NFSU JOURNAL OF FORENSIC SCIENCE
ISSN: 3049-2408 (Online)
Journal Homepage: https://jfs.nfsu.ac.in/

SIM Swapping Attacks: Mechanisms, Identity Takeover Pathways, and Forensic Countermeasures in Modern Telecom Networks

Hiba A N[1][0009-0007-9692-4732], Steve Jerson K[1], Shreya Naik[10009-0003-7804-3211], Naveen Kumar Chaudhary[2] [0000-0002-5851-6996], and Sandeep Munjal[1,2, [0000-0002-3318-5748]

[1]Multidisciplinary Research & Innovation Centre, National Forensic Sciences University, Goa Campus, Curti, Ponda, Goa, India, 403401

[2]School of Cybersecurity and Digital Forensics, National Forensic Sciences University, Gandhinagar, Gujarat, India, 382007
drsandeepmunjal@gmail.com (Corresponding Author) *

Abstract

Due to the ubiquity of mobile devices for digital identity verification, SIM swapping has emerged as an unintended high-stakes vector for cybercrimes. With the advancement of telecommunications technology from GSM to 5G, reliance on the Subscriber Identity Module (SIM) for two-factor authentication (2FA) has become a critical vulnerability. In this paper, fraudsters employ a variety of techniques, ranging from social engineering to technological exploitation, across both traditional and contemporary network infrastructures. We investigate identity takeover methods that circumvent traditional security mechanisms and cause significant financial and personal losses. In addition, this study assesses telecom infrastructure weaknesses where unique vulnerabilities of GSM, LTE, and UMTS interworking exist, and covers new attacks, including AdaptOver. Eventually, we propose a model for forensic countermeasures and mitigation by focusing on location-based verification, device-specific authentication binding, and increased ceremony modelling to protect subscriber identities.

Keywords: telecommunication fraud, SIM swapping, identity theft, authentication, network security, forensic analysis

1. Introduction

The mobile phone number has evolved into a form of digital identification, rather than a mere communication address, in the current digital environment. It is the main mechanism for account restoration, banking transactions verification and Two-Factor Authentication (2FA) for social media and e-mail. As a result, the telecommunication field is experiencing an epidemic of “SIM swapping” fraud. It is known as a SIM split or port-out scam, in which a fraudster uses a mobile network operator (MNO) to transfer the victim's phone number to a new SIM card under the fraudster's control. The attacker will be able to bypass the SMS-based security procedures by listening for calls and SMS Interception after the transfer (Kim et al., 2022). The frequency of these attacks shows a very clear contrast between the quick adoption of digital service development and the vulnerability of the security infrastructure. Even as modern technology, such as LTE and 5G networks, continues to evolve, legacy protocols like Global System for Mobile Communications (GSM) are still being implemented as "back-up" networks, resulting in continuous vulnerability shortfalls. By exploiting these human-caused holes, attackers can successfully execute takeovers. Financial gain is one of the main motivations behind such attacks when the adversary acquires access to the line of a victim, and immediately pursues wallet and bank account accounts within days (Bhavana et al., 2024). The problem is made worse by the truth that the stuff used to carry out these frauds isn’t strictly technical – as well as cyber-attacks – it can also be an amalgam of social engineering as well as technical exploitation. As Kim et al. as well as the more people can access personal data on dark web, attackers can produce detailed dossiers on the victims to trick the customer support representatives (Kim et al., 2022). A critical study of these mechanisms is provided in this paper. Here, we start with the operational stages of exploitation and identity takeover. Further, we examine the fundamental infrastructural weaknesses, ranging from GSM vulnerabilities to the current adaptive overshadowing assaults, that cause these crimes. In order to prevent these widespread threats, we conclude with advanced precautions such as location-based data usage and heterogeneous information binding.

2. Explanation mechanisms and identity takeover

Differing from phishing or malware, a SIM swap attack aim at the user-versus-the service provider connection instead of the user device itself. A holistic, total takeover of identities is resulted due to several forms of exploitation, including data acquisition, fraudulent provisioning, and service exploitation.

