Ghost SIM Attack
How to take advantage of weak authentication policies in 2G, 3G, 4G and 5G mobile networks

Pedro Cabrera
Ethon Shield
pedro.cabrera@ethonshield.com

Miguel Gallego
Ethon Shield
miguel.gallego@ethonshield.com

Javier Valero
Ethon Shield
javier.valero@ethonshield.com

Abstract – The authentication policy of a mobile operator dictates the frequency and conditions under which an authentication procedure is triggered on the subscriber following a set number of events. A lax or insufficiently robust authentication policy may allow an attacker to perform the Ghost SIM Attack, attack that takes advantage of weak authentication policies by extracting essential SIM card information to perform fraud. This paper presents a comprehensive overview of the experimental setup and methodology utilized to execute the Ghost SIM Attack, along with an in-depth analysis of the authentication policies implemented by various operators and technologies across multiple countries around the world. The results reveal that the Ghost SIM Attack is successful across all the selected technologies and operators highlighting the weak authentication policies configured. Finally, some countermeasures are proposed for the attack while also addressing its limitations.

Keywords: ***Ghost SIM, 5G, SIM, AKA, elementary files, authentication policy, AT commands, 3GPP***

1. Introduction

The objective of this research was to analyze the potential for fraud in mobile networks due to a lack of a robust configuration in the authentication policies. To achieve this, the Ghost SIM Attack was developed, a method in which an attacker obtains the necessary information from a victim's SIM card to perform fraudulent activities.

This paper is organized into several sections. The background section provides an overview of essential concepts required to understand the attack. It will be shortly discussed how SIM cards store information, what is the purpose of an authentication procedure and what is meant by "authentication policy".

Subsequently, the specifics of the Ghost SIM attack are going to be depicted. This section outlines the necessary steps to execute the attack, including the methods used to obtain the victim's SIM card information and programming the fraudulent card. It will include the tools and techniques employed to perform the attack and the underlying technical details.

The experimental setup and methodology will also be described, as the attack was conducted in various countries. This section will detail the selection of locations for testing. By conducting the attack in diverse environments, the research aims to provide a comprehensive understanding of its feasibility and the varying degrees of vulnerability across different mobile networks.

The results of the attack and the analysis of authentication policies will be presented to assess the potential impact of the attack. This will include the quantitative data on the success rate of the attack and the types of network technologies most susceptible to exploitation. It will also be discussed the specific circumstances under which the attack can be executed, including its limitations.

Finally, some countermeasures will be proposed, concluding with recommendations to mitigate the risk of similar fraudulent attacks in the future. By addressing these vulnerabilities, the research aims to contribute to the development of more secure mobile communication systems and protect users from the growing threat of fraud.

2. Related Work

In 1997, much of the code for the first version of the COMP128 algorithm was leaked, allowing it to be analyzed

and leading to the demonstration in April 1998 of a vulnerability that made it possible to obtain the Ki of SIM cards in about 8 hours. Obviously, physical access to the SIM card was required to carry out the attack. [1][2]

SIM card swapping is a type of fraud where an attacker impersonates a victim and asks the network operator to transfer the victim's phone into a new SIM card. Once the attacker controls the victim's phone number, he will be able to send and receive fraudulent calls and text messages, including two factor authentication codes. There is an innumerous amount of literature on SIM swapping attacks. Furthermore, SIM swapping, although having the same outcome as the Ghost SIM attack, is mainly focused on social engineering and deception. According to a study conducted by the FBI, losses caused by SIM swap attacks in 2024 reached $26 million in 982 incidents recorded in the study [3].

In 2015, a collaborative research [4] demonstrated a side channel attack/differential power analysis vulnerability that allowed the Ki of 3G and 4G SIM cards to be obtained in less than two hours, using an oscilloscope to monitor the power consumption of the original SIM while the card evaluated authentication requests.

All these investigations illustrate how SIM cards have been susceptible to numerous forms of attacks since the early days of mobile networks. From cryptographic vulnerabilities in early authentication algorithms to modern side-channel attacks and socially engineering SIM swapping, these threats highlight the evolving attack surface of SIM technology.

3. Background

In this section, the detail of the necessary knowledge needed to understand the attack will be presented.

3.1. SIM cards

SIM cards are integrated circuits that enable a subscriber to securely register to a mobile network and perform the necessary actions to protect against any attacks on the identity or privacy. To ensure secure network access and maintain a baseline level of security, SIM cards store essential information, including the IMSI, location data, and the authentication keys used to encrypt the air interface.

This information is stored in the so-called elementary files or EFs [5]. Each EF is designed to hold specific data, ensuring that the SIM card can efficiently manage and protect the subscriber's credentials and operational parameters. One of the initial steps in the Ghost SIM Attack is to access these elementary files and obtain the information required to perform fraud.

