International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

SIM - Swap Technique - A Legitimate Customer Request

Depavath Harinath

Lecturer, Department of Computer Science, Hyderabad, Telangana, India

Abstract: ***Subscriber Identity Module (SIM) swapping is a legitimate procedure performed by a customer to change their mobile SIM card when the SIM card has been lost, damaged or stolen; or when a customer want to upgrade his SIM from 2G/3G SIM to 4G/5G SIM or when a customer want to move to another mobile telecom service provider – which is called number portability. But fraudsters misuse this SIM swap technique to steal legitimate SIM card user's data which is a cyber fraud through a successful social engineering. As a result, the fraudster gain access to the bank accounts and can receive all the SMS and video calls intended for the legitimate subscriber. Therefore fraudsters can perform online banking frauds. This paper illustrates what SIM swap is and its related issues.***

Keywords: SIM, eSIM, SIM swap, Cyber attack

1. Introduction

A Subscriber Identity Module or subscriber Identification Module (SIM) is an integrated circuit intended to securely store the International Mobile Subscriber Identify (IMSI) number assigned by mobile telecom service provider and its related key, which are used to identify and authenticate subscribers on the Global System for Mobile Communications (GSM) telephony devices. Technically the actual physical card is known as a Universal Integrated Circuit card (UICC). We identify individual subscribers with its unique international mobile subscriber identify number or SIM card number. Our SIM card stores identifying information that authenticates our mobile phone service and allows us to connect to mobile network. Our mobile phones are loaded with information, right from contact lists, photos, emails, and Short Message Services (SMSes) to financial details such as Automated Teller Machine (ATM) withdrawal alerts and One Time Passwords (OTPs) sent by banks for net banking transactions.

Figure (i): illustrates a typical SIM card

Now this SIM card's number is becoming an entrance for criminals. Cyber criminals don't even need to steal mobile phone to gain access to our mobile number and personal information. This recent trend in hacking is known as SIM card swapping or simply SIM swap. SIM swap service is offered by telecom providers. SIM swap offers a simple way to get our stolen SIM card number again by blocking the old SIM and activating the new SIM with the same phone number.

Therefore Subscriber Identity Module (SIM) swapping is a legitimate procedure performed by a customer to change their SIM card when:

1) The SIM card has been lost, damaged or stolen; or
2) When a customer want to upgrade his SIM card from 2G/3G SIM to 4G/5G SIM format; or
3) When a customer want to subscribe to another mobile telecom provider (e. g.: from Jio SIM to Airtel SIM) - which is called number portability.

But fraudsters misuse this SIM swap technique by exchanging a SIM of target person with new SIM held by fraudster without knowing by the target. As a result, all calls and text messages to the victim's number are directed to the impostor's phone, including One Time Passwords for banking transactions. After getting a One Time Password (OTP) from a bank, the impostor can then access the victim's bank account and transfer funds.

Therefore SIM swap scam involves an attacker hijacking a victim's mobile phone number by porting the number to a SIM card that is under his control by impersonating the victim to mobile telecom service provider.

2. How a SIM swap scam works

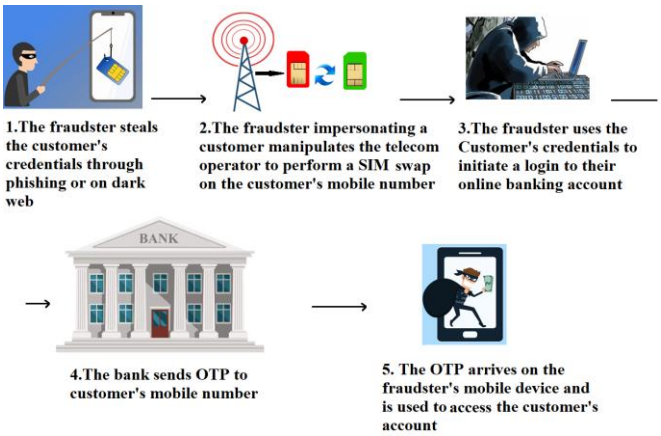

Figure (ii): illustrates SIM - swap scam process

a) SIM swap scam (also known as port - out scam, SIM splitting, Smishing and simjacking, SIM swapping) involves collecting so much information about the victim. In this scam fraudster might send phishing mail or through Trojan horse malware to collect sensitive information from victim.

