

Router Penetration Testing Based on CEM Vulnerability Assessment Criteria

Tai-Ying Chiu*, Bor-Yao Tseng*, Bagus Tri ATMAJA*,

Jiann-Liang Chen*, Jian-Chang Hsu**

* Department of Electrical Engineering, NTUST (National Taiwan University of Science and Technology)

** ITRI (Industrial Technology Research Institute), Taiwan

M11107508@gapps.ntust.edu.tw, M11107501@mail.ntust.edu.tw, D11207806@mail.ntust.edu.tw,
lchen@mail.ntust.edu.tw, hcc@taics.org.tw

Abstract— As a crucial component of modern network infrastructure, routers' performance can be severely impacted if they fall victim to hacker attacks, affecting all network devices connected to them. Router manufacturers should ensure sufficient cybersecurity measures for their products, such as undergoing information security certification, to prevent customers from encountering unforeseen vulnerabilities when using their routers. In reality, most routers on the market have not been certified for information security, primarily because the certification process is time-consuming and costly. One of the main reasons for this is that security testing during the certification process requires different security validation methods based on the product's functionalities. This study adheres to the Common Methodology for Information Technology Security Evaluation (CEM) testing methodology under the international information security certification standard "Common Criteria." It conducts penetration testing on common router functionalities. It integrates the necessary testing tools, processes, and results to provide a reference for future researchers, reducing testing complexity and enhancing product security assurance.

Keywords— Common Criteria, Router, Common Methodology for Information Technology Security Evaluation(CEM), Penetration Testing, Vulnerability Assessment

I. INTRODUCTION

As information technology advances, concerns about information security grow. Routers, central to data transmission in modern networks, are vital. Securing routers is crucial because malicious actors can exploit their vulnerabilities, causing data leaks, network disruptions, and potential attacks. Hence, router security assessment is a vital product indicator.

Since August 1999, an ISO standard called Common Criteria (ISO/IEC 15408) has existed for IT product security certification. However, CC certification is expensive and complex, demanding substantial resources. Consequently, most routers on the market often lack CC or other security certifications.

The complexity and cost of CC certification result from the need to account for diverse product functionalities and designs. This lack of standardization prolongs testing. This paper adheres to CC standards and references CEM documentation.

It employs CEM's testing methods and assessment report requirements to document router product security tests. The goal is to compile testing tools and procedures as a reference for future researchers to streamline router testing and reduce duration.

II. RELATED WORK

This chapter introduces global infosec standards, relevant security concepts, and research literature on router product security testing methods.

A. Common Criteria

CC (ISO/IEC 15408) is a global standard for evaluating and certifying information security products and systems. It offers a standardized framework for assessing security solutions, ensuring they meet specific requirements. CC has evaluation levels from EAL1 to EAL7. It comprises three main parts: Introduction and General Model [1], Security Functional Requirements [2], and Security Assurance Requirements [3].

B. Common Methodology for Information Technology Security Evaluation

The Common Methodology for Information Technology Security Evaluation (CEM) [4] ensures consistent and effective information security assessments, particularly in the Common Criteria (CC) certification framework. CEM offers specific guidance for assessors, including assessment procedures, testing methods, and report writing to align with CC requirements. It promotes standardization and interoperability in global information security assessments. Our research will follow the AVA_VAN chapter requirements in CEM, focusing on procedures and criteria for analyzing vulnerabilities and weaknesses to assess the target system or product's security.

C. Penetration Testing

Security assessments often employ penetration testing, a method simulated by attackers to uncover vulnerabilities in computer systems, applications, or networks [5]-[10]. Baluni et al. [8] note its time-consuming complexity, involving tailored security validation methods. Türpe et al. [11] stress the vital role of the testing environment to prevent harm, data

leaks, disruptions, and legal issues. Zakaria et al. [12] highlight the need for standardized report formats, as reports may differ across companies.

[5]-[9] introduce practical penetration testing tools like Nmap, Metasploit, and Wireshark, and mention Kali Linux in [10]. Kali Linux, a specialized Debian-based OS, is designed for testing and evaluating infosec tools. It offers a range of network testing, vulnerability scanning, and password cracking tools, empowering security professionals to enhance system security. Kali Linux comes with pre-installed or installable versions of these tools, making it an ideal testing platform for our research.

