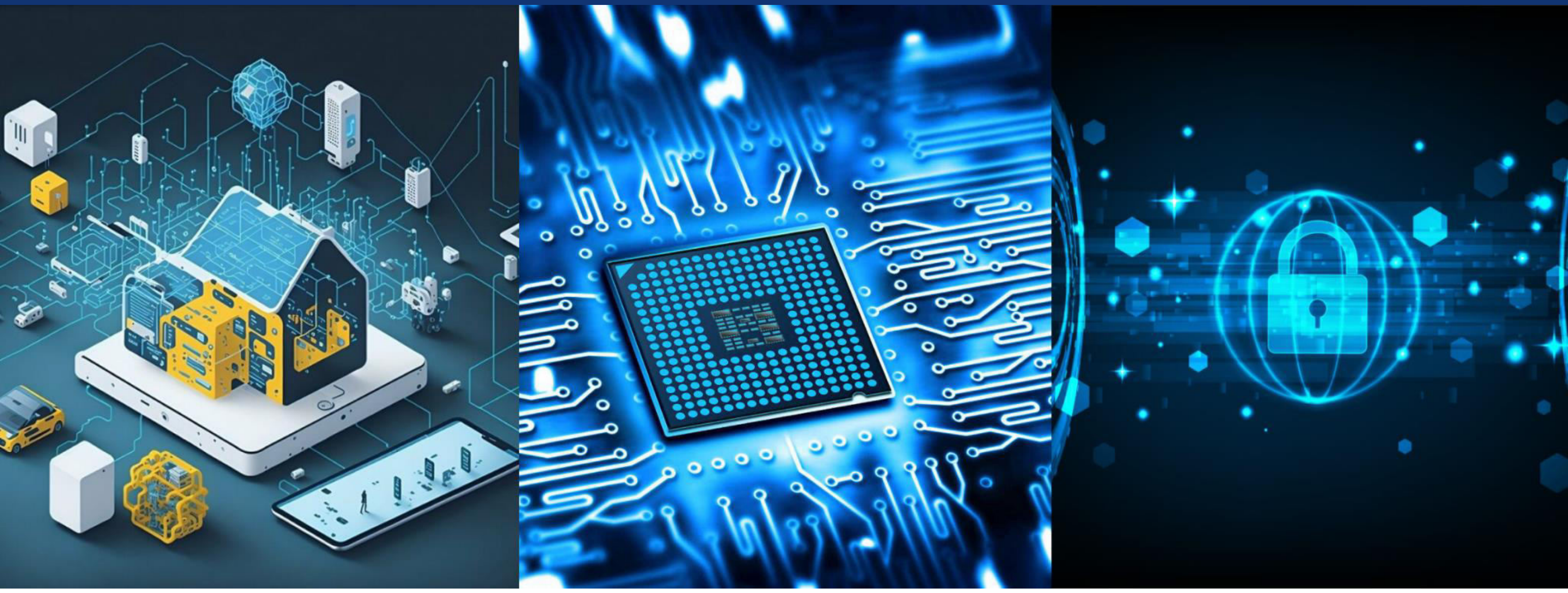
IJIRCCE

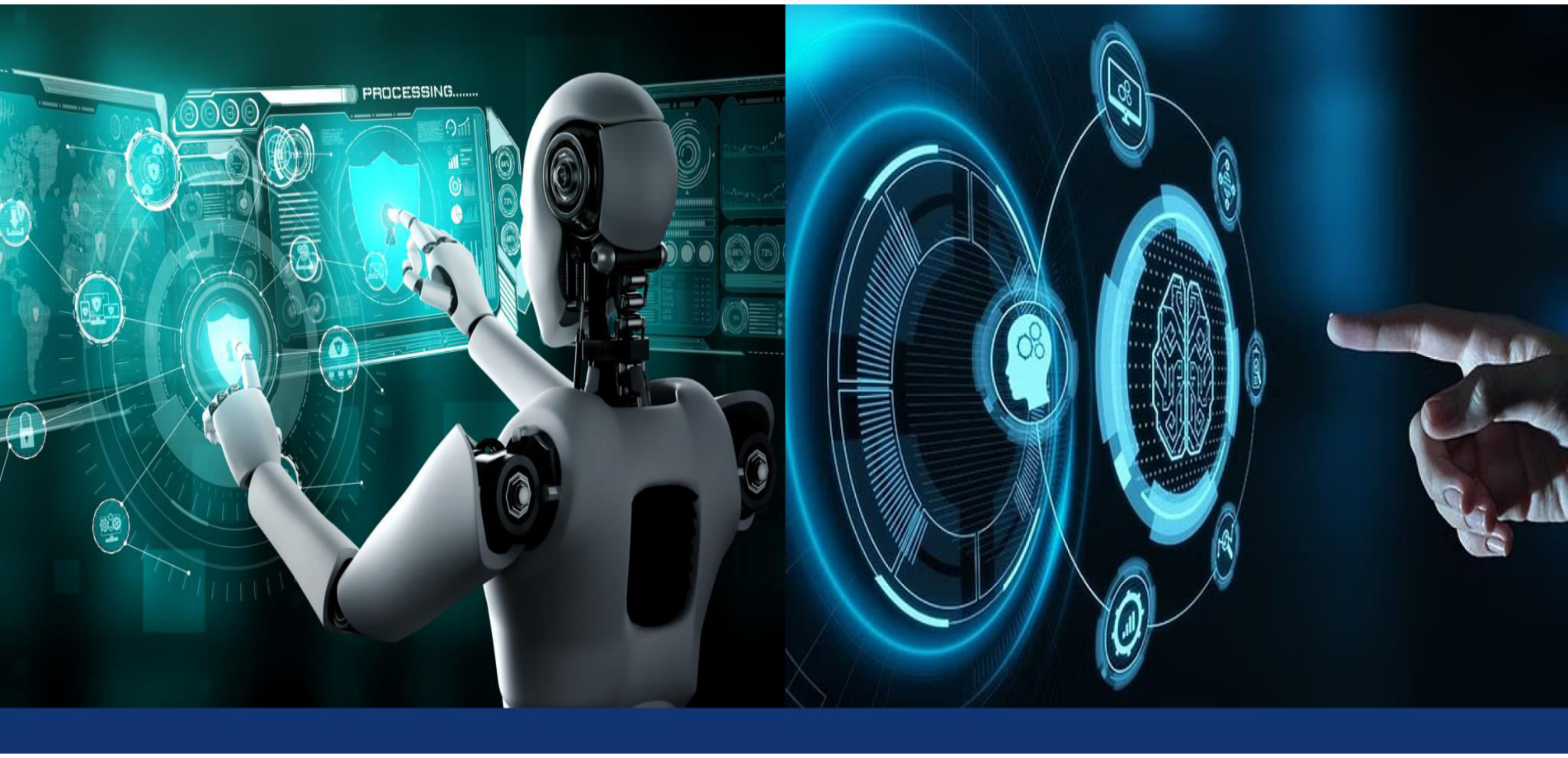
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 5, May 2025

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305055

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

An Attack on One-Tap Authentication Services in Cellular Networks

Ahalya G[1], Prof Dr S Bhargavi[2]

Student, Dept. of Electronics and Communication, SJC Institute of Technology, Chickaballapur, India[1]

Professor, Dept. of Electronics and Communication, SJC Institute of Technology Chickaballapur, India[2]

ABSTRACT: One-tap authentication services have gained significant traction in cellular networks due to their ease of use, speed, and integration with biometric and device-based verification mechanisms. These methods, often leveraging fingerprints, facial recognition, or single-use codes, offer a streamlined user experience for secure access to mobile applications and online platforms. However, the increasing reliance on one-tap authentication has also introduced new security vulnerabilities. Attackers are developing sophisticated techniques to exploit weaknesses in these systems, aiming to bypass authentication and gain unauthorized access to sensitive user data. This paper explores the underlying architecture of one-tap authentication in cellular networks, identifies common attack vectors, and analyzes recent incidents highlighting the vulnerabilities of these systems. Additionally, it discusses mitigation strategies and potential improvements to enhance the security of one-tap authentication while maintaining user convenience. The findings underscore the critical need for robust security frameworks to protect users in an increasingly mobile-centric digital environment.

