Received 14 December 2023; revised 18 January 2024; accepted 3 February 2024. Date of publication 12 February 2024; date of current version 23 February 2024.

Digital Object Identifier 10.1109/OJCOMS.2024.3364840

Security Threats to xApps Access Control and E2 Interface in O-RAN

CHENG-FENG HUNG (Graduate Student Member, IEEE), YOU-RUN CHEN, CHI-HENG TSENG, AND SHIN-MING CHENG (Member, IEEE)

Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taipei 106335, Taiwan

CORRESPONDING AUTHOR: C.-F. HUNG (e-mail: d10915002@mail.ntust.edu.tw)

This work was supported in part by the Trend Micro Incorporated through the Project 5G and O-RAN Threat Resource Security Research and in part by the National Science and Technology Council (NSTC), Taiwan, under Grant 111-2221-E-011-067-MY3 and Grant 113-2923-E-011-005-MY2.

ABSTRACT Open Radio Access Networks (O-RANs) represent a novel wireless access network architecture that decomposes traditional RAN functions and makes them openly accessible. O-RANs enable real-time coordination, RAN performance optimization, and management through RAN Intelligent Controllers (RICs) and their related xApps. Due to the openness of O-RAN, developers have the flexibility to download various pre-developed xApps from the Internet for deployment. They can even develop their xApps to enhance the flexibility and innovation of the RAN. The current O-RAN official WG11 has defined numerous specifications for secure implementations. However, not only is accurately detecting malicious xApps a significant challenge, but the existing H-Release also does not fully adhere to the specifications in its implementation. This could potentially introduce security risks and threats. In this paper, we implement an experimental O-RAN H-Release environment and discover significant threats from the absence of specified access control permissions for xApps. Malicious attackers can illegally access APIs to utilize other services or launch attacks on legitimate xApps and E2 nodes through the E2 interface, potentially causing a complete RAN disruption. We used the identified vulnerabilities to design three attacks, providing detailed explanations and a comprehensive analysis of their impact on the system. Finally, we also submit the discovered threats to CVEs (CVE-2023-42358 and CVE-2023-41628), providing a reference for O-RAN officials to improve security in the future.

INDEX TERMS Authentication, malicious xApp, Open-RAN.

I. INTRODUCTION

OPEN Radio Access Network (O-RAN) is an open and interoperable wireless access network architecture. It enables connectivity and communication between devices from different vendors through open interfaces. Unlike 3GPP, O-RAN emphasizes multiparty collaboration, openness, and interoperability, removing barriers in traditional wireless infrastructure to encourage innovation and flexible deployment [1]. Hence, access control is crucial in implementing the O-RAN framework. The Open-RAN architecture of the O-RAN Alliance consists of several key components that interact through different interfaces for guidance, control, and information gathering [2]. Among them, Near-RT (real-time) RIC (RAN Intelligent Controllers) enables real-time control and optimization of RAN elements through the E2 interface. At the same time, xApps serve as open applications deployed on Near-RT RIC with highly customizable capabilities. xApps leverage information from the O-CU and O-DU, along with the computational power of machine learning algorithms, to detect, respond, and manage the RAN in real-time, closed-loop operation, enabling efficient wireless network control, dynamic resource allocation, and network optimization [3]. This offers a platform for vendors and developers to collaborate on innovation. However, it also brings up security concerns related to data transfer through interfaces [2].

The official O-RAN documentation [4], [5] enumerates a range of potential threats to O-RAN components and interfaces, including U-plane, S-Plane, and C-Plane attacks between O-RU and O-DU [6], malicious base station attacks against O-RU [7], malicious xApps attacks on Near-RT RIC [8], threats arising from the lack of authentication in

SMO and O1 [9], and threats to the A1 interface between Non-RT RIC and Near-RT RIC [10]. These threats have been discussed from the O-RAN architecture and components perspectives. Although O-RAN has proposed numerous security specifications in the official WG11 [4], [5], [11], [12], the occurrence of the attacks mentioned above is still possible without the implementation of these security specifications. For instance, deployers can download pre-developed xApps from the Internet for deployment in their environments. Although O-RAN WG11 specifies the need for security testing and analysis before deployment [5], accurately identifying malicious xApps presents a significant challenge. Even on the relatively mature Android platform, where developers and Google conduct security testing and analysis, there continues to be an annual proliferation of malicious apps. This vulnerability increases the risk of uploading problematic xApps, ranging from poorly optimized to malicious or infected, introducing real-time threats, including resource consumption, interruptions, misjudgments, and potential undetected malicious attacks [8], [13].

