wireless security architecture. However, to achieve the low-latency characteristics of 5G technology, only identity verification and management are discussed, whereas resilience between identity privacy and performance is not considered.
Intelligent Zero Trust Architecture for 5G/6G Tactical Networks: Principles, Challenges, and the Role of Machine Learning [3]	This study shows that in an environment where the 5G/6G network is untrustworthy, it is necessary to securely and mutually trust the dynamic authorization of network assets. Therefore, using the zero trust (ZT) principle to provide information security in the environment, a smart zero is proposed. A trust architecture, based on which artificial intelligence algorithms can be developed to provide information security, and an interface similar to the O-RAN architecture, are used to obtained necessary machine learning data. However, only the architecture and methods are proposed in the study, whereas the methods and minimum performance requirements of the system proposed are not analyzed or discussed.
5G Security Artifacts (DoS / DDoS and Authentication) [4]	The study, which is based on 5G cellular secure communication channels, investigates the effectiveness of traditional DOS/DDoS and authentication attacks in SDN and NFV environments. Furthermore, the DOS/DDOS mitigation strategy is proposed, and a strict authentication mechanism is introduced. However, only security mechanisms and strategies are proposed in the study; resilience in network performance is not achieved, and security protection mechanisms are not discussed.
A Survey on Security Aspects for 3GPP 5G Networks [5]	The study outlines the 3GPP 5G network architecture and security functions, as well as research pertaining to new features and technologies such as device-to-device communication and network slicing, which may result in security challenges. It also discusses security features, security requirements, or security vulnerabilities in the 3GPP 5G network; existing security solutions; and some unsolved research issues. However, only a brief discussion regarding existing problems and aspects to be addressed are provided, whereas practical content is not discussed comprehensively.
O-RAN Security Threat Modeling and Remediation Analysis [6]	This technical specification document focuses on the model construction of O-RAN security threats and the strategic design of threat solutions. The report describes the threats encountered and the establishment of models. Vulnerabilities as well as threat actors, profiles, scopes, and effects are discussed. The report provides general discussions and explanations, but does not include relevant cases and practical operating instructions.
Security in Open RAN [7]	This white paper presents a method to implement an open RAN architecture using a zero-trust security framework, which is a secure, open-interface method. New functions and control supported by the open RAN architecture that enable operators to effectively assess and manage security risks are discussed, and the method by which the O-RAN provides operators with end-to-end network security in high visibility and control ability is introduced. However, this white paper only provides an overview of ideas and architecture; it does not provide references and suggestions for practical content and practices.

To ensure the safety of O-RAN's important assets, five primary aspects, including confidentiality, integrity, availability, retransmission, and authentication, were selected in this study as the basis for the protection level. The purpose of confidentiality is to prevent unauthorized users from revealing the content of data intentionally or unintentionally. When confidential data are transmitted and stored, security agreement is used for encryption to ensure the confidentiality of data transmission and storage. Integrity is to prevent unauthorized users or processing procedures from tampering with the data. The documents used must be proven to be untampered with or infringed during the transmission or storage process to ensure the integrity of the data. Usability ensures that when users or applications access the system, the system's data and services remain available and are not affected by hardware or software conditions. Replay attacks are repeated transmission of data or delayed transmission of data for achieving malicious or deceptive purposes by the receiving device or application service. Authenticity ensures that the identification of a device or application service is its declared nature/characteristics.

III. Case Study

O-RAN's new open interfaces, such as the fronthaul interface, O1, O2, A1, and E2, are introduced. The purpose of introducing the new interface is to allow the RAN to realize the programmable execution of software. However, the introduction of the new interface introduces a new threat. Because these new interfaces do not satisfy the requirements of 3GPP specifications, attackers can use these new open

interfaces to attack the system, resulting in denial of service, data tampering, or data leakage, which indirectly affects the security of the entire system. However, the vulnerabilities that expose the interface to threats include incorrect or missing authentication and authorization processing, inaccuracy in the encryption process of sensitive data, incorrect integrity verification of sensitive data, inaccurate replay protection, inaccurate re-key verification, and incorrectly built interfaces.

Herein, a case study pertaining to O-RAN network information security is presented since new interfaces and O-RAN functions are incorporated. Each interface and function may result in different threat levels, and each threat will result in a certain effect. For all the aspects and assets, different security strategies and solutions will be applied for each threat. In addition, each security strategy requires a test case to verify whether it satisfies the security indicators.

Since each interface and function may encounter different threats and vulnerabilities, all possible vulnerabilities will be counted in the "vulnerability" aspect. We confirm the effects of assets from the perspective of security vulnerabilities, and identify the affected interfaces or functions which may be threatened.