KEYWORDS: Authentication, leveraging, sophisticated, recognition.

I. INTRODUCTION

In today’s rapidly evolving digital landscape, mobile devices have become the primary medium for accessing online services, conducting financial transactions, and managing personal data. As a result, ensuring secure and user-friendly authentication mechanisms has become a critical requirement. One-tap authentication services have emerged as a popular solution, offering users a seamless and efficient way to verify their identities with minimal friction. These services typically rely on biometric identifiers such as fingerprints or facial recognition, or utilize single-use passcodes (OTPs) sent directly to the user's device. Their widespread adoption can be attributed to the simplicity and convenience they provide, which significantly enhances the overall user experience.

However, the increasing reliance on one-tap authentication in cellular networks has also made these systems attractive targets for cyberattacks. Threat actors are continuously devising sophisticated techniques to exploit vulnerabilities in both the authentication protocols and the mobile network infrastructure. Attacks such as man-in-the-middle (MITM) interceptions, SIM swapping, and manipulation of OTP mechanisms present serious risks to the integrity of user authentication. Moreover, mobile operating system vulnerabilities and social engineering tactics further expand the attack surface, making it imperative to address security concerns proactively.

In the context of cellular networks, the threat landscape becomes even more complex due to the interconnected nature of devices, communication protocols, and data transmission layers. Security flaws in encryption, data handling, and protocol design can be leveraged by attackers to bypass authentication and gain unauthorized access to sensitive information. Given the critical role that mobile authentication plays in safeguarding user accounts and personal data, the consequences of such breaches can be severe, including identity theft, financial loss, and privacy violations.

Furthermore, traditional password-based systems have proven to be inadequate in addressing both usability and security challenges. Users are often required to remember multiple complex passwords, leading to poor password hygiene and increased vulnerability to attacks such as credential stuffing and phishing. One-tap authentication services aim to mitigate these issues by simplifying the authentication process, yet they introduce their own set of risks that must be thoroughly understood and addressed.

This paper investigates the security vulnerabilities associated with one-tap authentication services in cellular networks. It analyzes common attack vectors, highlights recent incidents, and discusses potential countermeasures to enhance the resilience of these systems. By exploring the intersection of usability and security, this research aims to contribute to the development of more robust and secure mobile authentication frameworks suitable for the dynamic environment

II. LITERATURE SURVEY

One-Tap Authentication (OTAuth) based on the cellular network is a password-less login service provided by Mobile Network Operator (MNO) through the unique communication gateway access technique. The service allows app users to quickly sign up or log in with their mobile phone numbers without entering a password. Due to its convenience, OTAuth has been widely used by various apps. However, some studies have elaborated that OTAuth services are of great drawbacks from the perspective of mobile security and identified several flawed designs, which prevent the MNO from distinguishing malicious apps from normal ones and cause impersonation attacks [1].

It proposed a recently emerged cellular network-based One-Tap Authentication (OTAuth) scheme that allows app users to quickly sign up or log in to their accounts conveniently: Mobile Network Operator (MNO) provides tokens instead of user passwords are used as identity credentials [2].

They introduced self-organizing networks (SON) have emerged as a promising approach for managing and optimizing the performance of modern wireless networks. However, the dynamic and autonomous nature of SON also introduces security vulnerabilities and risks, making effective threat detection and mitigation crucial for ensuring the integrity and resilience of the network infrastructure [3].

It suggested that the threat landscape continues to evolve, companies have increasingly turned to a diverse array of tools and techniques to detect and combat potential risks. Cyber Threat Intelligence (CTI) emerges as a crucial resource, empowering organizations to stay one step ahead of these threats. However, in the face of constantly evolving security challenges, traditional Security Operations Centers (SOCs) reliant solely on SIEMs [4]