3.2. AKA procedure

The AKA is a security protocol used in mobile networks which pursues two objectives. The first one is the authentication between two entities; in the context of mobile networks, ensuring that both the network and the client are who they claim to be. The second, key agreement, referring to the computation of the necessary keys for encryption between these two entities. The details on how the AKA procedure works can be found in [6][7].

After every successful AKA procedure, the user equipment will have generated new ciphering and integrity keys. These keys are used to encrypt the air interface between the user equipment and the radio node and are derived from the secret key Ki. However, it is important to highlight that the Ki is not stored in an accessible part of the memory of the SIM card, preventing the user from retrieving this fundamental key.

3.3. Authentication Policy

To prevent a potential increase in signaling message load within the core network, the mobile operator determines a policy for the number of authentication procedures initiated on the subscriber, known as the authentication policy.

This authentication policy is typically structured around time-based or event-based criteria. In a time-based approach, subscribers are authenticated after a predetermined duration, while an event-based strategy triggers authentication procedures following a specific number of predefined events.

The events that trigger an authentication procedure are operator dependent, but generally include calls, registration requests, mobility updates or SMS. Additionally, other factors that may prompt an authentication procedure include changes in network conditions, subscriber behavior such as mobility, and other security considerations. As an example, an authentication

procedure could be triggered after N number of "*Tracking Area Updates*" from the subscriber.

Part of the investigation for the attack includes an in-depth analysis of the authentication policy of the different mobile networks across multiple technologies. This analysis is essential because understanding the policy in different scenarios and networks can significantly influence the impact of the Ghost SIM Attack.

4. Ghost SIM Attack

The idea behind the attack is the following: the SIM card stores critical data. By extracting this data, without needing the Ki, and copying it to a fraudulent SIM card, the attacker can enable the fraudulent SIM to possess all the necessary information to successfully connect to the mobile network, provided that the network does not trigger an authentication procedure. If an authentication procedure is started, the fraudulent SIM card will not have the Ki, essential for generating the challenge-response exchanges with the network and will not be able to successfully complete the authentication procedure.

There are several steps needed to successfully perform this attack.

- The first and foremost requirement is to have physical access to the victim's phone, as this access enables the attacker to interact directly with the device and its SIM card.
- Once the victim's phone is accessible, the SIM card information will be obtained.
- This information is copied into a programmable SIM card, which will be used for fraud.
- The programmable SIM card will be inserted into a mobile device that will try to connect to the network.

The fraud will work if there is a weak authentication policy, and the network does not perform any authentication procedures on the fraudulent SIM card.

The following sections will provide a detailed breakdown of each step involved in the Ghost SIM attack, highlighting the techniques employed in each of them.

4.1. Prerequisites and limitations

The first prerequisite for the attack to be successful is to have physical access to the targeted phone. Therefore, being in the victim's location or at least having the victim's mobile device is a condition for a hypothetical attacker to proceed.

If this condition is met, the next step of the procedure would be to extract certain information stored in the SIM card. Three different methods have been identified:

- Method 1: Extract the SIM card from the phone, plug it in a SIM card reader and use it to obtain necessary information; referenced in Figure 1.

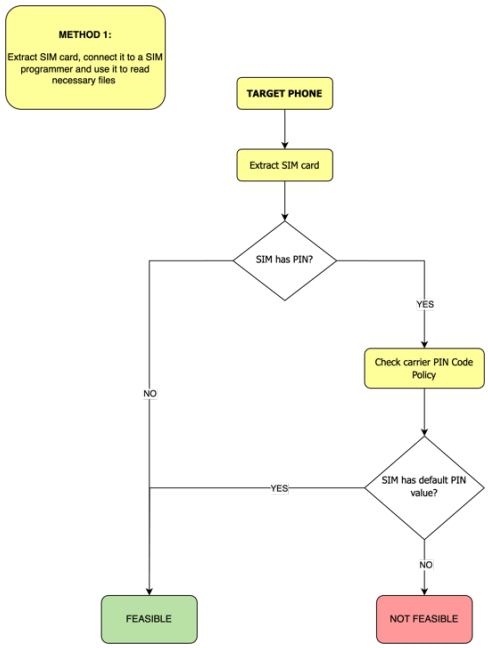

Figure 1- Illustrative schematic of first method employed to extract SIM card info

- Method 2: Interact with the phone's modem via *adb* shell by sending 3GPP AT commands to read necessary files from the SIM card; referenced in Figure 2.

- Method 3: Interact with the phone's USB ACM interface by sending 3GPP AT commands to read necessary files from the SIM card; referenced in Figure 3.