D. Related Research on Router Vulnerabilities

Karamanos Emmanouil [13] delves into router security, illustrating router-targeted attacks. Niemietz Marcus et al. [14] performed XSS and UI redressing attacks on routers from ten manufacturers, showcasing rapid fingerprinting attacks and suggesting countermeasures. Fuzz testing by F. Li et al. [15] unveiled Ping of Death and Denial of Service flaws in Cisco routers. Jin-bing Hou et al. [16] summarized firmware vulnerabilities in embedded systems, covering multiple router models and offering an overview of vulnerability detection.

III. METHOD

In the documents we tested, based on the previously mentioned CEM, and with Zyxel company's firewall product ATP 100 as our testing target. In the Vulnerability Assessment document standard, the testing phase is divided into 11 steps, and we will conduct the evaluation of the Target of Evaluation (TOE) in accordance with the testing specifications and its assessment report.

During the assessment phase, the testing is divided into 11 sections, including requirements, evaluator findings, rationale, and conclusions.

A. AVA_VAN.1-1

First is the requirement of AVA_VAN.1-1, which demands that the evaluator, when inspecting the TOE, must confirm the consistency of the test configuration with the evaluation configuration specified in the Security Target (ST). Therefore, it is necessary to examine its features and firmware version. At the time of our testing, the device had a firmware version of V5.37(ABPS.0), which is newer than the V5.31 indicated in the User's guide. Furthermore, a comparison between the User's guide and the TOE's backend management revealed feature consistency, and in terms of the physical configuration of the device, it aligns with the specifications provided in the ST. Therefore, the conclusion drawn at this stage is that the test configuration of the Zyxel ATP 100 is consistent with the evaluation configuration in the ST.

B. AVA_VAN.1-2

The requirement at this stage is for the evaluator to verify that the TOE is correctly installed and ensure that it is in a known state. In this assessment, the evaluator follows the steps outlined in the User's guide, as follows:

1. Plug the device into the power cord and ensure that it is receiving power.
2. Turn on the device.
3. Use RJ-45 to connect the wall outlet to the WAN interface of the ATP-100.
4. Use RJ-45 to connect to the computer from the LAN port of the ATP 100.
5. Configure the device from the web user interface (192.168.1.1).
6. Follow the "Initial Setup".
7. Configure the WAN Network address
IP Address: 140.118.xxx.xxx
Subnet Mask: 255.255.255.0
Gateway: 140.118.xxx.xxx
8. Upgrade the firmware to the newest available version by following these steps
Maintenance -> File Manager -> Firmware Management -> Upgrade
9. The device is ready, and it is working properly.

After the installation is completed, a comprehensive inspection of the TOE is carried out to ensure that each function operates correctly, indicating the successful installation and initial configuration.

C. AVA_VAN.1-3

Next is AVA_VAN.1-3, where the requirement is for the evaluator to search in publicly available information to identify potential vulnerabilities in the TOE. In this stage, we utilized various publicly available sources such as Zyxel's official security advisory page and the MITRE Corporation's Common Vulnerabilities and Exposures (CVE) database. Here are some of the CVE vulnerabilities we found related to the Zyxel ATP series: CVE-2020-29299, CVE-2021-35029, CVE-2022-0342, CVE-2022-0734, CVE-2022-0910, CVE-2022-2030, and more. Additionally, we identified some common patterns within these vulnerabilities, such as potential vulnerabilities in the device's web interface leading to Cross-Site Scripting (XSS), risks associated with device functionality during authentication, and potential exploitation via Directory Traversal to access undisclosed confidential data in the TOE. Since the impact and exploitation of each vulnerability require significant expertise, this information is considered essential for evaluating the TOE. In this stage, we present the results of identifying past vulnerabilities in the ATP series as part of completing AVA_VAN.1-3.

D. AVA_VAN.1-4

The requirement of AVA_VAN.1-4 is for the evaluator to document the identified potential vulnerabilities, which are candidates for testing and applicable to the TOE within its operational environment. In our actual examination, we can locate the section titled "Security Problem Definition" in the TOE's Security Target document and analyze potential vulnerabilities that may exist therein. We found vulnerabilities that may exist in the TOE documented in the file, which are considered test candidates, as shown in Table 1. Once the stage is complete, and testing of vulnerability issues can proceed to the next step.

E. AVA_VAN.1-5

In the requirement standard AVA_VAN.1-5, the evaluator must take the potential vulnerabilities identified through research and design penetration tests. Before commencing testing, it is necessary to prepare the tools required during the testing process, such as NMAP, Wireshark, LOIC, and others, as detailed testing items correspond to the tools mentioned in Table 1.

