SECTOR
BRIEFINGS
October 1-2, 2025
METRO TORONTO CONVENTION CENTRE

Ghost SIM attack

Hacking mobile network authentication policies

Ghost SIM attack

The Ghost SIM attack extracts essential SIM card information to take advantage of weak authentication policies to perform fraud in 2G, 3G, 4G and 5G mobile networks.

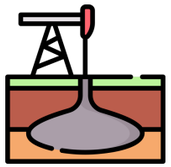
To be able to understand the previous statement, the following questions need to be answered

What is a SIM card and how does it store information? How do we extract this information?

What is an authentication policy? What do we mean by “weak”?

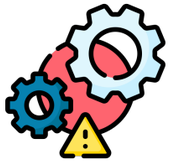
How and why is this attack capable of performing fraud in the mobile network?

Outline



Extracting Information

- SIM cards hacking
- Mobile Phones
- Android security features



Inefficient policies

- Mobile Networks

And the fraud was committed

- Making the Ghost

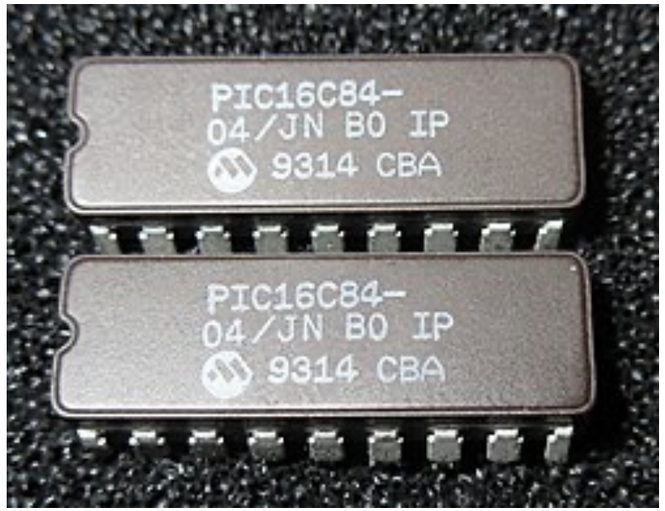
Results

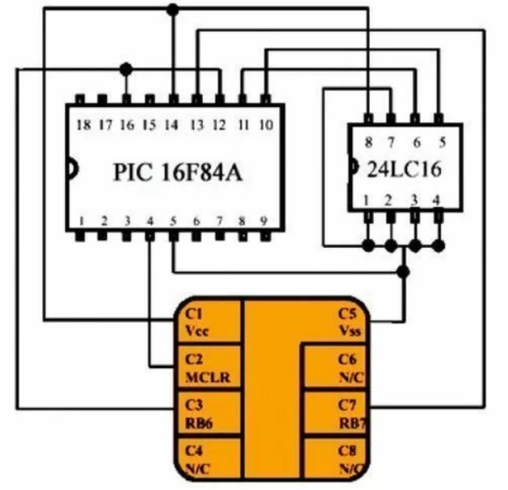
Recommendations & Remediation

Take aways

SIM cards 101 hacking

Between 1993 and 1998, the PIC16C84 (SMD implementation with EEPROM: “GoldWafer”) and PIC16F876 (SMD implementation : “Silver card”) microcontrollers became very well known.