However, after the successful deployment of xApps, three security concerns arose: openness, authorization, and transmission encryption. Regarding openness, if developers directly deploy xApps within the current O-RAN architecture, malicious attackers can access information about the K8s pods and services of the Near-RT RIC, allowing them to access running services directly. Regarding authorization, the current O-RAN architecture lacks access control for xApps. A malicious attacker can use xApps to access the E2 Manager API and use the exposed service to maliciously shut down all E2 nodes (such as O-CU and O-DU) by disconnecting E2AP. Regarding transport encryption, although O-RAN WG11 has the specification that IPsec should be adopted in the network layer of OSI layer 7 to protect E2 traffic, the official H-Release of O-RAN is still not implemented. Currently, transmission still relies on conventional IP, SCTP, and E2AP protocols. As a result, potential threats and vulnerabilities continue to exist. Furthermore, many APIs on the current Near-RT RIC are transmitted via HTTP, lacking comprehensive permission management and transmission encryption protection. This indicates that attackers could potentially access any service API provided through HTTP on the Near-RT RIC via xApps, posing a particular threat level. Despite the use of HTTP for API communication among Network Functions (NFs) in the 5G core network, the inherently closed nature of 5G and the implementation of identity verification and authorization mechanisms among NFs make it challenging for attackers to exploit vulnerabilities in HTTP. Therefore, the openness of O-RAN further highlights the prominence of such threats [11].

In this paper, we established an O-RAN H-Release environment and designed three types of attacks based on the identified vulnerabilities. The absence of proper xApp authorization can lead to disconnection between E2 nodes and Near-RT RIC. In addition, issues related to encryption in

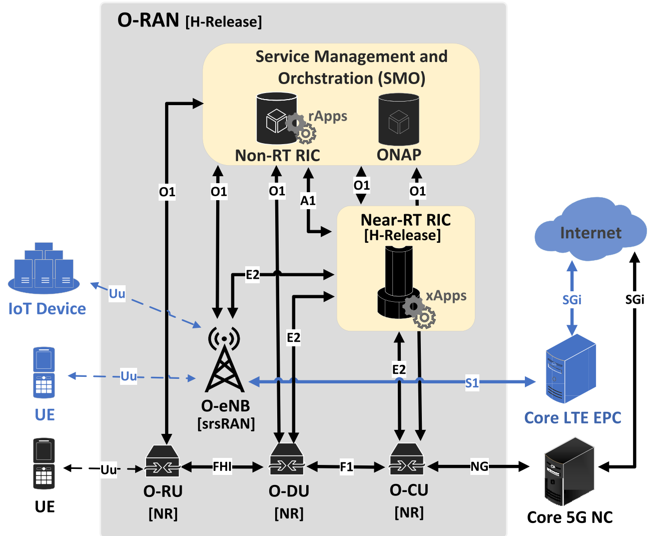

FIGURE 1. SDR-enabled O-RAN Architecture.

the E2 interface transmission and the lack of signal integrity verification affect the regular operation of xApps and the Near-RT RIC, leading to potential Denial of Service (DoS) attacks. This paper can be a foundational cornerstone for other scholars and the O-RAN community's research on xApp access control.

II. BACKGROUND AND RELATED WORK

O-RAN is essential for rapidly deploying and managing 5G networks, ensuring fast and stable network experience, and enabling industry transformation [14]. However, there are security challenges associated with the openness of O-RAN. In the following, we will use Fig. 1 to illustrate the security of the transmission interface and the threat to the components.

A. THREATS TO O-RAN TRANSPORT INTERFACE

The security of O-RAN open interfaces is a critical challenge. Weak authentication mechanisms can be exploited by malicious attackers, resulting in unauthorized access and manipulation of critical network policies and configurations.

- A1 Interface: Due to a flaw in the bi-directional authentication between the Non-RT RIC and the Near-RT RIC, hostile Near-RT RICs can connect through the A1 interface. Consequently, internal attackers can perform man-in-the-middle attacks and jeopardize the policy integrity of the Non-RT RIC. Unauthorized policy changes and access can severely impact RAN performance and functionality [4], [10].
- O1 Interface: The O1 interface allows the SMO and the Near-RT RIC to access resources and services. To ensure security, the SMO must be authenticated before accessing the counterpart's resources. Unfortunately, due to the lack of identity verification and logging, the SMO cannot confirm the identity of both parties. As a

result, data transmission and policies for the SMO and the Near-RT RIC are directly compromised [9].