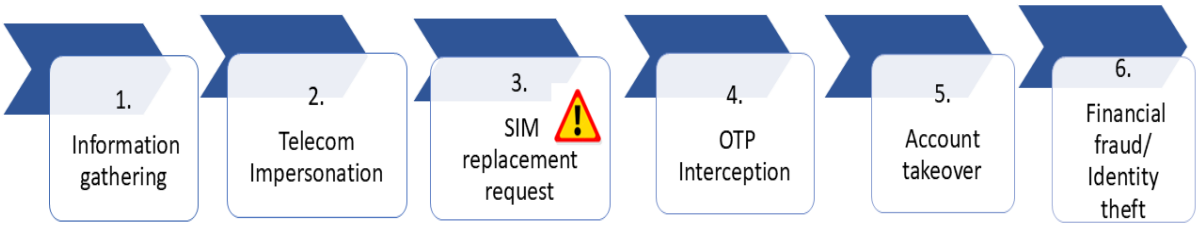

Fig.1. SIM swap attack flow diagram: step-by-step attack lifecycle from attacker to victim impact.

2.1 Personal Data Theft and Social Engineering.

The accumulation of personally identifiable information (PII) is the first stage in SIM swapping. Attackers can use data obtained from phishing, previous data breaches or open-source intelligence (OSINT) without the need of physical access to a victim's device. Here is an example in which Kim et al explains how the fraudsters take advantage of this stolen information, such as addresses, birth dates, and at times even the partial social security number, to get past the security questions asked by telecom customer service. Here, it is critical to manipulate the telecom support staff psychologically. To obtain SIM activation on a new card, the attacker usually pretends as a real subscriber and claims a lost or broken phone. In some complicated scenarios, it is also witnessed that the "insider threats", i.e., the criminals, may bribe or threaten the telecom employees to directly perform the swap, avoiding the verification procedure entirely. When processing the request, the legitimate user's SIM card becomes "No Service" and it no longer connects to the network when the carrier responds. This signal of disconnection has become the ultimate indicator that the identity takeover is on-going.

2.2 The second type of attack, service use: Exploitation of a Service and the 'Domino Effect'.

An attacker may be able to take advantage of systems through the "forgot password" of different online services once a successful SIM swapping is achieved to get the "forgot password" features of a lot of services by exploiting the system. As the vast majority of mobile-based services rely on SMS for the sending of One-Time Passwords (OTP), the attacker has the codes sent to their hand and sends the victim's phone number, which they are now using, and a few other codes are sent to the compromised device for targeting. Faircloth et al. highlight that this has a fast but "domino effect," whereby gaining a primary email account generates a series of compromises across banking, social media and cryptocurrency platforms (Faircloth et al., 2022). The identity takeover goes further than the financial loss. Such as sending messages to a victim's contacts, calling on them for help or sending them malware. The study by Bhavana et al. emphasizes that the speed of this exploitation is very important,

attackers regularly initiate a password reset process in order to make this exploit go as fast as possible to do maximum damage possible before reaching out to the service provider to reverse the change (Bhavana et al., 2024).

2.3 Limitations of Multi-Factor Authentication (MFA)

SIM swapping essentially negates the value of SMS-based Multi-Factor Authentication. 2FA is a critical security best practice that is currently most commonly recommended, but the Short Message Service (SMS) makes use of the illusion that owning the phone number itself will give you ownership over that phone. This assumption is rendered invalid by SIM swapping. The studies suggest user credentials (passwords) may still be secure, and the compromise of the second factor enables attackers to authenticate successfully (Bhavana et al., 2024). However, given that SMS is commonly used in the industry and is simple and clear for the general public when looking for an authentication method, this vulnerability has led many to call for a decoupling mechanism outside of the SIM card, especially with regards to the application-based generators or hardware keys.

2.4 Telecom infrastructure vulnerabilities

Social engineering usually served as the primary method to start SIM swapping, inherent vulnerabilities in the telecommunications infrastructure make these attacks often feasible and successful. Mobile networks use a sophisticated network of interconnected technologies that support each other including 2G(GSM), 3G (UMTS), 4G (LTE), and 5G.