III. ARCHITECTURE OF THE SYSTEM

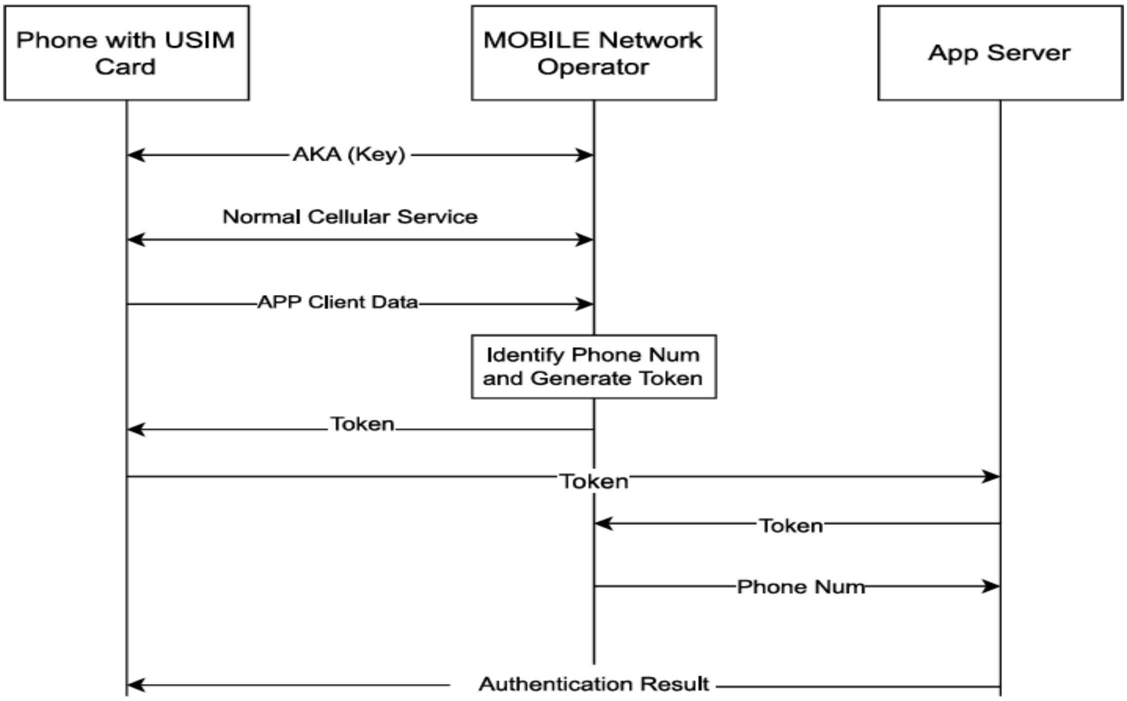


Figure 3.1.1 Block diagram for One-Tap Authentication Services in Cellular Networks

OTAuth is a secure SIM-based authentication method that uses the mobile network operator (MNO) to verify a user's identity via their phone number. The user's device must have a valid USIM and complete the AKA process to connect to the network. Once authenticated, the MNO assigns a LAN IP and uses it to link traffic to the user. The OTAuth app sends data to the MNO, which returns a token tied to the user's number. This token is verified by the app server through the MNO to approve or deny access.

Flow Algorithm

The OTAuth flow involves five key entities: the user, app client, MNO's SDK, app server, and MNO server. The app integrates the MNO's OTAuth SDK, using assigned appId and appKey for identification. The process is divided into three phases: Initialization, Token Request, and Phone Number Request. In the Initialization Phase, the app is configured with credentials and server IP. During the Token Request Phase, the app client communicates with the MNO to obtain a secure token. Finally, in the Phone Number Request Phase, the app server verifies the token with the MNO to authenticate the user.