In the threat model step, the description, source, identification, assets, and effect of the threat will be used to establish a model for the threat. After analyzing various threats, security strategies or solutions for each threat will be proposed in the security strategy step.

In the test case step, test cases will be designed for different scenarios and verified based on the security indicators for every threat to ensure that the security strategy satisfies the requirement. In this study, the security vulnerabilities and threats of O1 Interface, SMO, and Near-RT were investigated.

Figure 1 shows an illustration of the proposed case study, which includes vulnerability, exposed assets, threat model, security strategy and test case modules. The vulnerability module identifies the various vulnerabilities of the O-RAN communication network, which includes authentication, authorization, ciphering, integrity, replay, key reuse, implementation, and validate inputs. The exposed assets module identifies the assets and equipment exposed in the O-RAN network environment, including A1, E2, O1, Near-RT RIC, Non-RT RIC, O-CU, O-CU-CP, O-CU- UP, O-DU, O-RU, and RAN. The threat model is a security model based on vulnerabilities that can be used as a reference by stakeholders. Its content includes the threat description, threat agent, threat identifiers, and threat-asset-affected components. The security strategy is a vulnerability response strategy that can be used as a reference for strengthening system security and solving threats. It contains identity, credential, access management, network domain security, IPSec, and datagram transport layer security. The test case module verifies whether the solutions proposed by the security strategy effectively avoid threats. It includes security compliance testing, vulnerability testing, grey testing, and white-box testing.

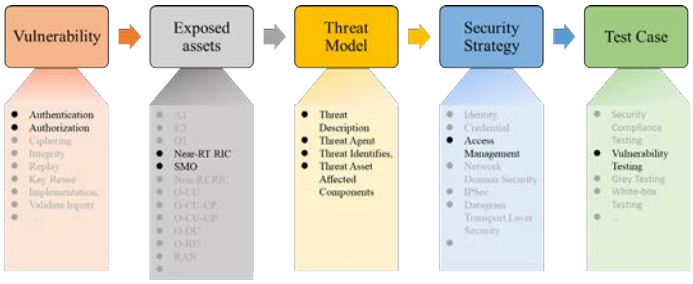

Figure 1. Security Threat Analysis and Treatment Strategy System Architecture

3.1. Missing Authentication and Authorization

The security vulnerability of missing authentication and authorization is defined and explained herein. Authentication is the process of determining whether an SMO or Near-RT RIC can transmit data, access the other party's resources, or perform operations based on the component's permissions and any permissions applicable to the resource or other access control specifications. Authorization verification is performed by the SMO responsible for the fault, configuration, accounting, performance, and security management. When the SMO or Near-RT RIC is required to transmit data, access the other party's resources, or perform operations through the O1 interface, authorization is necessitated. If the SMO does not perform authorization verification, the threat or attacker can directly pretend to be an SMO or a Near-RT RIC to transmit data, access resources, or perform operations that are prohibited.

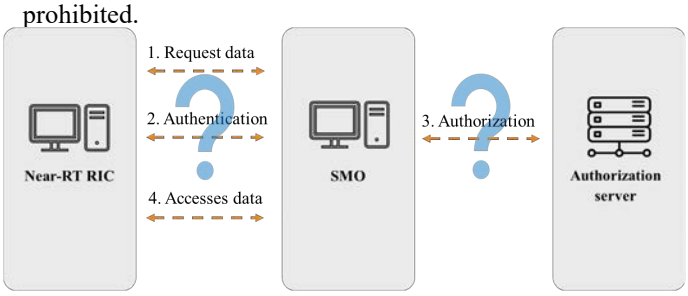

Figure 2. Missing Authentication and Authorization

3.2. Affect Assets and Security Protection Level

This vulnerability will expose components such as Near-RT RIC, Non-RT RIC, CU, DU, and SMO to threats, as shown in Figure 3. This threat exists in two modes, i.e., "at rest" and "in transit," and the security indicators that will be affected in both modes include confidentiality, integrity, and availability. If a person pretends to be an SMO or Near-RT RIC to access resources or after obtaining the resources, he intentionally or unintentionally reveals the content of the data that cause confidential data leakage; hence, the confidentiality of the security indicator will not be preserved. In addition, when an attacker pretends to be an SMO or a Near-RT RIC and tampers with the data that the component is preparing to transmit, the component will receive the wrong data. Consequently, the subsequent processing will be affected, and the integrity of the safety indicators will be compromised. However, a replay attack will cause network service delays and interrupt network services, thereby violating the

availability of the security indicators. In the transit mode, the replay and authenticity will be additionally affected. When an attacker pretends to be an SMO or Near-RT RIC, constantly accesses component resources, or delays the transmission of data and hence delays the network service, the replay principle of the security indicators may be violated. In addition, if the other party does not verify the identity of another party before mutually accessing resources, transmitting data, and executing instructions, then the other party accessing resources or transmitting data may be counterfeited by a third party, which may violate the authenticity of the security indicators. The affected assets are shown in Figure 1 and Table 2.