F. AVA_VAN.1-6

Next is AVA_VAN.1-6, where the requirement is for the evaluator to thoroughly document the penetration testing based on the list of potential vulnerabilities, ensuring that the testing can be replicated. Additionally, the documentation should include the prior preparation of testing tools and the anticipated test outcomes. Following the above guidelines, during our evaluation, we conducted tests on the TOE using the predetermined candidates outlined in AVA_VAN.1-4, utilizing the equipment and configurations established in AVA_VAN.1-5. The necessary tools and preparations for the testing candidates are listed in Table 3, and the expected outcomes are detailed in Table 2.

G. AVA_VAN.1-7

The requirement of AVA_VAN.1-7 is for the evaluator to initiate penetration testing, and our testing findings are summarized in Table 1.

TABLE 1. SUMMARY OF PENETRATION TESTING

Test Candidate	Test Candidate	Tests Performed
T.WEAK_CRYPTOGRAPHY	Wireshark	Packets use a reliable protocol, but TOE can't identify QUIC certificates.
T.NETWORK_ACCESS	IP block list, Scapy, Wireshark	List the target IP and use it to log in to Zyxel. Besides, we use Scapy to send a packet and Wireshark to check it.
Buffer overflow attack	NMAP	No buffer overflow vulnerability was found in the test report.
OS command injection	NMAP, Burp Suite	No command injection went through the router.
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Window CMD, ZYXEL Backstage, Google Authenticator	Enable two-factor in UI settings; configure Email and Google authenticator. Verified if the device asking extra code with two-factor enabled. The device sends and verifies a code for admin page access.

T.NETWORK_DISCLOSURE	Window CMD, ZYXEL Backstage	Set up the target IP in the block list, and then test whether the router can ping it and receive packets.
T.WEAK_AUTHENTICATION_ENDPOINTS	Wireshark, VPN setup of Zyxel ATP 100	Using IKE for IPsec VPN setup. Wireshark to inspect the encryption used for the packet.
T.UPDATE_COMPROMISE-upgrade test	HxD	Using HxD, modify the firmware update file, and update the modified file to verify if any issues.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Wireshark	Utilize Wireshark to verify TOE's management interface protocol and reliable certificates.
T.NETWORK_DOS	Hping3, LOIC, NMAP, Botnet Filter	Configure a computer as the target under a router and another with an external IP to launch a DoS attack.
T.DATA_INTEGRITY	Sandbox	Malware downloaded and then check logging and Sandbox service.
T.MALICIOUS_TRAFFIC	LOIC	Using LOIC to simulate DoS.

H. AVA_VAN.1-8

Following AVA_VAN.1-7, the next is AVA_VAN.1-8, where the requirement is for the evaluator to document the actual results of the penetration testing. In our documentation of the actual results, we will compare them with the expected outcomes previously defined in AVA_VAN.1-7, as detailed in Table 2.

TABLE 2. COMPARISON OF EXPECTED AND ACTUAL RESULTS FOR PENETRATION TESTING

Test Candidate	Expected result	Actual Result
T.WEAK_CRYPTOGRAPHY	SSL Inspection: Encrypts, decrypts, and scans reliable protocol packets; blocks unreliable ones.	SSL Inspection doesn't support QUIC, allowing its packets to pass uninspected.
T.NETWORK_ACCESS	It can block connections, packets, and access permissions.	Blocks computers from connecting but allows target login.
Buffer overflow attack	If NMAP finds a weakness then receive a warning of "ProFTPD server TELNET IAC stack overflow."	The NMAP report didn't include Buffer overflow vulnerability.
OS command injection	If the URL command injection exploit succeeds, router config files are visible. If NMAP shellshock testing detects vulnerability, a warning will received.	URL command injection failed, the router redirects to the login page. The NMAP report didn't include command injection vulnerability.