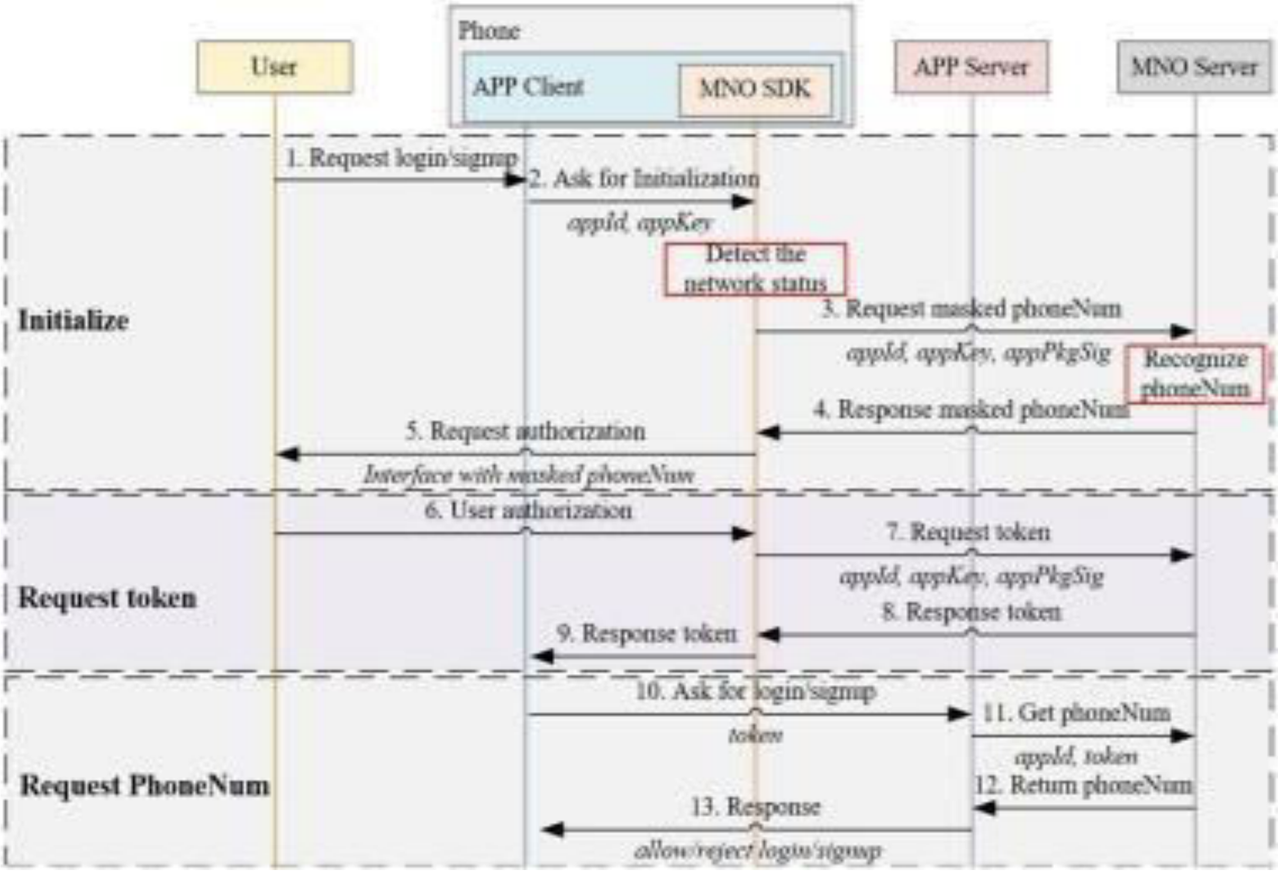


Figure 3.2.1 Phases for One-Tap Authentication Services in Cellular Networks

The OTAuth process involves three phases: Initialization, Token Request, and Phone Number Request. In the Initialization Phase, the user taps login, triggering the app to request authentication from the MNO SDK using appId. The SDK ensures mobile data is active, verifies app integrity, and sends the request to the MNO server. If valid, the server returns a masked phone number, which the app displays for user approval. In the Token Request Phase, upon user consent, the SDK sends a token request to the MNO server via mobile data. The MNO server verifies and returns a token linked to the user's phone number, without exposing the number itself. In the Phone Number Request Phase, the app client sends this token to the app server. The app server forwards it to the MNO serveral long with the appId. The MNO server verifies the request and returns the full phone number. The app server then decides whether to allow login or sign-up, ensuring a secure, SIM-based process.