- FHI Interface: The FHI interface connects the physically exposed O-RU and O-DU. However, malicious attackers can use this to launch DoS attacks, man-in-the-middle attacks, and message tampering via the U-plane, S-plane, and C-plane. These attacks can disrupt the O-RU service and even compromise the O-DU system, significantly impacting the entire O-RAN network [4], [6].

B. SECURITY RISKS ASSOCIATED WITH O-RAN COMPONENTS

The modular design and multi-vendor environment of the O-RAN architecture introduce security risks. While the modular design provides flexibility and scalability, it also raises security concerns. Components from different vendors may have compatibility issues and security vulnerabilities, making the system susceptible to attacks such as intrusion, identity fraud, and information theft [7].

- O-RU: Malicious attackers use technologies such as Software-Defined Radio (SDR) and Universal Software Radio Peripheral (USRP) to launch malicious base station attacks [7], [15]. This attack method takes advantage of the comprehensive signal coverage to force nearby User Equipment (UE) devices to connect to the malicious base station [16]. Malicious attackers can obtain the UE's Subscriber Privacy Identifier and 5G Global Temporary Identifier, leading to disconnection of the UE from legitimate base stations causing service disruptions.
- Non-RT RIC: Attackers can infiltrate the non-RT RIC and gain unauthorized access via the SMO, posing various threats. First, attackers can track the location and behavior of UEs, resulting in a breach of user privacy. Second, attackers can modify the information within the Non-RT RIC, causing data corruption or manipulation and disrupting the regular operation of the system. In addition, attackers can use these privileges for other malicious activities, such as stealing sensitive data, launching DoS attacks, or infiltrating the system, posing serious security risks to the entire O-RAN network [9].
- Near-RT RIC: Near-RT RIC's open platform allows third-party xApp deployment but also introduces security risks. Malicious attackers can use this vulnerability to deploy malicious xApps, compromising sensitive user data [4]. Users are exposed to various risks, including data theft, privacy breaches, financial losses, disrupted operations, service disruptions, a compromised user experience, and system-wide damage or intrusion [8].
- xApps: Vulnerabilities from untrusted or unmaintained sources may be present in xApps, resulting in serious consequences [8], [13]. If attackers discover exploitable xApps, they can disrupt existing network services, infect other xApps, or compromise the entire Near-RT RIC, impacting the O-DU and O-CU. Malicious xApps can consume network resources, causing performance degradation through methods like Fork bombs. Furthermore, attackers may launch adversarial attacks against AI/ML models within xApps, further disrupting the operation of the entire RAN [17], [18]. Finally, these malicious xApps may gain unauthorized access to the Near-RT RIC APIs or launch disruptive attacks such as DoS attack. However, the current O-RAN specification only mentions what threats may exist but does not provide a detailed description of these threats and the process of threat occurrence. Moreover, unknown threats may still exist [4], [5], [12].

III. THREAT COMPONENTS AND ATTACK ANALYSIS

The introduction of xApp provides O-RAN with a more flexible and scalable architecture, allowing deployers to download various xApps from the Internet for deployment in their environments to enrich further and customize wireless network functionalities. Although the O-RAN WG11 specifications mention the need for security analysis before deployment, dealing with a relatively new application platform like xApp poses a significant challenge. This is evident as even on the relatively mature Android platform, despite security scans conducted by developers and Google, numerous malicious apps continue to circulate on the platform. Therefore, we assume that xApp is a potential attack vector. xApp can be compromised through the supply chain or hijacking the inbound process. Even a normal xApp can be a threat if it sends wrong or abnormal signaling. After deploying xApp to Near-RT RIC, we assume proper isolation between virtual machines (VMs) and containers is maintained. Under this assumption, attackers could not launch attacks against other xApps from a malicious xApp through the hypervisor, host operating system, or hardware resources. At the same time, we do not consider the deployment status of O-RAN in private or public clouds. Our focus is on the issues between Near-RT RIC and xApp, and it is not directly related to the deployment location.

During our implementation and development process, we found threats from O-RAN A-Release to the latest H-Release that O-RAN officials do not yet know. We try to map these threats and attacks into the threat model of O-RAN WG11 [4], as shown in Table 1. We first describe the privilege management attacks caused by unreasonable access control Settings in xApps. Based on this threat, we designed two other attacks to exploit the E2 interface of malicious xApps.