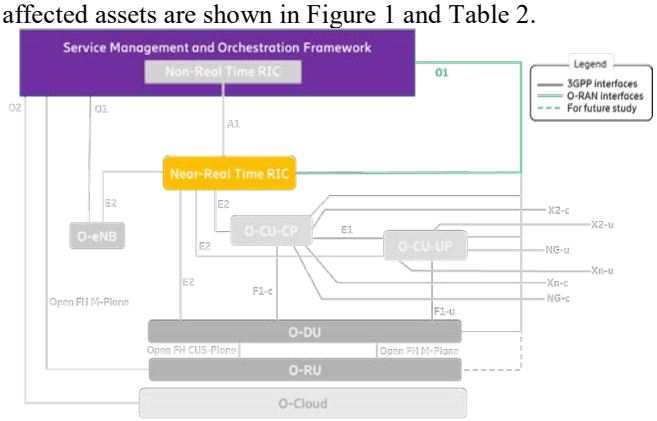

Figure 3. Affected Asset (AA-1)

TABLE 2. ASSETS' PROTECTION LEVEL

Asset ID	Component & Description	Interface	when		Protection Level				
			At rest	In transit	Confidentiality	Integrity	Availability	Replay	Authenticity
Data & Interface									
A-A1	Near-RT RIC, SMO	O1		X	X	X	X	X	X
			X		X	X	X		

3.3. *Threat Model*

The content of the threat model includes the threat description, threat agent, method for identifying the threat, threatened assets, and components that affect the threatened assets. This study focuses on the threat model designed for missing authentication and authorization, as shown in Table 3. When the threat has not yet occurred, the SMO and Near-RT RIC access each other's resources or perform operations through the O1 interface. The SMO must perform authentication verifications in advance and validate the identity before authorizing the device for operation. Cyber-criminals, insiders, hacktivists, cyber-terrorists, script kiddies, and the nation state are possible because no authentication record exists, and no inspection services or structures to perform authentication are introduced in advance; as such, the attack occurs when the SMO cannot prove the nature of both parties. This threatens assets such as data or instructions transmitted through the O1 interface, and directly affects components such as the SMO and Near-RT RIC.

TABLE 3. THREAT MODEL

Threat ID	T-O1-MA
Threat title	SMO did not perform authentication or authentication is invalid.
Threat Description	When SMO or Near-RT RIC accesses the other party's resources or performs operations through the O1 interface, SMO should perform identity verification in advance and confirm the validity of the verification before granting authorization.
Threat Agent	All
Identifies Vulnerability	• No identity verification record. • No service or structure (for example Certificate Authority) for identity verification has been introduced in advance. • During identity verification, SMO cannot prove the nature of both parties.
Threat Asset	A series of operations such as data transmission through the O1 interface, commands, or access to the other party's resources.
Affected Components	SMO, Near-RT RIC

3.4. *Security Strategy*

This study focuses on the security strategy required before an attack occurs and introduces the public key infrastructure architecture, which is composed of three main components: the certificate authority, registration authority, and certificate repository. Among them, the certificate authority is a trusted third party and is responsible for verifying the legitimacy of the public key in the public key system. First, the SMO and Near-RT RIC must register with the registration authority; subsequently, the registration authority will confirm the identities of the SMO and Near-RT RIC. After the confirmation is completed, the certificate authority signs the digital certificate to prove the authenticity of the public key, and then believes that the public key signed by it is valid and belongs to the SMO and Near-RT RIC; subsequently, it stores the public key in the certificate repository. Next, the certificate authority will issue a certificate to the applied SMO or Near-RT RIC. Finally, the two nodes possessing the certificate will conduct a two-way verification before commencing communication. The implementation framework is shown in Figure 4.