The first scenario requires the SIM card to have no PIN code configured or to use a default code that the attacker might know.

In Europe it is common that SIM cards are shipped with a custom PIN number that must be unlocked every time the phone is powered on or if the SIM card is inserted. However, in other countries, is it likely that SIM card, specially prepaid ones, are sold with default PIN codes or with no PIN code all, leaving the responsibility of its configuration to the end user. For instance, several US

operators typically use '1111' as the default PIN [8], meanwhile the SIM cards of an operator from the UK are shipped with the PIN feature turned off by default [9].

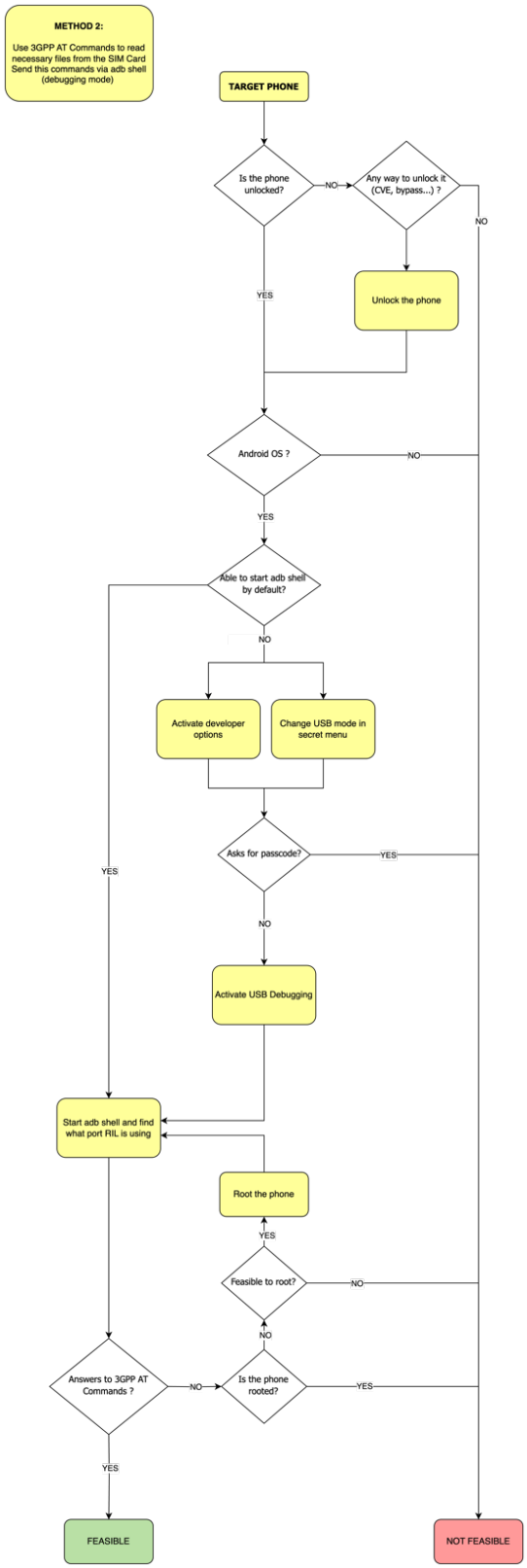

Figure 2 Illustrative schematic of second method employed to extract SIM card info (Serial commands over Android Debug Bridge)

For the two remaining scenarios it is assumed that the SIM card is protected by a PIN code only known by the legitimate user but has been unlocked as it is connected to the legitimate network. Furthermore, it is required that the device is unlocked during the attack procedure. The referred methods have only been tested over Android devices, so this would be considered as an additional limitation of the attack.

The second scenario requires a user to send 3GPP AT Commands directly to the phone's modem while executing an android debugging shell. Depending on the model and manufacturer, this action might require root privileges for the user. This have been proven the case for most recent tested models, but previous studies show that it is possible for a non-privilege user to send AT Commands to the modem in older Samsung devices [10].

The third scenario requires that the phone exposes USB ACM interface when connected via USB cable to another device (frequently shown as a mapped *tty* device). Some devices expose this functionality by default, but for others it might be necessary to set a specific type of USB configuration, as explained in [8].

In addition, both second and third scenarios assume that 3GPP AT commands are available for execution on the target phone. However, in recent years, mobile devices have typically come with 3GPP AT commands disabled by default, which means that, even if a user is able to send AT commands, there will be no response to the specific set of commands needed to perform this attack.