The privilege management and E2 interface transport threat models are described below:

- *Threat Description:* Due to the current changes in the development paradigm, attackers can exploit vulnerabilities by uploading xApps with weaknesses or threats, including malicious xApps, to the Internet disguised as legitimate xApps for deployment by unsuspecting users. However, due to the lack of pre-validation mechanisms and robust access control management,

TABLE 1. Analysis table of attack mapping for O-RAN WG11 threat models and related research. The symbols in the table are represented as follows: Resolved "+", mentioned "○", unmentioned "*" and unsolved "x."

Related Research/Threat Type	Deploying Malicious xApp	Privilege Management Threats	E2 Subscription Issues	DoS Attack
[4] T-NEAR-RT-01	*	*	○	*
[4] T-NEAR-RT-02	○	○	*	*
[4] T-NEAR-RT-03	*	○	*	*
[4] T-NEAR-RT-04	*	○	*	*
[4] T-xApp-01	○	*	*	*
[4] T-xApp-02	*	*	*	○
[4] T-xApp-03	○	*	*	*
Polese et al. [8]	○	○	x	x
Liyanage et al. [10]	○	○	x	x
Atalay et al. [13]	○	○	x	x
Groen et al. [18]	○	+	x	x

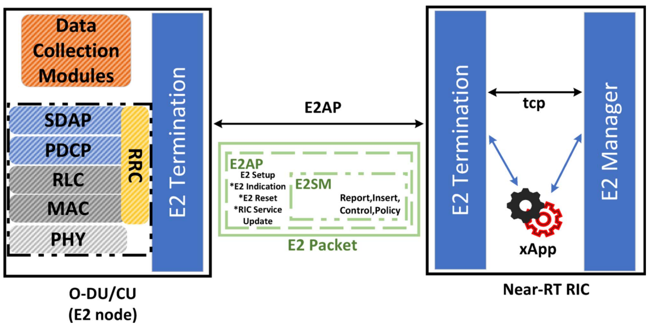

FIGURE 2. E2 Protocol.

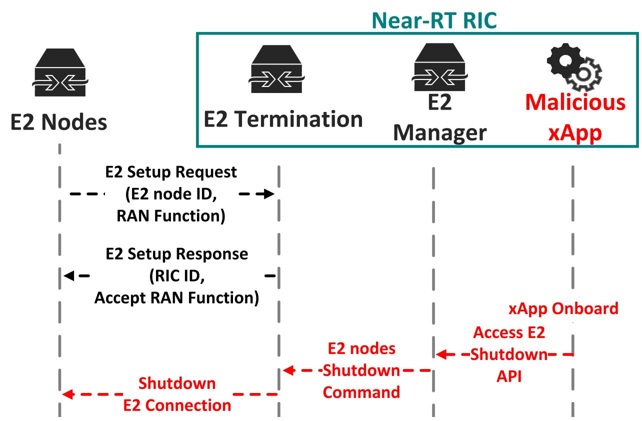

FIGURE 3. Access E2 Manager API.

deploying these xApps in one's environment may lead to unauthorized access, privacy breaches, and service disruptions. Additionally, the absence of integrity authentication mechanisms in E2 transmission and the non-implementation of IPsec provides malicious attackers with opportunities to send malicious signals and packets, leading to the theft of E2 node information or launching DoS attacks.

- *Threat Agent:* All.
- *Identifies Vulnerability:* No deployment validation, Improper Privilege Management, Insufficient Verification of Data Authenticity.
- *Threat Asset:* Malicious xApps illegally access Near-RT RIC services, disrupting O-CU, O-DU, and O-RU operations, as well as E2 nodes and other xApps.
- *Affected Components:* Near-RT RIC, O-CU, O-DU, O-RU.

A. PRIVILEGE MANAGEMENT THREATS FOR XAPP

As shown in Fig. 2, xApp connects with the E2 Termination and utilizes the E2 Interface to collect data and provide specific UE services through the E2 node. The E2 Manager, depicted in Fig. 2, manages the E2 Interface components. Through the E2 Manager, xApp can access the relevant functionalities and resources of the E2 Interface. It can control, configure, and monitor the E2 nodes using the APIs provided by the E2 Manager, enabling more flexible and autonomous network management and optimization.

However, it is unfortunate that the current APIs provided by the E2 Manager still use the HTTP protocol instead of HTTPS, making the information transmitted between them insecure. We discovered that the current xApp can access all APIs on the E2 Manager that use the HTTP protocol. This allows malicious attackers to illegally access these APIs to exploit services provided by other containers and even disrupt the operation of other components, as shown in Fig. 3. Suppose an abnormal xApp is deployed on the Near-RT RIC without access restrictions on individual APIs. In that case, the attacker can leverage the xApp to access the API on the E2 Manager within the Near-RT RIC. This access enables them to send signaling to the E2 Termination, thereby interrupting the connections of all E2 nodes with the Near-RT RIC. The implementation process of the attack will be detailed in Section IV-B.