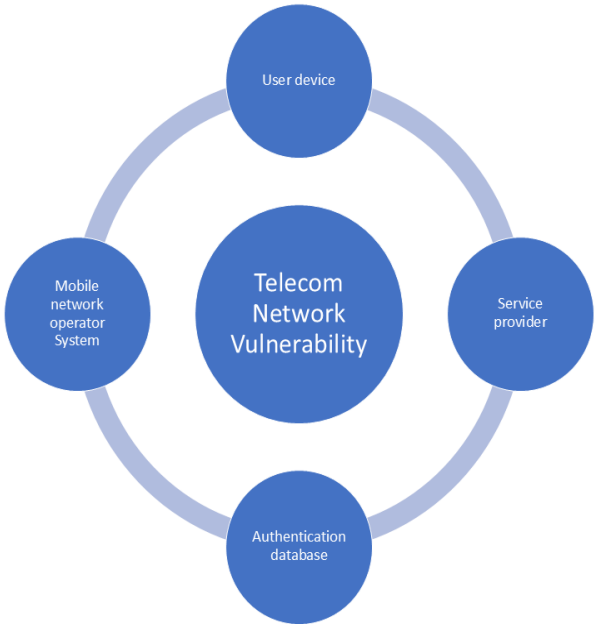

Fig.2. Telecom Network Vulnerability Model: depiction of where the weakness exists in the telecom ecosystem.

2.5 GSM and the Man-in-the-Middle Attack.

Even with a broad migration to LTE and 5G, GSM networks are most commonly kept up for compatibility and emergency service coverage. GSM protocols do not require mutual authentication (meaning the phone authenticates to the network, but the network does not authenticate to the phone). This flaw also allows for IMSI catchers (Stingrays) and base station spoofing. Bello and Kanu showed that penetration testing on GSM networks demonstrates a significant vulnerability to MITM. An attacker can establish an untrusted base station in which nearby telephones must downgrade to 2G encryption (one of the most vulnerable formats to be cracked) or no encryption at all (Bello & Kanu, 2023). Furthermore, Voznak et al. stress that these chosen attacks against GSM are practical and feasible in practice with inexpensive hardware, rather than theory (Voznak et al., 2015). Although these technical attacks may be separated from administrative SIM swap, they are part of the larger whole and part of a wider ecosystem of SIM insecurity. When an IMSI catcher adopts an attack, attackers have an opportunity to obtain the IMSI (International Mobile Subscriber Identity) and use the IMSI for a specific spoofing or swapping attack at a later time.

2.6 Interworking hazards of UMTS and LTE.

The security improvements brought onboard with UMTS (3G) and LTE (4G) proposed to remedy the GSM weaknesses but issues still exist in the interworking, i.e., the handoff between generations. Ahmadian et al. explain where security protocols are lowered at handover between UMTS and GSM, thus leaving open the possibility of interception or redirection (Ahmadian et al., 2010). If a network makes a user abandon an older protocol, the precautions of the new ones lose their protection. This heterogeneity makes the SIM swapping process even more challenging to identify fraudulent activity. A legitimate user’s device and an attacker’s device (after the swap) may try to register on the network using different protocols or device identifiers (IMEI), not flagging this anomaly immediately in legacy systems.

2.7 More sophisticated attacks in cellular networks: AdaptOver.

When faced with security challenges that involve sophisticated attacks in cellular networks like "AdaptOver" (also known as Adaptive Overshadowing). Erni et al. model this strategy, in which an adversary sends packets into a cellular network by dominating the legitimate signal (Erni et al., 2022).The AdaptOver is primarily involved with denial-of-service or privacy-leak vector due to its relevance to SIM swapping lies in the manipulation of control plane messages. If an attacker can

overshadow the legitimate registration messages of a user or the network's denial messages, they can create confusion regarding the state of the subscriber. This depicts that even the air interface of modern networks is susceptible to manipulation which in turn compromises the integrity of subscriber identities. Implementing embedded SIMs, or eSIMs is based upon the goal to reduce physical SIM theft. On the other hand, Kim et al., propose that eSIMs develop new digital channels for exchanging (Kim et al., 2022). An attacker can obtain an eSIM instantly to their device if they are able to access their account through the telecom portal. This removes the necessity for them to visit a store or obtain a physical card. The attack window is shortened by these quick activations, providing victims little to no time to react before their service is taken over or compromised.

2.8 Forensic countermeasures and mitigations

To prevent SIM swapping, a multi-layered approach that includes new subscription awareness, improvement of technical authentication technologies, and telecom operator's policies is necessary. Conventional methods for identification, like "static" information (such as the mother's maiden name and address) are now no longer relevant and it does not provide adequate security. Therefore, mitigation techniques need to move more toward real-time and dynamic that can adapt to changing threats.