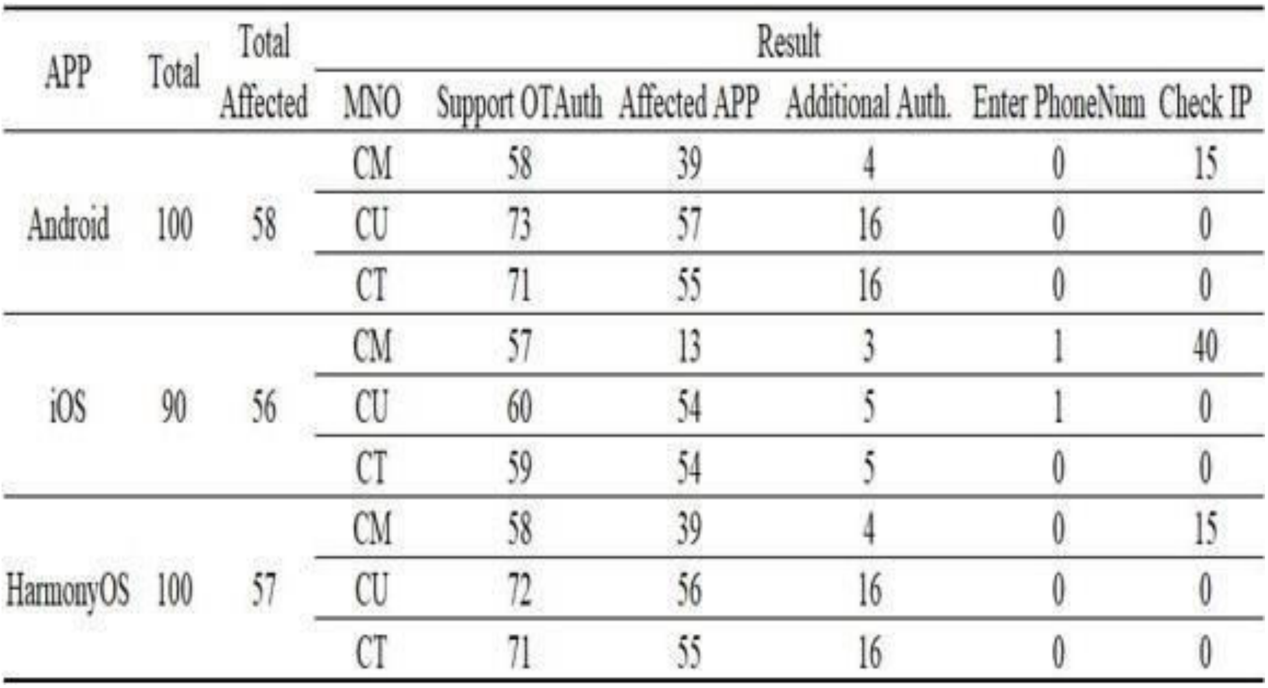
www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. RESULTS AND NOVEL CONTRIBUTION

To assess the vulnerability of OTAuth services, researchers tested popular apps on Android, iOS, and HarmonyOS using a controlled experimental setup. The setup included srsRAN, USRP B210, legal and programmable USIM cards, and smartphones, isolated in a shielding box to avoid external interference. A total of 290 high-download apps (100 Android, 90 iOS, 100 HarmonyOS) were selected based on prior research. Manual testing was conducted using a malicious 4G network to simulate attacks. OTAuth support was confirmed in 73 Android, 60 iOS, and 72 HarmonyOS apps.The attack model assumed the attacker accessed the victim's hotspot, and the victim had registered the app with their phone number. Unauthorized access was considered successful if the attacker could log in as the victim. Under this model, 58 Android, 56 iOS, and 57 HarmonyOS apps were found vulnerable. This revealed widespread weaknesses in OTAuth implementations acrossMNOs.The study highlights the need for stronger authentication safeguards in SIM-based systems.