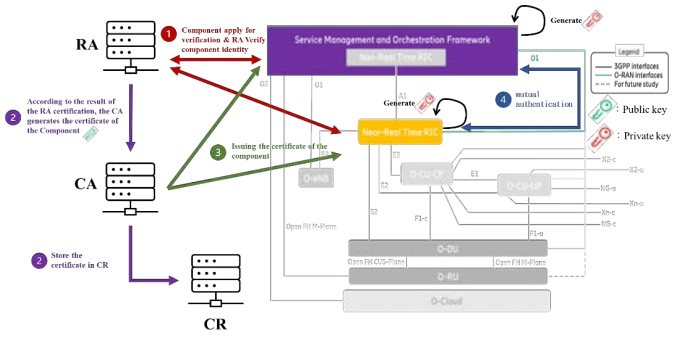

Figure 4. The O-RAN based architecture of adding Public Key Infrastructure

A detailed description of mutual authentication is shown in Figure 5. At the SMO, a keystore stores the private and public certificate of the SMO, whereas a truststore stores the public certificate of the Near-RT RIC. Meanwhile, at the Near-RT RIC, a keystore stores the private and public certificate of the Near-RT RIC, whereas a truststore stores the public key of the SMO. First, the SMO will send a "Hello" message to Near-RT RIC and request for Near-RT RIC resources. When the Near-RT RIC receives the "Hello" message, it will respond to the SMO with its public certificate (.crt) and return a "Hello". The SMO will verify the Near-RT RIC public certificate in its truststore. If the certificate is verified as valid and belongs to the Near-RT RIC, then SMO will generate a session key and use the public key of the Near-RT RIC to perform encryption. The Near-RT RIC will receive the session key sent by the SMO and then use its private key to decrypt the encrypted session key. Subsequently, Near-RT RIC will return the session key to the SMO and requests for a public key certificate from the SMO. The SMO sends its public key certificate to the Near-RT RIC for verification. If it is verified that the public key is valid and belongs to SMO, then the Near-RT RIC will use SMO's public key to encrypt the encrypted session key and return it to the SMO. When the SMO receives the encrypted session key sent by the Near-RT RIC, the SMO uses its private key to decrypt the encrypted session key, thereby completing the mutual authentication process.

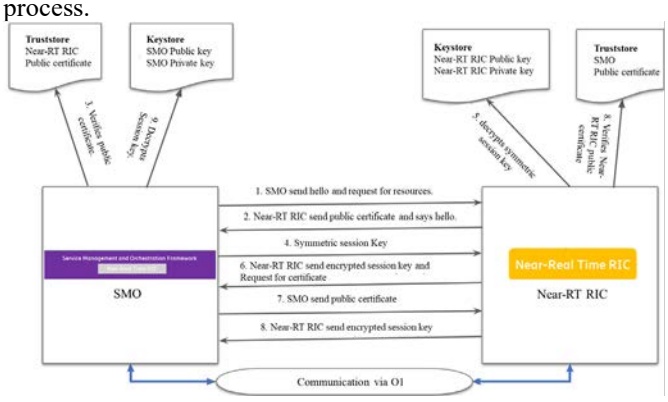

Figure 5. The flow of mutual authentication

3.5. Test Case

In this study, a test item was designed to verify the existence of a certificate, and a test item was written to test whether the SMO authenticates the visitor. Not only were the pre-conditions, inputs, execution conditions, and expected results of the test project detailed in a list of points, but also a case model was established to concretely instantiate the execution steps of the test project. First, an SMO and a Near-RT RIC were deployed and connected to each other. Subsequently, based on the conditions introduced by the certificate authority, two scenarios were designed. In Case I, the Near-RT RIC tester who has not obtained the certificate attempts to access the SMO. In Case ii, the Near-RT RIC tester who obtained the certificate attempts to access the SMO. Using this test case will ensure that both parties can verify each other's identity by verifying the certificate.

TABLE 4. TEST CASE CONFIRMING THE AUTHENTICATION ON EACH NODE

Missing authentication	
Test Title	Check whether the SMO verifies against the visitor.
Requirement	SMO needs to introduce certificate authority.
Requirement enhancements	None
Test Steps	Step 1. Write the test program, set the boolean value, the default is false (true means SMO has executed verification and the process is correct, false means no verification is executed or verification is invalid). **Case i** Step 2. Near-RT RIC testers who have not obtained the certificate try to access the SMO. Step 3. SMO should check whether it has received a valid certificate for Near-RT RIC. Step 4. If SMO does not obtain a certificate, SMO should deny access to the tester, and the program returns a status of true. Step 5. If the SMO does not obtain the certificate, but the tester can still access the SMO resources, it means that the SMO has not been verified or the verification is invalid, and the program returns a status of false. **Case ii** Step 6. The Near-RT RIC tester who obtained the certificate tries to access the SMO. Step 7. SMO should check whether it has received a valid certificate for Near-RT RIC. Step 8. If the certificate is received and the certificate is valid, the SMO

	should allow the tester to access itself, and the return status of the program is true. Step 9. If the certificate is received and the certificate is valid, but SMO still refuses the tester's access, there is no verification or the verification process is incorrect or missing, and the program returns a status of false.
Results	The return status is true: PASS
Remarks	If it returns false, check SMO or certificate authority and do follow-up processing.