T.UNAUT HORIZED _ADMINI STRATOR _ACCESS	Receive a two-factor authentication message through SMS, E-mail, or Google Authenticator, while logging in.	Successful two-factor with Google Authenticator; TOE sends and validates codes.
T.NETWO RK_DISC LOSURE	Shouldn't receive packet from IP block list, through both Router CLI and PC cmd.	In the router's CLI, ping to the blocked IP works, but the PC's CMD doesn't receive packets from the blocked IP.
T.WEAK AUTHEN TICATIO N_ENDPO INTS	The encryption is by IKE and used for packet transmission during the intermediate stages.	The payload is encrypted and authenticated by IKE.
T.UPDAT E_ COMPRO MISE- upgrade test	The TOE detects that the update file is insecure, resulting in a failed update and displaying a warning.	The TOE detects that the update file is insecure, resulting in a failed update and displaying a warning.
T.UNTRU STED_CO MMUNIC ATION_C HANNELS	Each packet of TOE's configuration interface uses a highly reliable protocol and certificate.	TOE employs TLSv1.3, yet the browser distrusts the Zyxel-signed certificate.
T.NETWO RK_DOS	TOE detects DOS attacks, and blocks malicious traffic. Script opens two server connections, and lacks final CRLF. After 10 seconds, the second connection sends an extra header. If the second times out after the first, the header extends timeout, exposing Slowloris DoS vulnerability.	TOE effectively shields protected devices from external IP DoS attacks. The Botnet Filter which can defend zombie devices, didn't show up on the device. Nmap report reveals no DoS vulnerability in open port scan.
T. DATA_IN TEGRITY	Detect malware files and intercept them at the same time.	Malware downloads: No detection by Logging and Sandbox services.
T.MALICI OUS_TRA FFIC	Using a DoS attack to test whether the TOE will crash.	After being attacked, the TOE will crash.

I. AVA_VAN.1-9

Next is AVA_VAN.1-9, where the requirement is for the evaluator to document the actual results of penetration testing, providing an overview of the testing methodology, configurations, depth, and outcomes. After conducting penetration tests tailored for the TOE, we provide detailed descriptions of the testing results, as outlined in Table 3.

TABLE 3. THE DETAILED RESULTS OF PENETRATION TESTING

Test Candidate	Expected result	TSFI	Actual Result
----------------	-----------------	------	---------------

T.WEAK CRYPTOG RAPHY	Wireshark: Check the protocol version of each package.	GUI	SSL Inspection doesn't support QUIC, allowing its packets to pass uninspected.
T.NETWO RK_ACCE SS	IP block list, Scapy, Wireshark	GUI	Blocks computers from connecting but allows target login.
Buffer overflow attack	Run NMAP ftp-vuln-cve2010-4221 testing	CLI	The NMAP report didn't include Buffer overflow vulnerability.
OS command injection	Adding URL command (Burp Suite) Run nmap -sV -p- --script http-shellshock <target>	CLI	URL command injection failed, the router redirects to the login page. The NMAP report didn't include command injection vulnerability.
T.UNAUT HORIZED _ADMINI STRATOR _ACCESS	Window CMD, ZYXEL Backstage, Google Authenticator	CLI/G UI	Successful two-factor with Google Authenticator; TOE sends and validates codes.
T.NETWO RK_DISC LOSURE	Window CMD, ZYXEL Backstage	CLI	In the router's CLI, ping to the blocked IP works, but the PC's CMD doesn't receive packets from the blocked IP.
T.WEAK AUTHEN TICATIO N_ENDPO INTS	Wireshark, VPN setup of Zyxel ATP 100	GUI	The payload is encrypted and authenticated by IKE.
T.UPDAT E_ COMPRO MISE- upgrade test	HxD: Modify firmware upgrade file.	GUI	The TOE detects that the update file is insecure, resulting in a failed update and displaying a warning.
T.UNTRU STED_CO MMUNIC ATION_C HANNELS	Wireshark: Verify TOE's config interface protocol version.	GUI	TOE employs TLSv1.3, yet the browser distrusts the Zyxel-signed certificate.
T.NETWO RK_DOS	Hping3, LOIC: Conduct a DOS attack on the device protected by TOE. NMAP, Botnet Filter	CLI	TOE effectively shields protected devices from external IP DoS attacks. The Botnet Filter which can defend zombie devices, didn't show up on the device. Nmap report reveals no DoS vulnerability

			in open port scan.
T. DATA_INTEGRITY	Sandbox	GUI	Malware downloads: No detection by Logging and Sandbox services.
T.MALICIOUS_TRAFFIC	LOIC	GUI	After being attacked, the TOE will crash.

J. AVA_VAN. 1-10

In AVA_VAN.1-10, the requirement is for the evaluator to examine the results of all penetration tests to ensure that the TOE can withstand attackers with basic attack potential in its operational environment. Here, we have reviewed all the test results and calculated the attack potential for each factor. Tables 4, 5, and 6 display the Attack Potential Calculation (APC) values we have computed for the TOE.