A tested solution to this limitation is to activate a specific toggle in the developer options menu which allows the use of 3GPP AT command and is, presumably, available for Android 10 and newer versions. Nevertheless, two possible difficulties arise: first, since Android 4.2, developer options menu is hidden by default [9], and since Android 8 its activation requires to know the device's passcode [10], which would be an impediment for the attack; second, in many recent devices the activation of the mentioned toggle option triggers a phone restart, which, if the SIM is protected by a PIN code, would again make the attack unfeasible.

Consequently, due to the many detected dependencies on device model and manufacturer, this attack has been tested on multiple mobile devices, trying to have a sample of different vendors and estimate the feasibility of the attack

for methods two and three. Nevertheless, the first method is likely to be the most realistic way to perform the attack, based on the information collected.

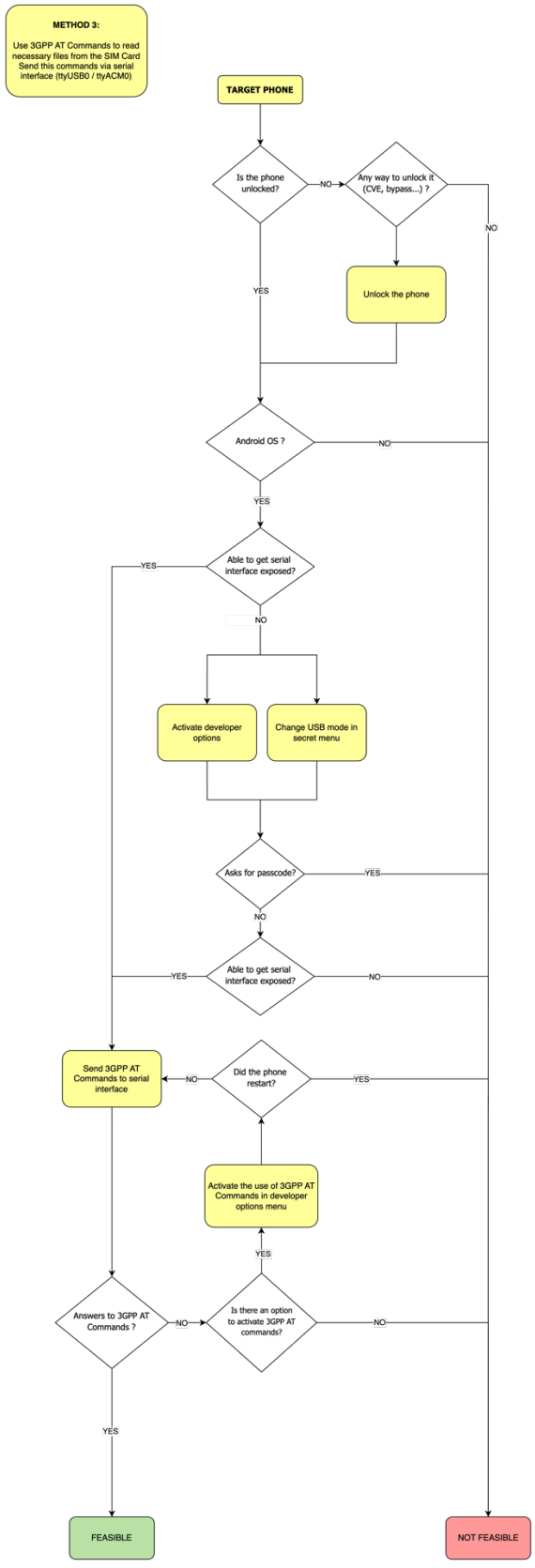

Figure 3- Illustrative schematic of third method employed to extract SIM card info (Serial commands on exposed USB devices)

It is also important to note that the heterogeneity of the Android ecosystem has contributed to a wide range of security vulnerabilities, such as screen lock bypasses [11] [12] [13] [14], insecure USB debugging configurations [15] [16], undocumented AT commands [17] and inconsistent implementation of security patches across devices [18]. Although these issues were not the primary focus of this research, they can significantly weaken the overall device security posture, making it considerably easier for an attacker to exploit methods two and three.

4.2. Obtaining SIM card info

The Ghost SIM attack has been developed to obtain the minimum required data to successfully perform the attack, drastically minimizing the time the attacker must be close to the victim's device.

Additionally, it is important to consider that for each technology, different elementary files must be accessed. This necessity arises from the introduction of new elementary files throughout the evolution of the different generations.

A clear example is 5G, where a whole new dedicated file has been created, the DF.5GS [5]. Inside this DF, there are new elementary files that contain location information or authentication and encryption keys.

4.3. Programmable SIM card

Once the information from the SIM card has been obtained, this data is copied into a programmable SIM card which then can be inserted into a mobile device. If the authentication policy is weak, this programmable SIM card will be able to connect to the mobile network, and depending on several factors addressed further on in this paper, it will be able to send and receive SMS, establish and receive calls and have mobile data connectivity.