Information of interest to the hacker includes ID numbers, contact details, residential and postal addresses, banking details such as account numbers, credit card numbers, debit card number, CVV (Card Verification Value) number, expiry date of card, and online banking credentials (such as username and password) etc. Sometimes fraudster calls target acting as a mobile service provider, customer care unit or a banking official to ask our private information like CVV/ATM card number or secret PIN (Personal Identification Number) etc. Then victim provides all sensitive information in hands of fraudster. Fraudsters also collect our personal data through our social media websites by hacking them. Therefore, SIM swap scam begins with a fraudster gathering personal details about the victim, either by use of phishing emails, by buying them from organized criminals, or by directly socially engineering the victim.

This attach may be launched in the following ways:

- **Phishing Email** – Attacker sends a fake email to the victim containing a form or a link to a spoofed website to capture personal information.
- **Vishing (voice phishing)** – Attacker calls the victim impersonating a bank official or an official of reputed company and collects personal information.
- **Smishing (SMS phishing)** – Attacker sends a fake SMS to the victim containing links to a fake website or a malware that can steal user information.

In many cases, SIM numbers are changed directly by telecom company employees bribed by criminals.

b) Once criminals gather enough information they create false identity of victim. First, they call mobile service providing operator and request them to block original SIM with fake reason like loss, theft or damage of SIM card.
c) After this fraudster visit the mobile operator's retail outlet with fake ID proof posing as a genuine owner and gets new SIM with owner's name. Once new SIM is issued, then genuine customer's mobile phone will not receive any phone calls or messages because mobile phone will be without mobile network. This happens within some hours before real owner lodging the complaints against mobile has stopped working.
d) The fraudster initiates financial transactions by generating One Time Password (OTP). Since this OTP received on new SIM which held by the fraudster, the money can be transferred into an account of someone else person who is known to fraudster. So, fraudster will not be caught by police and that person will get reward who had kept money in his bank account from fraudster.

3. Some of SIM Swap Fraud Incidents

a) Hindustan Times news report says – on 14th November 2018 - A caller posing as Airtel employee clones Pune (a place in India) man's SIM, steals Rs.93.5 lakhs: The fraudster called to Pune based man saying he is employee of Airtel telecom provider and asked to share information otherwise his SIM card will stop working. The victim shared details of his SIM card which was linked to bank account. The victim came to know later that Rs.93.5 Lakhs were transferred from his bank.

b) A number of high - profile hacks have occurred utilizing SIM swapping, including some on the social media sites Instagram and Twitter. In 2019, former Twitter CEO Jack Dorsey's Twitter account was hacked via this method.

c) Mumbai Mirror a daily newspaper says – on 2nd January 2019 – Mahim (a place in India) based businessman loses Rs.1.86 crore in six late - night missed calls: The victim received the six missed calls on the mid night of 27 - 28 December 2018 from two mobile numbers, after which his SIM was deactivated. He was informed by mobile service provider that the SIM was deactivated by himself for new SIM card. But he did not requested for deactivation of SIM and become a victim of fraud. He rushed to his bank to find the fraud of Rs 1.86 crore from his account. He was told that his money was transmitted to 14 accounts across the country through 28 transactions. The bank was able to retrieve only 20 lakh rupees.

d) Telecom Company told to pay Rs.8 lakh to victim of SIM - swap fraud: The civil court for cybercrimes in Maharashtra (a state in India) on 28th February 2019 directed Telecom Company Tata Docomo to compensate Rs.8.2 lakhs to an ICICI bank account holder for issuing a duplicate SIM. The SIM card was used by fraudster to get Rs.7.8 lakh using internet banking.

e) In May 2020, a lawsuit was filed against an 18 year old Irvington High School senior in Irvington, New York, Ellis Pinsky, who was accused with 20 co - conspirators of swindling digital currency investor Michael Terpin - the founder and chief executive offer of Transform Group – of $ 23.8 million in 2018, when the accused was 15 years old, through the use of data stolen from smart phones by SIM swaps. The lawsuit was filed in federal court in White Plains, New York and asked for triple damages.

f) The HINDU news report says – on 14th December 2022 – SIM swap fraud: man gets missed calls, loses Rs.50 lakh: A south Delhi (in India) based businessman was duped of more than Rs.50 lakh by some unknown scammers through a series of missed calls, the police said that the victim had not shared any ITP or any personal details with the accused. The Man, in his complaint, said he received several missed calls and when he picked up one of the called, there was no response from the caller. Later, he found out that multiple transactions were made from his bank account and he lost nearly Rs.50 lakh. A case has been registered at the Delhi police's cyber crime unit. According to a senior police officer, initial inquiry suggested the victim was duped using a SIM - swap technique.