B. THREATS TO RIC SUBSCRIPTION AND SIGNALING PROCESSES

As the intelligent controller within O-RAN, Near-RT RIC is responsible for network management, optimization, and decision-making functions. It actively subscribes to E2 nodes to receive updates on specific resources, event notifications, and changes in network status. It takes targeted actions based on this information, enabling more flexible and intelligent network management. Unfortunately, there are still numerous hidden threats during the E2 subscription process, which can affect the regular operation of the RAN. In the following, we will explain the two problems we found, the reason for the attack, the process of the attack, and the impact of the components. The implementation process of the attacks will be detailed, respectively, in Sections IV-C and IV-D. The threat model of the E2 interface transport threat is as follows.

1) E2 SUBSCRIPTION ISSUES

If the RIC Message Router(RMR) on Near-RT RIC encounters the same Message type intended for different destinations, the original target will not receive the expected message. Attackers can exploit this mechanism by deploying malicious xApps and continuously sending E2 subscription requests to E2 nodes for repeated subscriptions. As a result, the subscribed xApp will not initially accurately receive the messages sent by the E2 node, leading to a delay in obtaining the real-time status of the E2 node.

The attack process is depicted in Fig. 4 (B). In the RIC subscription messages, xApps establish RMR tables with the E2 Termination through the Routing Manager for proper routing of E2 messages. However, if a malicious xApp repeatedly sends subscription messages, resulting in the creation of multiple RMR tables, the RMR will only route messages based on the rules of the last created table. As a result, the legitimate xApp will fail to receive messages from the E2 node, as the messages will be routed to the malicious xApp instead.

2) NEAR-RT RIC E2 TERMINATION DOS ATTACK

Attackers can exploit abnormal signaling flows to send malicious signals, resulting in the collapse of E2 Termination and causing a DoS attack that disrupts the service. Currently, the E2 Termination in Near-RT RIC lacks integrity checks for signaling. Furthermore, if E2 connections are established differently from the standard procedure in the specification, E2 Termination can collapse, thereby paralyzing E2 Interface.

Fig. 4 (C) demonstrates the E2 DoS attack we implemented to exploit such vulnerabilities. In the normal signaling flow, the E2 node initiates the establishment of an E2 connection by sending an E2 Setup request, and the E2 Termination responds with an E2 Setup response to complete the connection establishment. However, if the connection establishment process deviates from the normal flow, it results in the collapse of E2 Termination.

Due to the lack of restrictions on the messages that xApps can send in the current Near-RT RIC, attackers can exploit this vulnerability by deploying malicious xApps, as shown in Fig. 4 (C) and sending a malicious response to a RIC subscription request to the E2 Termination. Upon receiving such a request, the E2 Termination processes the signaling without performing integrity checks, resulting in its collapse. This allows the attackers to achieve a DoS attack on the E2 Interface service through malicious traffic.

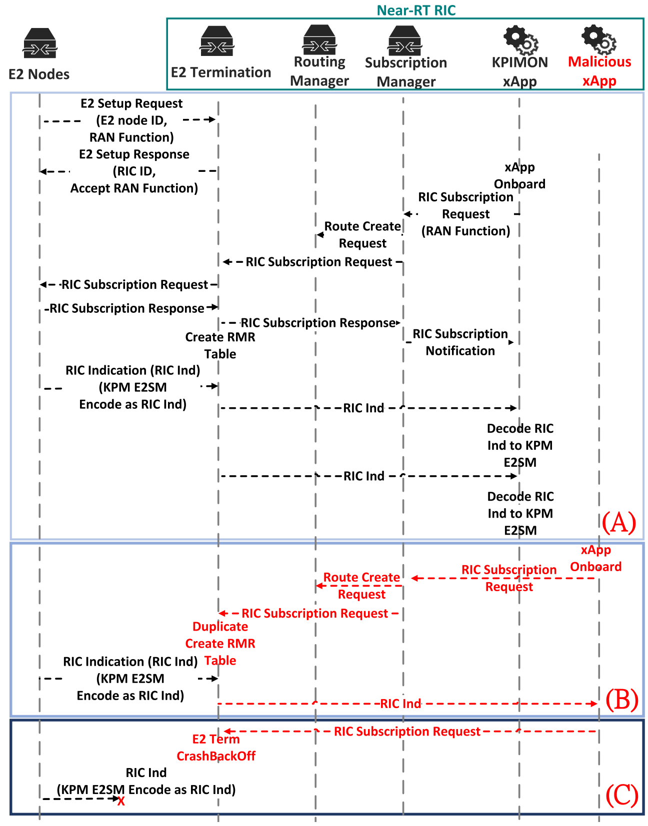

FIGURE 4. Duplicate RMR Table Flow Attack(A to B) and DoS Data Flow Attack (A to C).