TABLE 4. ASSESSMENT OF APC VALUES FOR EACH TEST (1)

Test Candidate	Buffer overflow attack	OS command injection	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	T.NETWORK_DISCLOSURE
Factor	Value	Value	Value	Value
Elapsed Time	7	4	4	10
Expertise	6	3	3	8
Knowledge of TOE	4	4	3	4
Window of Opportunity	10	4	4	4
Equipment	4	4	9	4
Total	31	19	23	30

TABLE 5. ASSESSMENT OF APC VALUES FOR EACH TEST (2)

Test Candidate	T.NETWORK_DOS	T. DATA_INTEGRITY	T.WEAK_CRYPTOGRAPHY	T.UPDATE_COMPROMISE-upgrade test
Factor	Value	Value	Value	Value
Elapsed Time	1	1	7	10
Expertise	3	0	6	6
Knowledge of TOE	3	0	3	3
Window of Opportunity	4	0	4	10
Equipment	4	0	4	4
Total	15	1	24	33

TABLE 6. ASSESSMENT OF APC VALUES FOR EACH TEST (3)

Test Candidate	T.UNTRUSTED_COMMUNICATION_CHANNELS	T.NETWORK_ACCESS	T.WEAK_AUTHENTICATION_ENDPOINTS	T.MALICIOUS_TRAFFIC
Factor	Value	Value	Value	Value
Elapsed Time	19	7	10	1
Expertise	6	6	6	3
Knowledge of TOE	7	3	7	0
Window of Opportunity	10	10	4	1
Equipment	7	4	7	0
Total	51	30	34	5

K. AVA_VAN. 1-11

Finally, in AVA_VAN.1-11, the requirement is for the evaluator to report all exploitable vulnerabilities and any remaining vulnerabilities, along with detailed explanations of their sources. After a series of tests examining public vulnerabilities and security threats, the last stage involves summarizing the results. Out of the 12 testing items, the TOE failed in the following categories: T.MALICIOUS_TRAFFIC, T.UNTRUSTED_COMMUNICATION_CHANNELS, and T. DATA_INTEGRITY. Detailed information regarding these failures will be provided in Chapter 4, while all other testing candidates pass successfully.

IV. EVALUATION

In the penetration testing conducted on the router, we followed the Vulnerability Assessment standards outlined in the CEM, planning and documenting the testing process and results. Throughout this process, we conducted thorough testing of the TOE. However, we discovered that several testing items did not fully align with the functionalities mentioned in its User's guide. Below are our findings.

Regarding T.UNTRUSTED_COMMUNICATION_CHANNELS, this test aimed to confirm the TOE's ability to use highly reliable protocols and certificates. While the TOE uses the highly reliable TLSv1.3 protocol, browsers did not trust the certificates signed by Zyxel, resulting in a test failure. In T.DATA_INTEGRITY, the test was designed to evaluate the TOE's Sandbox functionality, which isolates unknown files and detects new malware to enhance network security. However, during testing, the TOE failed to detect and block malicious files, leading to a test failure. The handbook mentions that the Sandbox should be able to identify unknown threats, but this was not achieved in this test. Lastly, in T.MALICIOUS_TRAFFIC, we simulated a DoS attack to evaluate the TOE's firewall functionality for blocking malicious traffic and DoS attacks. The test results showed that the TOE encountered issues during a DoS attack and did not provide the expected protection, resulting in a test failure.

V. CONCLUSION

In today's technologically advanced era, there has been a significant increase in general awareness of information security in daily life. Concurrently, to ensure that users can use information and communication products such as routers with greater confidence, various countries have introduced a certification framework for the security of IT products known as Common Criteria. This article is based on the certification framework mentioned above, utilizing the Common Methodology for Information Technology Security Evaluation. It is a specialized method for evaluating information security and we implement penetration testing for routers within this framework. This includes recording the development of testing tools, procedures, and results as required by AVA_VAN in the CEM. Additionally, certain vulnerabilities and shortcomings in the TOE are identified.

The current information security issues are of utmost significance, and international certification standards are a major focus. This article takes routers as an example and is written based on the testing methodology outlined in the CEM. It aims to provide a reference for future researchers, reduce testing complexity, and enhance product security assurance.