A. Location-Based and Behavioral Verification.

Continuous use of MNO's real-time telemetry is one among the most promising safeguards. Cheruyot et al. suggest a security framework that uses an encryption method to validate SIM swap requests using user location data (Cheruyot et al., 2024). Its reasoning is based on the physical probability that a request for a SIM card switch would be classified as high-risk if it came from a location, such as kiosk or IP address, that is physically far away from the known location of your mobile device. This includes a digital layer of physical context to the request. Also, the detection systems can also be trained to identify unusual behaviour patterns. That includes looking at the "age" of the request (eg the user has changed passwords in recent times? their frequency of calls to customer service and device history. These heuristics, if integrated into the automation, can ensure the creation of human agents to be socially engineered when a suspicious provisioning request is created.

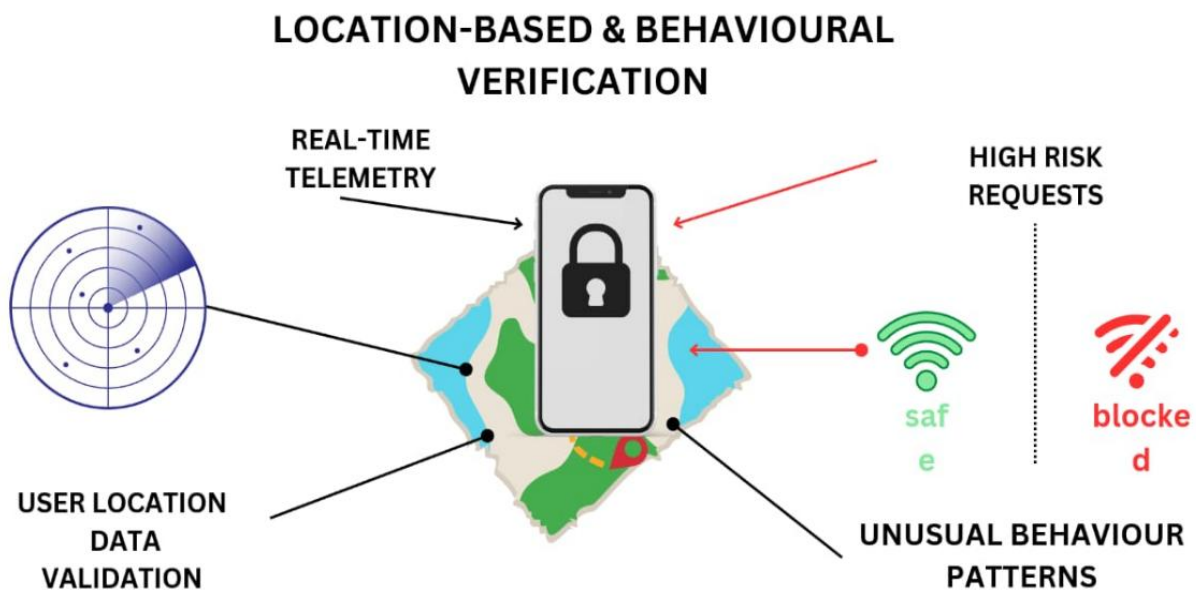

Fig.3. Location-Based Behavioural Verification: Uses real-time data to detect anomalies and block risky access.

B. Heterogeneous Information Binding and Protocol Hardening.

Technical controls must then bind the identity more closely to the hardware to prevent cloning and unauthorized identification transfers. Yang et al. propose an M2M (Machine-to-Machine) device authentication scheme that associates heterogeneous data to the USIM card (Yang et al., 2020). In practical terms, not only would the network-authentication require valid SIM credentials (IMSI/Key), but also a pre-registered (or compatible) hardware signature (such as, the IMEI). If the SIM is transferred to an unknown device (the attacking device's mobile phone), the match will not allow authentication. Similarly, Zidouni et al. describe new safety features that are intended to defend 3G/4G SIM cards against cloning (Zidouni et al., 2018). Whereas physical cloning is less popular than administrative swapping, the need to apply the cryptographic pairing (and thus, cryptographic pairing of the card to each corresponding to the underlying network core) at the physical level is important to block spoofing in general.