4. Steps to avoid becoming a target of a SIM swap fraud

a) Don't reply to doubtful emails. Your bank would never ask you to enter any private information into an email.
b) Don't ever click on web links that may lead you to phishing websites.
c) Use private email address that nobody but you and your

bank know for net banking purpose.

d) Always visit official website of your bank by typing URL in address bar. Don't book mark website name because malware could tamper with bookmarks and redirect you to phishing website.
e) Change net banking password regularly and make sure it should be strong password too.
f) Do not share personal sensitive information like Customer ID, Credit/Debit card number, expiry date card, CBB number to anybody including bank person (on Phone), customer care executive of mobile service provider over call, email or SMS.
g) If our phone is out of network continuously for a few hours, it is an alert and you should complain the same to your mobile operator immediately.

5. Steps to follow in case of SIM swap attack

a) First, call your bank and block your debit and credit card transactions in case you have identified a fraud transaction.
b) Second, call your operator, and file a proper complaint. You are required to visit them with original ID proof and address proof to complain about your case.
c) If you see no service on your SIM, contact the mobile service operator at the earliest. If your SIM has been deactivating at midnight, you can't do much about it.
d) If your phone is out of coverage network constantly for a few hours, then you must take it seriously and be alert and complain the same to a mobile operator.
e) Never switch off your mobile for long period of time to avoid unsolicited calls. Instead, try not to pick them. Otherwise, activate DND (Do Not Disturb) service for your SIM.
f) It is a good idea to safeguard your account, mobile number through various ways. What is more important is awareness of where and how you share your personal information.

6. Recommendations

6.1 For Mobile Network Operators:

a) Regular and targeted training of employees:
While technical controls can minimize the risk of SIM swapping, the human factor is the one that needs to be constantly managed.

According to the ENISA (European Union Agency for Cyber security) Threat Landscape 2020, 84% of cyber attacks relay on social engineering.

Mobile Network Operators (MNOs) should provide regular cyber security awareness training for both their own and third party employees to ensure they can recognise and appropriately deal with the SIM - swapping threat. The security awareness programme should be tailored to the audience and focused on the specific topic. For example, employees should know and understand how spear phishing and other social engineering attacks work, what they should take into account when authorizing a SIM swap and the actions they should take to minimize the risk of fraud.

There should be well - documented and checked processes that are regularly communicated and followed with vigilance. Moreover, records of the training courses and those who attended should be maintained.

b) Application Programming Interface (API) between Mobile Network Operators and banks:
Banks can use an Application Programming Interface (API) provided by the MNOs to check whether a SIM swap has been recently performed. Such an API has been developed in several European Union (EU) countries as a cross - MNO initiative. In Italy, for instance, the national regulatory authority, AGCOM, has been coordinating a trial in which participated representatives of the Bank of Italy, the Italian Data Protection Authority, the Ministry of Economic Development, the police (including financial police), banks, operators that offer messaging services to the banks and MNOs. The trial involves MNOs informing banks of the latest SIM swap, either through the subscriber's IMSI (International Mobile Subscriber Identity) or hashed IMSI or by sending information about the time of the latest SIM swap.

The API works as follows:

- The customer initiates a fund transfer on their mobile banking application or on a computer.
- The bank interrogates the customer's MNO's database through an API.
- The customer's MNO checks whether a SIM swap has recently occurred on the Customer's MSISDN (Mobile Station Integrated Services Digital Network). Alternatively, the bank sets the timing threshold (e. g.24 hours) and the MNO responds if a SIM swap occurred in less than the timing threshold.
- If no recent SIM swap has been detected on the customer's MSISDN, the information is sent from the MNO to the bank and the bank performs additional checks in order to authorize the transaction.

c) Restrict the provision of 'empty' SIM cards:
During my research, I came across fraud cases with the attacker using an inactive SIM card and managing to perform a fraudulent SIM swap.

To address this threat, MNOs could consider not authorizing SIM swaps without knowing the origin of the new SIM card. SIM cards should be provided only through the MNO's logistics centres, while using of existing stocks at the subscriber's disposal should be discouraged.

Additional internal controls may be implemented within the mobile network operators:

- Keeping an inventory of the blank SIM cards;
- Strong controls on the issuance and activation of blank SIM cards; and
- Activation of the SIM cards only when the order and/or delivery is confirmed by the customer.

d) Artificial intelligence and behavioural analysis:
Artificial intelligence (AI) may be used to perform automatic behavioural analysis of subscriber's activities. The AI engine could store several habits of each customer (e. g. connection history, IP address location) in order to have a basis for comparison at the time of a requested SIM swap.