5. Experimental setup

To extract the SIM card info in methods two and three it is necessary to establish a physical connection with the victim's mobile device, using in this case a standard USB cable. For method three, once the connection was successfully made and the *tty* device was mapped, AT commands were sent to retrieve information from the SIM

card. These commands were sent using shell scripting. For method three, once connected to the adb shell and

After acquiring all the necessary data, a SIM card reader and open-source software (*pySim-shell* tool [19]) was employed to program a programmable SIM card from sysmocom [20]. Finally, this programmable SIM card was inserted into a mobile device. The fraudulent mobile device was also connected to the computer to analyze the traffic and understand all the mobile network procedures taking place, using the open-source software *scat* [21].

Taking advantage of the fact that the attack does not require special computational resources or specialized hardware, a miniaturized version of the attack was implemented on a low-cost ARM single-board computer (SBC). A Raspberry Pi 3 was selected, equipped with a small display to present the progress and outcome of the attack. The ARM board was powered by a compact 5 V battery chosen for its small size, and a programmable SIM card reader/writer was connected to the rear of the board in order to keep the entire setup compact.

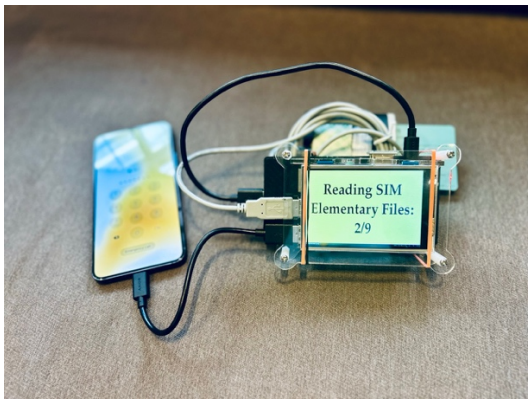

Figure 4Full miniaturized kit, Raspi3 SBC with display, battery, and SIM card programmer

This implementation is not the smallest possible; other boards of this class could likewise be adapted to carry out the attack, substantially reducing the overall size and thereby rendering the device even more discreet. Because the attack requires proximity to the victim's mobile device, the ability to minimize and conceal the implementing device is important to avoid detection.

Table 1 provides a summary of the devices tested during the extraction of SIM card information.

	Samsung A52s 5G	Samsung Galaxy S21	Samsung Galaxy S22	Samsung A25 5G	LG Nexus 5X
Android version	13	12	15	14	7
Method two exploitation Interact with the phone's modem via **adb shell** by sending 3GPP AT commands	NO	NO	NO	NO	YES
Method three exploitation Interact with the phone's USB **ACM interface** by sending 3GPP AT commands	YES	YES	YES	YES	YES

Table 1: Android based mobile devices tested

This research did not aim to evaluate a wide range of Android-based devices, but rather to assess the impact of the Ghost SIM attack across multiple mobile operators in different countries. While device diversity can introduce additional variables in terms of security posture, this study prioritized the network-side behavior to gain insights into how operator configuration may contribute to or mitigate attack success.

6. Methodology

To analyze the outcome of the attack in different mobile network operators, SIM cards were purchased in official stores on the street. Once the SIM card activation was verified, the battery of tests programmed to check the success rate of the Ghost SIM Attack could start.

The following procedure was implemented for each technology and operator:

- Connect the victim's mobile device with the legitimate SIM card to the appropriate technology (2G, 3G, 4G, 5G).
- Generate random traffic in both CS and PS by activating and deactivating airplane mode and browsing the Internet.
- Connect the mobile device to a computer using a USB cable.
- Extract the SIM card information for the corresponding technology by executing a proof of concept developed in shell scripting language.
- Program the programmable SIM card with the extracted data.
- Insert the fraudulent SIM card into a different mobile device, previously configured to connect to the corresponding technology. This configuration can be determined in the mobile networks menu inside settings where there are multiple options to choose from: "2G only", "3G only", "3G and 2G", "4G, 3G, 2G" and "5G, 4G, 3G, 2G".
- Perform subscribers' regular actions such as accessing the internet, sending and receiving SMS messages, and making and receiving calls, while obtaining the control plane traces using the debugging tool scat [12].

- Analyze, compute and document the results.

This methodology provides a systematic approach to evaluating the effectiveness of the Ghost SIM Attack across various mobile network operators and technologies.

7. Authentication Policy Analysis

To be able to determine the impact of the Ghost SIM attack, it is crucial to understand the authentication policy of the network operator. The reason for this is the following: if the authentication policy of an operator is weak and the Ghost SIM Attack succeeds, the exploitable period increases, meaning the attacker will have more time to impersonate the victim. For instance, if the authentication policy of an operator is time-based, and authenticates the user every 24 hours, the impact will be higher compared to another operator that authenticates the user every 30 minutes. The time available for the attacker to interact with the mobile network (calls, SMS, internet access, and more) is considerably reduced in the latter, minimizing the impact.