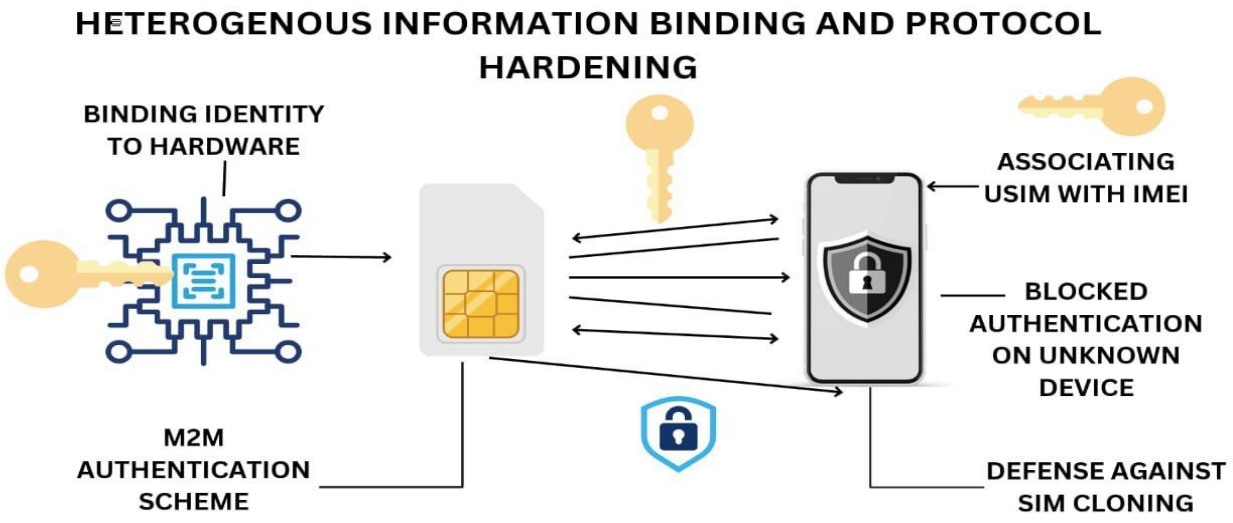

Fig.4. Secure SIM Authentication via Identity Binding and Protocol Hardening: prevents unauthorised access and SIM cloning.

C. Ceremony Modelling and Procedure Enforcement.

From the forensic and procedural perspectives, the human component of the SIM swap "ceremony" (the interactions between users and operator) must be protected. Rosa et al. explore the problem of weak authentication by applying "Ceremony modeling" to detect security loopholes in the validation process (Rosa et al., 2025). It takes the human protocol as an example and acts on it as a cryptographic protocol, capturing every interaction with our clients and tracing exactly where they make authorization problems. By embedding such ceremonies into the organization's rules, operators can place required conditions on the customer by including a mandatory cooling off period after a SIM swap request, or another verification to the old device via a non-SMS (e.g., email or push notification through Wi-Fi) before the SIM swap is finalized, etc.