TABLE 2. System specifications and software versions.

Hardware & Software/Description	Description
Processor (CPU)	Intel i7-12700 CPU with 12 cores
Graphics Processor (GPU)	NVIDIA RTX 3060
Memory (RAM)	64GB
Storage Capacity	1.5TB SSD
Operating System	Ubuntu 20.04
O-RAN components	H-Release
4G core network	srsRAN
5G core network	OpenAirInterface (OAI)
RAN	Ettus USRP B210 SDR

IV. EXPERIMENT RESULT

A. RESEARCH QUESTION

We have designed the following research questions to evaluate the effectiveness of exploiting these threats in the O-RAN environment.

- RQ1: Does insufficient privilege management in O-RAN generate exploitable threats for attackers?
- RQ2: Does the lack of signal integrity protection and the signaling confirmation process allow attackers to carry out exploits?

All experimental environments in this paper, including the hardware specifications and software versions, have been compiled in Table 2.

TABLE 3. Attack impact and recovery time assessment.

Threat Type	Service Recovery Time(s)	Services to be Restarted	Scope of Impact
Privilege Management Threats	5.09	E2node	E2 node, O-RU, UE
E2 Subscription Issue	48.058	E2node	E2 node, Near-RT RIC, O-RU, UE
DoS Attack	177.075	E2 Termination	E2 node, O-RU, UE

B. PRIVILEGE MANAGEMENT THREATS

To address RQ1 and demonstrate that attackers can exploit vulnerabilities in privilege management to launch attacks affecting RAN operations, we designed and implemented a specific attack. After IP scanning of Near-RT RIC internal services using Nmap in the deployment of xApp, we can obtain the IP of the E2 Manager located in the Near-RT RIC and access the E2 manager. We can then test the API provided by the open-source E2 Manager in O-RAN SC, one by one, to access to the E2-Manager service API. Following our testing, those that contain these APIs disconnect the E2 node from the API. Suppose such an API does not restrict access. In that case, xApp will be able to launch attacks such as Fig. 3, disconnecting E2 connections in all E2 nodes connected to Near-RT RIC, making it impossible for other xApps to collect data returned from the E2 node.

Given the threats above, we recommend adopting an authentication mechanism such as API Key or OAuth 2.0 to ensure the system's security. This ensures that only authorized users can access the API, mitigating potential risks associated with unauthorized access. We can effectively monitor and track each API client by implementing API Keys, ensuring that only authorized applications or users can utilize the relevant API functionalities. OAuth 2.0 authorization mechanisms can also be employed, issuing Access Tokens to legitimately authorized xApps with limited access permissions, allowing them to invoke APIs.

C. E2 SUBSCRIPTION ISSUES

To address RQ2 and demonstrate that attackers can exploit the lack of E2 signaling confirmation processes to impact RAN operations, we designed and implemented a specific attack. During E2 message transmission in the Near-RT RIC, the RMR library developed by the O-RAN SC routes messages to their destinations through its tables. When xApps send E2 setup requests, they also use RMR to route messages to the components within the Near-RT RIC and to complete the subscription of the E2 node. At this point, RMR establishes connections by creating new RMR table rules for messages between E2 nodes and xApps. Our experiments found that when deployed xApps send identical subscription requests to E2 nodes, the components in the Near-RT RIC create new RMR tables. Consequently, if the messages routed by these tables are the same as those processed by previously deployed xApps, the messages are routed to the later-deployed xApps, as shown in Fig. 4 (B). This problem occurs because the RMR implementation only follows the rules of the most recently created table. If multiple xApps need to route the same message to different destinations, only the most recently created RMR table rules are executed, causing the original xApps to stop receiving messages sent by E2 nodes.

Given the above threat, we recommend matching each package of E2 subscription issued by xApp with the respective UUID and RMR Table of xApp. The UUID value should be added when creating an RMR Table rule in order to differentiate it from other xApp rules. In addition, this can stop malicious xApp falsification signals from interfering with the RAN's functionality.