With regard to confidentiality, integrity, and replay, because the SMO did not receive the certificate or the certificate is invalid, the SMO should refuse to accept any request from the tester, such as receiving data, accessing resources, and performing operations. With regard to availability, owing to the prevention of replay attacks, Internet services are typically available. With regard to authenticity, if the SMO has not received the Near-RT RIC public key signed by the trusted certificate authority, then it cannot confirm the authenticity and validity of the Near-RT RIC, and hence cannot identify a real Near-RT RIC.

IV. Conclusions and Future Work

Herein, the definition of missing authentication and authorization, the formulation of the category that affects the assets and security protection levels, the design of threat models, the implementation of security strategies, and the implementation of test cases were presented. In the upcoming studies, some test items for confidentiality, integrity, availability, retransmission, and authentication will be introduced to verify whether the security specifications are satisfied. Confidentiality will be tested by accessing Near-RT RIC resources, transmitting data, and performing operations. Integrity will be tested by sending tampered data and wrong commands to the Near-RT RIC. Meanwhile, availability and replay will be determined by continuously accessing resources such as the Near-RT RIC, as well as observing whether it causes network delays or interruptions to ascertain whether the security of this indicator is fulfilled. The test of authenticity is to detect whether the pretender can successfully deceive the authorization verification to determine the function of the component.

References

[1] "TS #33.511 Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class_v17.0.0," The 3rd Generation Partnership Project (3GPP), 2021.

[2] D. Fang, Y. Qian and R. Q. Hu, "Security for 5G Mobile Wireless Networks," IEEE Access, vol. 6, pp. 4850-4874, 2018.

[3] K. Ramezanpour and J. Jagannath. "Intelligent Zero Trust Architecture for 5G/6G Tactical Networks: Principles, Challenges, and the Role of Machine Learning," arXiv, 2021. (arXiv:2105.01478)

[4] M. A. Javed and S. khan Niazi, "5G Security Artifacts (DoS / DDoS and Authentication)," Proceedings of the International Conference on Communication Technologies, pp. 127-133, 2019.

[5] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu and L. Xiong, "A Survey on Security Aspects for 3GPP 5G Networks," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 170-195, 2020.

[6] "O-RAN Security Threat Modeling and Remediation Analysis," O-RAN Alliance, O-RAN.WG1.SFG.Threat-Model-v01.00, 2021.

[7] Security in Open RAN, https://www.altiostar.com/wp-content/uploads/2021/01/Open-RAN-Security-White-Paper-January-2021.pdf (Last visited: 2021/09/01)

Chih-Ting Shen is a student at National Taiwan University of Science and Technology. He recieved a bachelor's degree in software engineering and management from National Kaohsiung Normal University in Taiwan. His research interests include the Internet of Things, software engineering development, and network technology research and development.

Yu-Yi Xiao is currently studying the M.S. degree in Electrical Engineering of National Taiwan University of Science and Technology, Taipei, Taiwan. Her research interests include open radio access network, information security, and tactile internet.

Yi-Wei Ma is an assistant professor in National Taiwan University of Science and Technology. He received the PhD degree in the Department of Engineering Science at National Cheng Kung University, Tainan, Taiwan. His research interests include internet of things, cloud computing, future network and ubiquitous computing.

Jiann-Liang Chen received the Ph.D. degree in Electrical Engineering from National Taiwan University, Taipei, Taiwan in 1989. Since August 2008, he has been with the Department of Electrical Engineering of National Taiwan University of Science and Technology, where he is a professor now. His current research interests are directed at cellular mobility management and personal communication systems.

Cheng-Mou Chiang received the M.S. degree in Electrical Engineering of National Taiwan University of Science and Technology, Taipei, Taiwan. His research interests include network function virtualization, and software-defined network.

Shiang-Jiun Chen is working in TTC (Telcom Technology Center) Taiwan and received her PhD degree in the The University of Texas at Arlington. Her research interests include numerical analysis, software defined networking, software testing.

Yu-Chuan Pan is working in TTC (Telcom Technology Center) Taiwan and received the PhD degree in the Department of Information Management of National Taiwan University. His research interests include AIoT, Cyber security, Internet service, 5G and cloud computing.