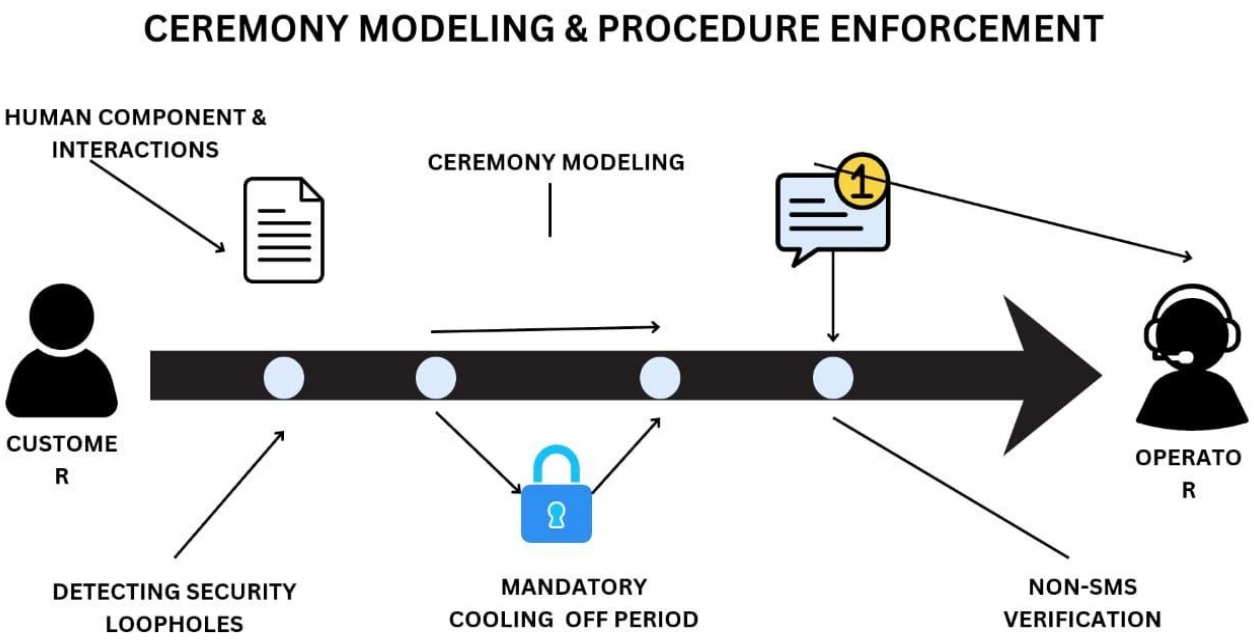

Fig.5. Structured ceremony modelling with enforced procedures to secure customer-operator interactions and mitigate vulnerabilities.

D. User Alerts and Forensic Testing.

In the case of an incident, post-incident forensics is crucial for launching an action and patching a system. Faircloth et al. demonstrate that an exploration of swap logs reveals patterns that may be revealing such as what internal operator tools were utilized during the migration. Second, improved logging helps to differentiate technical error and malicious swap. By the end user, automatic notification processes are critical. Users must be informed every time a SIM not associated with their IMEI will register and/or any port-out requests on the member-linked bank account. A recent trend analysis in India showed that without real time visibility, users are not aware until they experience financial harm.

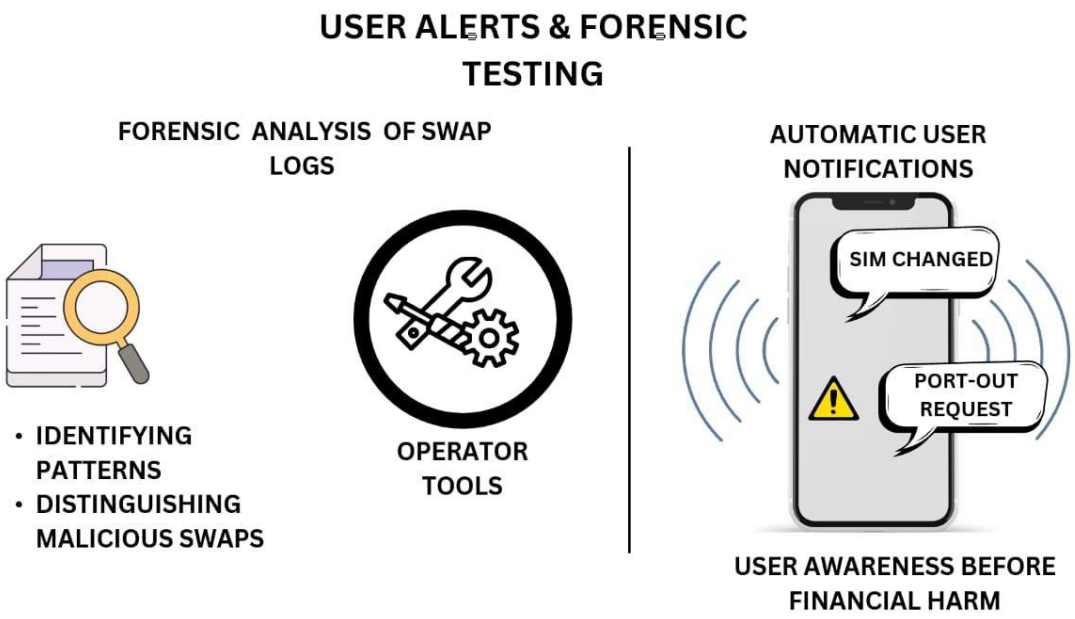

Fig.6. User Alerts and Forensic Testing Framework: for Detecting and Preventing SIM Swap Fraud.