To analyze the authentication policies of different operators and in all available technologies, methodological tests were performed. The objective of these tests was to understand if the authentication policy of the studied mobile network was time-based or event-based. If it was event-based, understand which events, messages or subscriber behavior triggered an authentication procedure.

These tests differed between technologies as 2G and 3G have both circuit switched and packet switched networks, whereas 4G and 5G technologies only have packet switched networks.

Although the operators were carefully selected so that they were 5G SA capable networks, in some of the studied countries only prepaid SIM cards could be bought due to legal regulations. Unfortunately, most prepaid SIM cards are restricted to PS networks and do not have 5G SA capabilities.

Furthermore, not all operators supported all technologies, as many are in the process of phasing out older ones like 3G. Among the technologies analysed, 4G was the most widely supported, and the authentication policy could be studied in eight different operators. In contrast, only three operators could be analysed for 3G.

7.1. Authentication Policy Results

The tests across all technologies followed a similar approach: generating events such as network registrations, SMS, or voice calls, and observing how many authentication requests were triggered by the network. For example, Table 2 presents the analysis of the 2G authentication policy using four main tests. The first involved sending "*Location Updating Requests*" in the circuit-switched domain; the second involved sending an SMS to another mobile device; the third consisted of making a phone call to another device; and the fourth involved sending "*Attach Requests*" in the packet-switched domain.

For example, in Table 2 in the network registration test, Operator #5 performed 20 successful registration attempts, of which 15 triggered subscriber authentications, indicating a relatively robust authentication policy for this type of event.

The analysis of the authentication policies across all technologies and multiple network operators shows a generalized weak authentication policy.

The only exceptions found have been in the PS domain in both 2G and 3G technologies, where in some operators the subscriber is authenticated at each "*Attach Request*", preventing the success of the Ghost SIM Attack in this domain.

2G Authentication Policy					
Event	Operator				
	[Spain] Operator #1	[Spain] Operator #2	[Netherlands] Operator #3	[Germany] Operator #5	[Germany] Operator #6
Location Update Request (CS)	20	20	20	20	20
Authentication Request	1	1	2	15	13
SMS	20	20	-	14	23
Authentication Request	1	2	-	1	17
Phone call	20	20	-	14	9
Authentication Request	2	1	-	2	1
Attach Request (PS)	20	20	20	19	21
Authentication Request	20	20	20	15	20

Table 2- Details of the authentication policy of the operators analyzed in 2G/GSM radio technology

3G Authentication Policy			
Event	Operator		
	[Spain] Operator #1	[Spain] Operator #2	[Netherlands] Operator #4
Location Update Request (CS)	20	20	20
Authentication Request	1	2	20
SMS	20	20	20
Authentication Request	2	1	6
Phone call	20	20	20
Authentication Request	2	2	7
Attach Request (PS)	20	20	20
Authentication Request	20	1	19

Table 3- Details of the authentication policy of the operators analyzed in 3G/UMTS radio technology

4G Authentication Policy				
Event	Operator			
	[Spain] Operator #1	[Spain] Operator #2	[Netherlands] Operator #3	[Netherlands] Operator #4
Attach Request	20	20	20	20
Authentication Request	3	1	2	0
Authentication Request	1	0	-	-
SMS	20	20	-	-

4G Authentication Policy				
Event	Operator			
	[Germany] Operator #5	[Germany] Operator #6	[Singapore] Operator #7	[Singapore] Operator #8
Attach Request	20	20	21	21
Authentication Request	4	0	1	3
Authentication Request	4	5	0	0
SMS	20	21	20	20

Table 4- Details of the authentication policy of the operators analyzed in 4G/LTE radio technology

5G Authentication Policy		
Event	Operator	
	[Spain] Operator #1	[Spain] Operator #2
Registration Request	20	21
Authentication Request	1	1
Authentication Request	-	1
SMS over NAS	-	20

Table 5- Details of the authentication policy of the operators analyzed in 5G/NR radio technology

8. Results

Once the prerequisites are fulfilled, the Ghost SIM Attack is successful across all technologies in all network operators. The results have been obtained from operators all over the world, choosing the most representative ones from European, Asian and North American countries.