If abnormal behavior is detected (e. g. Sudden change of the IP address location, several concurrent connections from different IP addresses), the MNO is alerted in real time in order to block the SIM - swapping process.

6.2 For the Banks:

a) API between MNOs and banks:
By using Application Programming Interface (API) banks have the possibility to check whether a SIM swap has been recently performed with the use of an API provide by the MNOs.

b) Migrate from a simple SMS two - factor authentication to app - based two - factor authentication:
The latest banking frauds related to SIM swapping suggest that a simple SMS two - factor authentication (AFA) may not provide a sufficient level of security.
App - based 2FA relies on biometric, PIN or password - based authentication of the customer, and thus does not pose a risk of the SMS OTP being intercepted. We note that such app - based 2FA is already used by many banks to authorize transactions, replacing the SMS 2FA process.

c) Reach out to the public:
Banks, along with the MNOs, can carry out awareness campaigns towards their customers, in order to warn them about SIM - swapping attacks.

6.3 For the National Authorities:

a) Guidelines for secure authentication:
Customer authentication is at the heart of the SIM swapping process, no matter the channel used (e. g. store, phone, chat bot, mobile application).
Competent authorities could contribute to fulfilling this objective by issuing appropriate guidelines for the MNOs. Specifically, they could recommend putting in place a set of challenges for subscribers initiating a SIM swapping process. This list of mandatory challenges could be different from one MNO to another, but the competent authority could nevertheless consider recommending a basic common set of challenges used in the SIM swapping process

b) SIM swapping process assessment:
The competent national authorities may perform ad - hoc audits to examine the existing SIM swapping processes employed by the MNOs and assess whether they are secure and actually followed by the MNO's employees.
Providing recommendations to enhance specific processes could contribute to the mitigation of the threat.

c) Promoting communication and active collaboration among stakeholders:
Establishing frequent communication between public authorities, MNOs and banks, sharing general information about incidents and discussing fraud prevention measures could all significantly contribute to building up risk mitigation know - how.

Furthermore, launching intuitive public awareness campaigns could contribute greatly to decreasing the threat of attacks occurring and minimizing their impact.

6.4 For the Public

a) Warning signs and recommended steps to minize impact:
The first sign of potentially falling victim to a fraudulent SIM swap is an inexplicable and more than momentary loss of mobile network access.

In this case, subscribers are strongly recommended to contact their MNO without any delay.

Also, subscribers should act fast in case of any unrecognized activity in their social media or email accounts. They should contact their MNO and change their account passwords.

b) Generic self - protection advice:
SIM - swapping fraud usually begins with phishing and/or social engineering against subscribers. To avoid phishing attacks subscribers should take the following precautions.

- Be cautious with the information shared on social media networks.
- Never open any suspicious internet hyperlinks or attachments received through email or messages.
- Avoid providing any personal information by email or by phone when called by someone claiming to be the MNO's representative. A real customer representative will never request personal details such as credit card details or 2FA SMS content. In some cases, MNOs can send an OLTP SMS for finalizing a SIM swap. This OTP password must never be communicated to anyone, even to persons who call the customers and claim to be an MNO's employee.
- Update account passwords on a regular basis.

c) Use better authentication mechanism:
Instead of using Single - Factor Authentication (SFA) method, use better Two - Factor Authentication (2FA). In SFA the user will be provided only one factor – typically, a password or passcode. And in 2FA method user will be provided password as the first factor and a second, different factor – usually either a security token or a biometric factor, such as a fingerprint or facial scan.

Therefore, 2FA adds an additional layer of security to the authentication process by making it harder for attackers to gain access to a person's devices or online accounts because, even if the victim's password is hacked, a password alone is not enough to pass the authentication check.

d) Protect your SIM by changing it to eSIM:
An eSIM (embedded - SIM) is the digital version of a traditional SIM card that can be embedded directly into a device.

- **How eSIM can prevent SIM - swaps:**

To activate eSIM we have to register our self with our details and Personal Identifiable Information (PII). We can also set biometric authentication like face ID or fingerprints to enable multiple layers of security to secure our eSIM account. Additionally, there is no physical SIM card in a eSIM system, so no scammer can claim that their SIM card got lost or damaged as all the identity details will reside in our phone. Thus preventing cyber criminals from acquiring another SIM card or re - registering the number in their name. The Telecom operators Jio, Airtel, and Vodafone - Idea offers eSIM facility for eSIM supported smart phones.