D. NEAR-RT RIC E2 TERMINATION DOS ATTACK

To address RQ2 and demonstrate that attackers can exploit the lack of integrity protection and signaling confirmation in E2 signaling to impact RAN operations, we designed and implemented a specific attack. In the E2AP process Fig. 4 (A), E2 nodes initiate Setup requests to the Near-RT RIC, establishing the E2 connection. xApps send Subscription Requests to E2 nodes, routed internally by the Near-RT RIC to E2 termination. RIC Subscription Response with RAN function information is returned to xApps, completing the subscription.

Our research found that the Near-RT RIC crashes if the E2 termination does not follow the standard E2 signaling process. This can result in a DoS attack. The red part in Fig. 4 (C) represents the attack performed with xApp sending continuous RIC subscription responses to the E2 termination, resulting in an E2 service DoS attack. The reason for the attack was that when an E2 node sends an E2 setup request to the E2 termination, the system internally creates a data array for the sending node. It causes unauthorized memory access and eventually crashes the E2 termination if the signals are not sent in the proper order by the E2 node.

To avoid the threats above, we recommend verifying the compliance of the E2 signaling confirmation process and providing integrity protection to ensure the compliance of E2 signaling content. As a result, evaluating and analyzing the processes and values of all E2 signaling is required, delivering timely alerts as needed.

E. PERFORMANCE EVALUATION

We found that these attacks affect the regular operation of the E2 Node and result in data leakage from UEs and service interruptions. As shown in Table 3, we measured the time it takes for the service to restart after each attack, conducting 50 repetitions and ultimately obtaining the average. Among these attacks, the recovery time for the DoS Attack is the longest. This is because, according to the O-RAN official specifications, E2 Termination cannot be manually restarted; instead, it relies on the Health Check in K8s to confirm whether the Pod is operating normally. When the livenessProbe detects that the E2 Termination Pod is not functioning correctly, K8s terminates and rebuilds the E2 Termination Pod to restore regular service operation. Therefore, such attacks have a significant impact on the overall RAN.

V. CONCLUSION

In this paper, we initially discuss the existing attack threats from the perspective of O-RAN components and interfaces. We then present the threats we discovered during our implementation process, specifically regarding xApp access control and previously unidentified vulnerabilities in the E2 interface. These threats disrupt the regular operation of other xApps. They can result in E2 interface interruptions between O-DU, O-CU, and Near-RT RIC, significantly impacting the proper functioning of the RAN. We implemented three attacks based on these identified vulnerabilities, provided detailed explanations of their occurrence, and analyzed their impact. Implementing the attacks helps us identify potential vulnerabilities, improve O-RAN network security, and accelerate everyone to follow and implement O-RAN official security specifications. We have also released these vulnerabilities as CVEs (CVE-2023-42358 and CVE-2023-41628).

REFERENCES

[1] W. Azariah, F. A. Bimo, C.-W. Lin, R.-G. Cheng, R. Jana, and N. Nikaein, "A survey on open radio access networks: Challenges, research directions, and open source approaches," 2022, *arXiv:2208.09125*.

[2] (O-RAN ALLIANCE e.V., Alfter, Germany). *O-RAN Architecture Description 10.0*. Oct. 2023. [Online]. Available: https://orandownloadsweb.azurewebsites.net/specifications

[3] S. D'Oro, L. Bonati, M. Polese, and T. Melodia, "OrchestRAN: Network automation through orchestrated intelligence in the open RAN," in *Proc. IEEE Conf. Comput. Commun.*, 2022, pp. 270–279, doi: 10.1109/INFOCOM48880.2022.9796744.

[4] (O-RAN ALLIANCE e.V., Alfter, Germany). *O-RAN Security Threat Modeling and Remediation Analysis 6.0*. Jun. 2023. [Online]. Available: https://orandownloadsweb.azurewebsites.net/specifications

[5] (O-RAN ALLIANCE e.V., Alfter, Germany). *O-RAN Study on Security for Application Lifecycle Management 2.0*. Jun. 2023. [Online]. Available: https://orandownloadsweb.azurewebsites.net/specifications

[6] S.-H. Liao, C.-W. Lin, F. A. Bimo, and R.-G. Cheng, "Development of C-plane DoS attacker for O-RAN FHI," in *Proc. 28th Annu. Int. Conf. Mobile Comput. Netw.*, 2022, pp. 850–852, doi: 10.1145/3495243.3558259.