APP	Total	Total Affected	Result					
			MNO	Support OTAuth	Affected APP	Additional Auth.	Enter PhoneNum	Check IP
Android	100	58	CM	58	39	4	0	15
			CU	73	57	16	0	0
			CT	71	55	16	0	0
iOS	90	56	CM	57	13	3	1	40
			CU	60	54	5	1	0
			CT	59	54	5	0	0
HarmonyOS	100	57	CM	58	39	4	0	15
			CU	72	56	16	0	0
			CT	71	55	16	0	0

TABLE 4.1 OVERVIEW OF OUR MEASUREMENT RESULTS

The study highlights significant differences in OTAuth security across mobile network operators (MNOs) and operating systems. China Mobile, China Unicom, and China Telecom implement OTAuth services differently, leading to varying vulnerability levels. Specifically, China Unicom and China Telecom do not verify local IP addresses during authentication, making their services more susceptible to attack compared to China Mobile, which includes this verification step. The experiment also revealed inconsistencies across operating systems; for instance, an attack on a China Mobile TikTok account succeeded on Android and HarmonyOS but failed on iOS. However, since many apps support cross-platform login, compromising one platform can allow access across all linked devices. The impact of the attack is further amplified by account linking between apps—gaining access to a UC Browser account, for example, could enable access to aconnected Sina Weibo account. This study also goes beyond prior research by Zhou et al., uncovering vulnerabilities in popular apps such as Ctrip, Meituan, and Huawei Music that were not previously examined. Unlike earlier attacks that relied on rooted devices, this approach operates without root access, bypassing common app defenses. These findings emphasize that OTAuth vulnerabilities vary widely across MNOs, operating systems, and app ecosystems, reinforcing the urgent need for stricter and more uniform security measures.

V. CONCLUSION

This study reveals critical security weaknesses in OTAuth services across major MNO sand platforms. The attack exploits flawed net work based authentication without requiring advanced privileges or device modification .Experimental results show widespread vulnerabilities and cross-app impact due to account linking. Existing defenses are inadequate, highlighting the need for stronger,standardized security mechanisms. Robust countermeasures must be adopted by MNOs and app developers to safeguard user identities.

VI. ACKNOWLEDGMENT

I am sincerely thankful to all my teachers for their guidance for my seminar. Without their help it was tough job for me to accomplish this task. I am especially very thankful to my guide Dr. S Bhargavi for his consistent guidance, encouragement and motivation throughout the period of this work. I also want to thank our Head of the Department (E&C) Dr.Rangaswamy for providing me all necessary facilities.

REFERENCES

[1] Z. Cui, B. Cui, J. Fu and B. K. Bhargava, "An Attack to One-Tap Authentication Services in Cellular Networks," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 5082-5095, 2023.

[2] Z. Zhou, X. Han, Z. Chen, Y. Nan, J. Li and D. Gu, "SIMulation: Demystifying (Insecure) Cellular Network based One-Tap Authentication Services," 2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Baltimore, MD, USA, 2022, pp. 534-546.

[3] C. S and J. J. Thangaraj, "Threat Detection And Mitigation In Self-Organizing Wireless Communication Network," 2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon), Singapore, Singapore, 2023, pp. 28-32,

[4] A. H. Nursidiq and C. Lim, "Cyber Threat Hunting to Detect Unknown Threats in the Enterprise Network," 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs), Bogor, Indonesia, 2023, pp. 303-308.

[5] S. Vongsuvat and C. Srisaan, "Cybersecurity Threat Detection Analysis via Exploratory Data Analysis," 2024 8th International Conference on Information Technology (InCIT), Chonburi, Thailand, 2024, pp. 484-489.

[6] J. Paramesh, K. P. Sriram, E. Anbalagan, S. Sasikumar and M. G. Vimal Kumar, "Developing an Adaptive Security Framework for Real-Time Threat Detection and Response in Cloud- Network Systems," 2024 International Conference on Cybernation and Computation (CYBERCOM), Dehradun, India, 2024, pp. 644-648.

[7] Z. Zou, B. Wang, F. Li and B. Ye, "Research on Network Security Threat Analysis Method Based on Knowledge Graph," 2024 IEEE 7th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 2024, pp. 668-672.

[8] K. T. Nitesh, A. K. Thirumala, U. F. Mohammed and M. R. Ahmed, "Network Security Threat Detection: Leveraging Machine Learning Algorithms for Effective Prediction," 2023 12th International Conference on Advanced Computing (ICoAC), Chennai, India, 2023, pp. 1-5.

[9] multi-target threat assessment," 2024 4th International Conference on Artificial Intelligence, Robotics, and Communication (ICAIRC), Xiamen, China, 2024, pp. 776-780.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details