7. Conclusion

SIM Subscriber Identity Module (SIM) swapping is a legitimate procedure performed by a customer to change their mobile SIM card when the SIM card has been lost, damaged or stolen; or when a customer want to upgrade his SIM from 2G/3G SIM to 4G/5G SIM or when a customer want to move to another mobile telecom service provider – which is called number portability. But fraudsters misuse this SIM swap technique to steal legitimate SIM card user's data which is a cyber fraud through a successful social engineering. As a result, the fraudster gain access to the bank accounts and can receive all the SMS and video calls intended for the legitimate subscriber.

To avoid falling into the trap of fraudster's SIM - swap fraud one must be very careful on sharing their personal data. Now maximum number of banking customers have mobile phone numbers linked with their accounts, for online transactions it needs One Time Passwords (OTP), unique registration number etc. which is all provided through registered phone numbers of users. Neither bank employee nor telecom service provider will ask for any OTP or any critical information which leads to online banking fraud. So every user must be careful and cautious while sharing any information. If we get any suspicious calls, SMSes containing malicious links or any mail with malware then one must not attend them, instead report this to cyber security officials.

To save oneself from SIM - swap fraud attack one must use eSIM (Embedded Subscriber Module), better Two - Factor Authentication (2FA) mechanism which provides two layers of security for our social accounts. And never share any personal data to unknown. National authorities must issue appropriate guidelines for the telecom providers to follow proper mechanism to have a secure customer authentication.

Acknowledgment
I would like to gratefully and sincerely thank my parents – father D. Chatur Naik and mother D. Ghammi Bai without whose unsustained support, I could not have completed this paper.

References

[1] https: //www.enisa. europa. eu/publications/enisa - threat - landscape - 2020 - main - incidents.
[2] Frauds in Indian Banking: Aspects, Reasons, Trend - Analysis and Suggestive Measures by Dr. Sukhamaya Swain published in International Journal of Business and Management Invention in July 2016 Vol 5 Issue 7.
[3] Literature review on Cyber Crimes and it's Prevention Mechanisms by Annamalai Lakshmanan.
[4] A Biometrics - based Solution to Combat SIM Swap Fraud by Louis Jordaan.
[5] "NPR Search: NPR". www.npr. org.
[6] Tims, Anna *(2015 - 09 - 26).* 'SIM Swap' gives fraudsters access - all - areas via your mobile phone".
[7] "Many Bengalureans lose cash to sim card swap fraud - Times of India". The Times of India. Retrieved 2018 - 08 - 22.
[8] Franceschi - Bicchierai, Lorenzo (2019 - 05 - 13). "AT&T Contractors and a Verizon Employee Charged With Helping SIM Swapping Criminal Ring". Vice News. Retrieved 2020 - 01 - 23.
[9] Barrett, Brian. "How to Protect Your Phone Against a SIM Swap Attack". Wired – via www.wired. com.
[10] Brandom, Russell (August 31, 2019). "The frighteningly simple technique that hijacked Jack Dorsey's Twitter account". The Verge.
[11] Stempel, Jonathan (7 May 2020). "U. S. cryptocurrency investor sues suburban NYC teen for $71.4 million over alleged swindle". Reuters. Retrieved 4 January 2021.
[12] Nadeau, Barbie Latza (May 8, 2020) "15 - Year - Old From Suburbs Led 'Evil Computer Geniuses' in $24M *Cryptocurrency Heist: Lawsuit" Daily Beast*
[13] Winters, Mike (February 19, 2022). "This SIM card scam once fooled Jack Dorsey—here's how to avoid it". CNBC. *Retrieved February 19, 2022.*
[14] Otis, Ginger Adams (February 18, 2022). "SIM - Swapping Attacks, Many Aimed at Crypto Accounts, Are on the Rise". The Wall Street Journal. Retrieved February 19, 2022.
[15] Depavath Harinath, et. al, "**A Review on Security Issues and Attacks in Distributed Systems**, " Journal of Advances in Information Technology (JAIT), Vol.8, No.1, pp.1 - 9, February, 2017. doi: 10.12720/jait.8.1.1 - 9

Author Profile

Depavath Harinath, received Master of Computer Applications degree from Sreenidhi Institute of Science and Technology, an autonomous institution approved by UGC, Accredited by NAAC with 'A' grade and accredited by NBA, AICTE, New Delhi – permanently affiliated to JNTU, Ghatkesar, Ranga Reddy, Hyderabad, Telangana, India. Having more than eight years of experience in teaching and already published 17 manuscripts in different international journals. Research field includes Computer Networks, Network Security and Artificial Intelligence.