	2G		3G		4G	5G
	CS	PS	CS	PS	PS	PS
[Spain] Operator #1	Vulnerable	Not Vulnerable	Vulnerable	Not Vulnerable	Vulnerable	Vulnerable
[Spain] Operator #2	Vulnerable	Not Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable
[Netherlands] Operator #3	Vulnerable	Not Vulnerable	NA	NA	Vulnerable	NA
[Netherlands] Operator #4	Vulnerable	Not Vulnerable	NA	NA	Vulnerable	NA
[Germany] Operator #5	Not Vulnerable	Not Vulnerable	NA	NA	Vulnerable	NA
[Singapore] Operator #7	NA	NA	NA	NA	Vulnerable	NA
[Singapore] Operator #8	NA	NA	NA	NA	Vulnerable	NA

Table 6- Summary table of the global results obtained in the 9 operators worldwide.

In multiple operators, the PS network in 2G and 3G technologies had a robust authentication policy, authenticating the user in every "*Attach Request*", making these operators not vulnerable to the Ghost SIM Attack.

It is highly relevant that in the most recent mobile technologies (4G and 5G SA), where one would expect to find a more robust authentication policy configuration, the highest probability of success for the Ghost SIM attack has been observed, regardless of the country or the operator.

Even if the results obtained in 5G SA are not considered—considering that testing could only be carried out in one country (Spain)—the probability of attack success observed in 4G technology across all countries remains significant.

2G and 3G networks may exhibit weak configurations due to their age. The global trend of phasing out these technologies could also explain why their security configurations have not been updated. However, it was in 3G technology where the most robust authentication policies were found, completely preventing the attack in the packet domain.

If the Ghost SIM Attack is successful in multiple technologies, it will result in the following consequences:

- The attacker will be able to establish and receive calls.
- The attacker will be able to send and receive SMS (including 2FA).
- The attacker will be able to use the victim IP address on the internet.

9. Countermeasures

There are several countermeasures that both users and mobile operators can implement to reduce the success rate of the Ghost SIM Attack.

By the user:

- Users should always configure a PIN for their SIM card to protect their mobile device.
- It is essential to set a strong PIN code that locks the device and to avoid leaving the phone unprotected at any time.
- Never leave the phone unattended, as attackers could use this time to interact with the SIM card.
- Have 3GPP AT commands deactivated (default behavior)
- Have USB debugging deactivated (default behavior)
- Always have the latest software version in the mobile device

By the mobile operator:

Mobile operators should have a robust authentication policy that will prevent a successful Ghost SIM Attack. The strength of these policies can vary significantly between operators and is often influenced by regional or national practices. Factors affecting this robustness include the capabilities provided by network equipment

manufacturers and specific design choices within the mobile network—such as the expected traffic volume handled by nodes responsible for generating authentication vectors, mobility configurations, and control plane traffic between core network nodes.

It is recommended to implement a viable fine-tuning of parameters (without causing traffic overprovisioning) while simultaneously ensuring that conditions which would allow a potential attacker to obtain benefits from the network without being authenticated are avoided. The following are examples of actions that could form part of a fine-tuning plan; the list is not exhaustive:

- Mandatory authentication of initial connections and initial registrations in both the circuit-switched and packet-switched domains.
- Review of periodic counters to avoid authentication-free windows longer than one hour.
- Review of event-based "1-in-n" counters, with the objective of grouping distinct events so as to increase the frequency of authentication.

10. Future work

To improve the success rate of the attack, reducing the limitations is a must.

Furthermore, this attack has only been tested on physical SIM cards. However, the growing adoption of eSIMs presents an interesting opportunity for future research. Investigating how the Ghost SIM Attack might be adapted to target eSIM technology could provide valuable insights.

Additionally, tested has been limited to Android devices. Extending the approach to iOS would broaden the scope of the study and potentially increase the number of affected targets.

Finally, as 2G and 3G networks are gradually being shut down, voice calls and SMS will increasingly rely on VoIP technologies. Modern SIM cards include a dedicated application that supports IMS registration, which is required for these services [22]. Consequently, it would be interesting to research whether it's possible to successfully register the Ghost SIM with VoLTE and VoNR capabilities.

11. Conclusion

The authentication policy of a mobile operator is a key feature in enhancing security and, when properly configured, can significantly mitigate fraudulent activities.

This research has revealed that most mobile operators lack a robust authentication policy, as evidenced by the successful execution of the Ghost SIM Attack across all examined networks. It is noteworthy to mention that, generally, in 2G and 3G PS networks, the authentication policy is very robust, authenticating all "*Attach Request*" messages.

However, it is essential to acknowledge the limitations of this attack, particularly the requirement for physical access to the victim's mobile device, which must be unlocked. This requirement inherently reduces the likelihood of a successful attack.

While strengthening authentication procedures can diminish the impact of such attacks, SIM swapping scams remain a concern, primarily due to the lack of verification when requesting a new SIM card.