REFERENCES

- [1] "Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model," November 2022.
- [2] "Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components," November 2022.
- [3] "Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components," November 2022.
- [4] "Common Methodology for Information Technology Security Evaluation – Evaluation methodology," November 2022.
- [5] H. M. Z. A. Shebli and B. D. Beheshti, "A study on penetration testing process and tools," 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, pp. 1-7, NY, USA, 2018.
- [6] Robert Shimonski, "Conducting a Penetration Test," in Penetration Testing For Dummies, Wiley, pp.129-145, 2020.
- [7] P. Anand and A. Shankar Singh, "Penetration Testing Security Tools: A Comparison," 2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART), pp. 182-184, MORADABAD, India, 2021.
- [8] S. Baluni, S. Dutt, P. Dabral, S. Maji, A. Kumar and A. Chaudhary, "Penetration Testing on Virtual Machines," 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp. 1-6, Noida, India, 2022.
- [9] M. Patel and H. R. Patel, "Analytical Study of Penetration Testing for Wireless Infrastructure Security," 2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), pp. 131-134, Chennai, India, 2019.
- [10] D. Sweigert, M. M. Chowdhury and N. Rifat, "Exploit Security Vulnerabilities by Penetration Testing," 2022 IEEE International Conference on Electro Information Technology (eIT), pp. 527-532, Mankato, MN, USA, 2022.
- [11] S. Törpe and J. Eichler, "Testing Production Systems Safely: Common Precautions in Penetration Testing," 2009 Testing: Academic and Industrial Conference - Practice and Research Techniques, pp. 205-209, Windsor, UK, 2009.
- [12] N. Zakaria, P. A. Phin, N. Mohamad, S. A. Ismail, M. N. Kama and O. Yusop, "A Review of Standardization for Penetration Testing Reports

and Documents," 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS), pp. 1-5, Johor Bahru, Malaysia, 2019.

- [13] Karamanos Emmanouil, "Investigation of home router security," 2010.
- [14] Niemietz Marcus and Jörg Schwenk, "Owning your home network: Router security revisited," arXiv preprint arXiv:1506.04112, 2015.
- [15] F. Li, L. Zhang and D. Chen, "Vulnerability mining of Cisco router based on fuzzing," The 2014 2nd International Conference on Systems and Informatics (ICSAI 2014), pp. 649-653, Shanghai, China, 2014.
- [16] Jin-bing Hou, Tong Li and Cheng Chang, "Research for Vulnerability Detection of Embedded System Firmware," Procedia Computer



Tai-Ying Chiu was born in Taiwan, in 1999. She received the B.S. degree, in 2022. She is currently pursuing the M.S. degree in electrical engineering with the National Taiwan University of Science and Technology, Taipei. Her main research interests include artificial intelligence, and the Internet of Things (IoT).



Bor-Yao Tseng was born in Taiwan, in 1999. He received the B.S. degree, in 2022. He is currently pursuing the M.S. degree in electrical engineering with the National Taiwan University of Science and Technology, Taipei. His main research interests include artificial intelligence, and the Internet of Things (IoT).



2019.

Bagus Tri Atmaja, born on December 4th, 1996, is currently a doctoral candidate in Electronic Engineering at the National Taiwan University of Science and Technology (NTUST). He is the third son of his family from East Java, Indonesia. Bagus completed his Master's Degree at NTUST in 2023, following a Bachelor's Degree from the Institut Teknologi Sepuluh Nopember (ITS), Indonesia, in



Jiann-Liang Chen Prof. Chen was born in Taiwan on December 15, 1963. He received the Ph.D. degree in Electrical Engineering from National Taiwan University, Taipei, Taiwan in 1989. Since August 1997, he has been with the Department of Computer Science and Information Engineering of National Dong Hwa University, where he is a professor and Vice Dean of Science and Engineering College. Prof. Chen joins the Department of Electrical Engineering, National Taiwan University of Science and Technology, as a Distinguished professor and Dean now. His current research interests are directed at cellular mobility management, cybersecurity, personal communication systems and Internet of Things (IoT). The second paragraph uses the pronoun of the person (he or she) and not the author's last name. It lists military and work experience, including summer and fellowship jobs. Job titles are capitalized. The current job must have a location; previous positions may be listed without one. Information concerning previous publications may be included. Try not to list more than three books or published articles. The format for listing publishers of a book within the biography is: title of book (city, state: publisher name, year) similar to a reference. Current and previous research interests end the paragraph.