[7] D. Mimran et al., "Security of open radio access networks," *Comput. Secur.*, vol. 122, Nov. 2022, Art. no. 102890, doi: 10.1016/j.cose.2022.102890.

[8] M. Polese, L. Bonati, S. D'Oro, S. Basagni, and T. Melodia, "Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1376–1411, 2nd Quart., Jan. 2023, doi: 10.1109/COMST.2023.3239220.

[9] C. Shen et al., "Security threat analysis and treatment strategy for ORAN," in *Proc. 24th Int. Conf. Adv. Commun. Technol.*, 2022, pp. 417–422, doi: 10.23919/ICACT53585.2022.9728862.

[10] M. Liyanage, A. Braeken, S. Shahabuddin, and P. Ranaweera, "Open RAN security: Challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 214, May 2023, Art. no. 103621, doi: 10.1016/j.jnca.2023.103621.

[11] (O-RAN ALLIANCE e.V., Alfter, Germany). *O-RAN Security Requirements and Controls Specification 7.0*. Oct. 2023. [Online]. Available: https://orandownloadsweb.azurewebsites.net/specifications

[12] (O-RAN ALLIANCE e.V., Alfter, Germany). *O-RAN Study on Security for Near Real Time RIC and xApps 4.0*. Oct. 2023. [Online]. Available: https://orandownloadsweb.azurewebsites.net/specifications

[13] T. O. Atalay, S. Maitra, D. Stojadinovic, A. Stavrou, and H. Wang, "Securing 5G OpenRAN with a scalable authorization framework for xApps," in *Proc. IEEE Conf. Comput. Commun.*, New York, NY, USA, 2023, pp. 1–10, doi: 10.1109/INFOCOM53939.2023.10228961.

[14] A. S. Abdalla, P. S. Upadhyaya, V. K. Shah, and V. Marojevic, "Toward next generation open radio access networks: What O-RAN can and cannot do!," *IEEE Netw.*, vol. 36, no. 6, pp. 206–213, Nov./Dec. 2022, doi: 10.1109/MNET.108.2100659.

[15] S.-M. Cheng, B.-K. Hong, and C.-F. Hung, "Attack detection and mitigation in MEC-enabled 5G networks for AIoT," *IEEE Internet Things Mag.*, vol. 5, no. 3, pp. 76–81, Sep. 2022, doi: 10.1109/IOTM.001.2100144.

[16] J.-H. Huang, S.-M. Cheng, R. Kaliski, and C.-F. Hung, "Developing xApps for rogue base station detection in SDR-enabled O-RAN," in *Proc. IEEE Conf. Comput. Commun. Workshops*, Hoboken, NJ, USA, 2023, doi: 10.1109/INFOCOMWKSHPS57453.2023.10225868.

[17] E. Habler et al., "Adversarial machine learning threat analysis and remediation in open radio access network (O-RAN)," 2023, *arXiv:2201.06093*.

[18] J. Groen et al., "Implementing and evaluating security in O-RAN: Interfaces, intelligence, and platforms," 2023, *arXiv:2304.11125*.

CHENG-FENG HUNG (Graduate Student Member, IEEE) received the M.E. degree in information technology and applications from the College of Science and Engineering, National Quemoy University, Kinmen, Taiwan, in 2019. He is currently pursuing the Ph.D. degree with the Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taipei. He visited the Warsaw University of Technology in 2022. His research interests are O-RAN and MEC security in mobile networks.

YOU-RUN CHEN received the B.S. and M.S. degrees in computer science and information engineering from the National Taiwan University of Science and Technology, Taiwan, in 2021 and 2023, respectively. His research interest is O-RAN security in mobile networks.

CHI-HENG TSENG received the B.S. degree in computer science and information engineering from the National Yunlin University of Science and Technology, Taiwan, in 2022. He is currently pursuing the M.S. degree in computer science and information engineering with the National Taiwan University of Science and Technology, Taiwan. His research interest is O-RAN security in mobile networks.

SHIN-MING CHENG (Member, IEEE) received the B.S. and Ph.D. degrees in computer science and information engineering from the National Taiwan University, Taipei, Taiwan, in 2000 and 2007, respectively. Since 2012, he has been on the faculty of the Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taipei, where he is currently a Professor. Since 2022, he has been serving as the Deputy Director-General in Administration for Cyber Security, Ministry of Digital Affairs. His current interests are mobile network security and IoT system security. Recently, he investigates malware analysis and AI robustness. He has received IEEE Trustcom 2020 Best Paper Awards.