12. Acronyms

2FA	Two-factor authentication
3GPP	3rd Generation Partnership Project
5G SA	5G Standalone
ACM	Abstract Control Model
ADB	Android Debugging Bridge
AKA	Authentication and Key Agreement
AT	ATention
CS	Circuit Switched
DF	Dedicated File
EF	Elementary File
eSIM	Embedded SIM
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
Ki	Subscriber Authentication Key/Long Term Key
LTE	Long Term Evolution
NR	New Radio
PIN	Personal Identification Number
PS	Packet Switched
SIM	Subscriber Identity Module
SMS	Short Message Service
USB	Universal Serial Bus
VoIP	Voice over IP
VoLTE	Voice over LTE
VoNR	Voice over NR

13. References

[1] B. Brumley, "A3/A8 & COMP128," T-79.514 Special Course on Cryptology, [Online]. Available: http://www.tcs.hut.fi/Studies/T-79.514/slides/S5.Brumley-comp128.pdf.

[2] G. MoU, "GSM MoU Association Responds to Recent Claims of Compromise to GSM Security," 15 April 1998. [Online]. Available: http://www.isaac.cs.berkeley.edu/isaac/wow.html#1423.

[3] FBI, "Internet Crime Report 2024," [Online]. Available: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

[4] F.-X. S. Z. G. D. G. S. W. Y. G. X. X. Junrong Liu, "Cloning 3G/4G SIM Cards with a PC and an Oscilloscope: Lessons Learned in Physical Security," 2015. [Online]. Available: https://www.blackhat.com/docs/us-15/materials/us-15-Yu-Cloning-3G-4G-SIM-Cards-With-A-PC-And-An-Oscilloscope-Lessons-Learned-In-Physical-Security.pdf.

[5] ETSI, *Universal Mobile Telecommunications System (UMTS); LTE; 5G; Characteristics of the Universal Subscriber Identity Module (USIM) application v18.4.0,* 3GPP, 2024.

[6] P. K. Nakarmi, "Cheatsheets for Authentication and Key Agreements in 2G, 3G, 4G and 5G," 2021.

[7] M. G. Pedro Cabrera, *SUCI Probing in the Wild,* 2024.

[8] M. Kreitzman, 23 August 2025. [Online]. Available: https://www.efani.com/blog/how-to-set-up-sim-card-lock-on-android-iphone.

[9] [Online]. Available: https://www.bt.com/help/mobile/how-do-i-get-a-pin-or-a-puk-code-for-my-mobile-phone-.

[10] D. (. T. a. G. H. a. J. I. C. a. V. F. a. C. R. a. P. T. a. H. V. a. L. H. a. A. R. a. M. G. a. K. R. B. Butler, "{ATtention} Spanned: Comprehensive Vulnerability Analysis of {AT} Commands Within the Android Ecosystem," in *27th USENIX Security Symposium (USENIX Security 18)*, Baltimore, MD, 2018, pp. 273-290.

[11] NIST, "CVE-2025-26428," 04 09 2025. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2025-26428.

[12] NIST, "CVE-2025-26421," 04 09 2025. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2025-26421.

[13] NIST, "CVE-2025-22434," 02 09 2025. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2025-22434.

[14] NIST, "CVE-2025-0077," 04 09 2025. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2025-0077.

[15] NIST, "CVE-2023-43488," 25 10 2023. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2023-43488.

[16] NIST, "CVE-2019-16273," 06 01 2019. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-16273.

[17] NIST, "CVE-2025-26412," 11 06 2025. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2025-26412.

[18] Android, "Android Enterprise Customer Community," 18 04 2024. [Online]. Available: https://www.androidenterprise.community/discussions/conversations/system-updates-behaving-differently-on-pixel-and-samsung-devices-/3567.

[19] "pysim," [Online]. Available: https://github.com/osmocom/pysim.

[20] s. -. s. f. m. c. GmbH. [Online]. Available: https://sysmocom.de/.

[21] "SCAT: Signaling Collection and Analysis Tool," [Online]. Available: https://github.com/fgsect/scat.

[22] ETSI, *Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Characteristics of the IP Multimedia Services Identity Module (ISIM) application v17.0.0,* 3GPP, 2022-05.

[23] I. a. C. F. a. H. S. R. a. C. O. a. B. E. Karim, "Opening Pandora's box through ATFuzzer: dynamic analysis of AT interface for Android smartphones," p. 529–543, 2019.

[24] [Online]. Available: https://developer.android.com/studio/debug/dev-options.

[25] R. Gao, 2 June 2017. [Online]. Available: https://www.androidpolice.com/2017/06/01/android-o-feature-spotlight-enabling-developer-options-requires-devices-passcode.