3. Conclusion

SIM swapping is the amalgamation of old network gaps, clever social engineering and generally we treat phone numbers like proof of our identity. Even though users have switched from GSM to 5G, the problem has not disappeared, it has just shifted the weak spots to behind-the-scenes parts of the telecom industry. Instead of attacking the basic networks, attackers have started targeting the telecom companies, customer service processes and various connections that are available between different network functions. Attackers don't need fancy tools to hack a system; they usually do phishing activities to trick people or steal information using SMS based two factor authentication. The real weak point isn't the technology but the human verification process which can be easily stolen by the attackers and has the ability to convince the telecom providers to transfer a victim's number to a new sim card. To reduce the risk, telecoms need to go beyond the knowledge-based questions. They need to use adaptive checks like device binding, location and phase out SMS for high value actions.

References

[1] Ahmadian, Z., Salimi, S., & Salahi, A. (2010). Security enhancements against UMTS–GSM interworking attacks. *Computer Networks*, *54*(13), 2256–2270.

[2] https://doi.org/10.1016/j.comnet.2010.01.005

[3] Bello, N., & Kanu, O. (2023). PENETRATION TESTING OF GSM NETWORK USING MAN-IN-THE-MIDDLE ATTACK. *JES. Journal of Engineering Sciences*, *0*(0), 0–0. https://doi.org/10.21608/jesaun.2023.226718.1249

[4] Bhavana, S. U., Doreen Hephzibah Miriam, D., & Rene Robin, C. R. (2024). Understanding the Implications of SIM Card Swap Fraud in India: A Comprehensive Study. *2024 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, 1–8. https://doi.org/10.1109/IC3IoT60841.2024.10550217

[5] Cheruyot, C. C., Michel Kouame, R., & Inaba, H. (2024). Securing SIM Toolkit-Based Mobile Money Applications Against SIM Swap Attacks Using User Location Data. *2024 IEEE 13th Global Conference on Consumer Electronics (GCCE)*, 100–104. https://doi.org/10.1109/GCCE62371.2024.10760647

[6] Erni, S., Kotuliak, M., Leu, P., Roeschlin, M., & Capkun, S. (2022). AdaptOver: Adaptive Overshadowing Attacks in Cellular Networks. *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM*, 743–755. https://doi.org/10.1145/3495243.3560525

[7] Faircloth, C., Hartzell, G., Callahan, N., & Bhunia, S. (2022). A Study on Brute Force Attack on T-Mobile Leading to SIM-Hijacking and Identity-Theft. *2022 IEEE World AI IoT Congress (AIIoT)*, 501–507. https://doi.org/10.1109/AIIoT54504.2022.9817175

[8] Kim, M., Suh, J., & Kwon, H. (2022). A Study of the Emerging Trends in SIM Swapping Crime and Effective Countermeasures. *2022 IEEE/ACIS 7th International Conference on Big Data, Cloud Computing, and Data Science (BCD)*, 240–245. https://doi.org/10.1109/BCD54882.2022.9900510

[9] Rosa, L. G., Zambonin, G., & Martina, J. E. (2025). *Enhanced SIM Swap Security Practices via Ceremony Modeling* (pp. 201–211). https://doi.org/10.1007/978-3-031-87775-9_17

[10] Voznak, M., Prokes, M., Sevcik, L., Frnda, J., Toral-Cruz, H., Jakovlev, S., Fazio, P., Mehic, M., & Mikulec, M. (2015). *Vulnerabilities in GSM technology and feasibility of selected attacks* (E. M. Carapezza, Ed.; p. 94560T). https://doi.org/10.1117/12.2177111

[11] Yang, T.-W., Ho, Y.-H., & Chou, C.-F. (2020). Achieving M2M-device authentication through heterogeneous information bound with USIM card. *Future Generation Computer Systems*, *110*, 629–637. https://doi.org/10.1016/j.future.2019.10.042

[12] Zidouni, N., Chitroub, S., Chebout, H., & Boukais, N. (2018). New safety measure to protect the 3G/4G SIM cards against cloning. *2018 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT)*, 1–8. https://doi.org/10.1109/MoWNet.2018.8428876