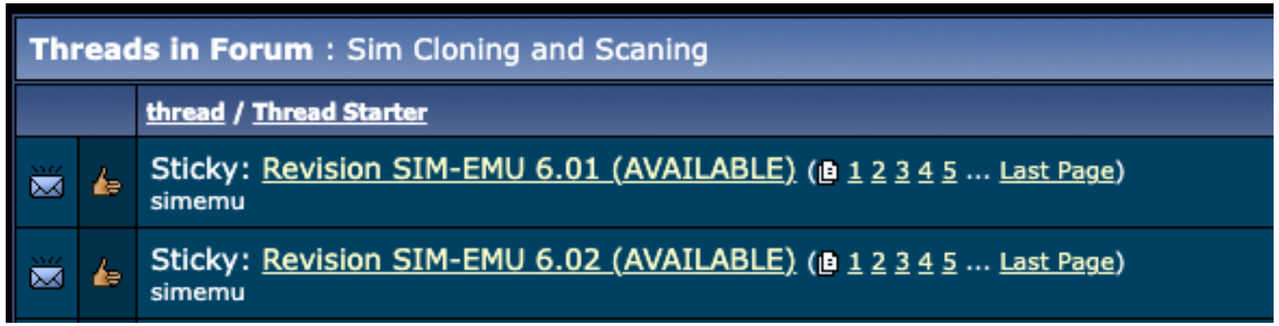
This family of microcontrollers became very popular in the context of hacking Pay-TV satellite platforms.

SIM cards 101 hacking

Soon, a SIM card emulator using the same microcontroller emerged: **SIM-EMU**

In those years, operators used an insecure version of a very important algorithm, which allowed SIM cards to be cloned in an attack that lasted 8 hours.

To clone a SIM card, physical access to it was required in order to insert it into a Smartcard reader, along with software that implemented the attack on the COMP128 (v1) algorithm.



SOURCE: https://forum.gsmhosting.com/

GSM MoU Association Responds to Recent Claims of Compromise to GSM Security

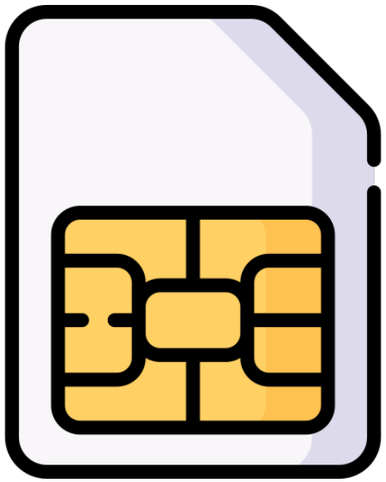
DUBLIN, Ireland, April 15, 1998 -- The GSM MoU Association, which represents the world's GSM network operators, regulators and administrative bodies from 109 countries/areas of the world, has received reports from the U.S. which claim that the security provided by the GSM SIM card may have been compromised.

The recent, unsubstantiated, reports concern the mathematical code (A3) used to provide authentication within the GSM smartcard.

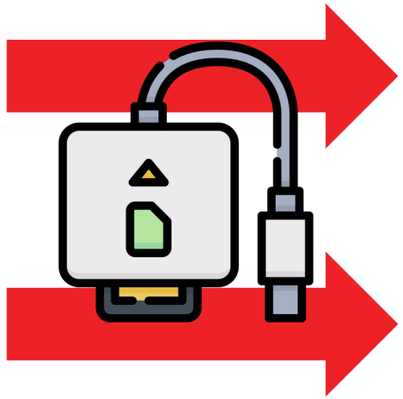
SOURCE: http://www.isaac.cs.berkeley.edu/isaac/wow.html#1423

SIM cards 101 hacking

What is SIM card cloning?

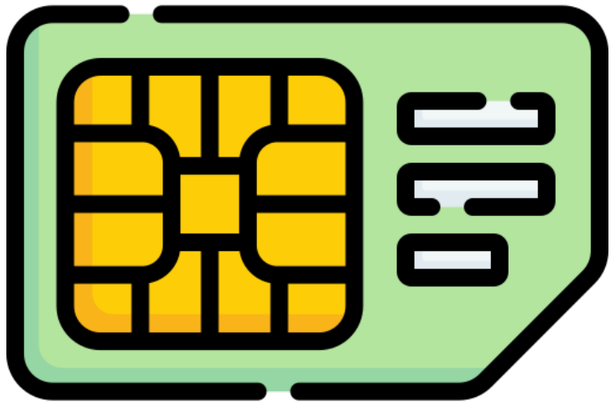


Original SIM



IMSI (Identity)

Ki (Secret Key)

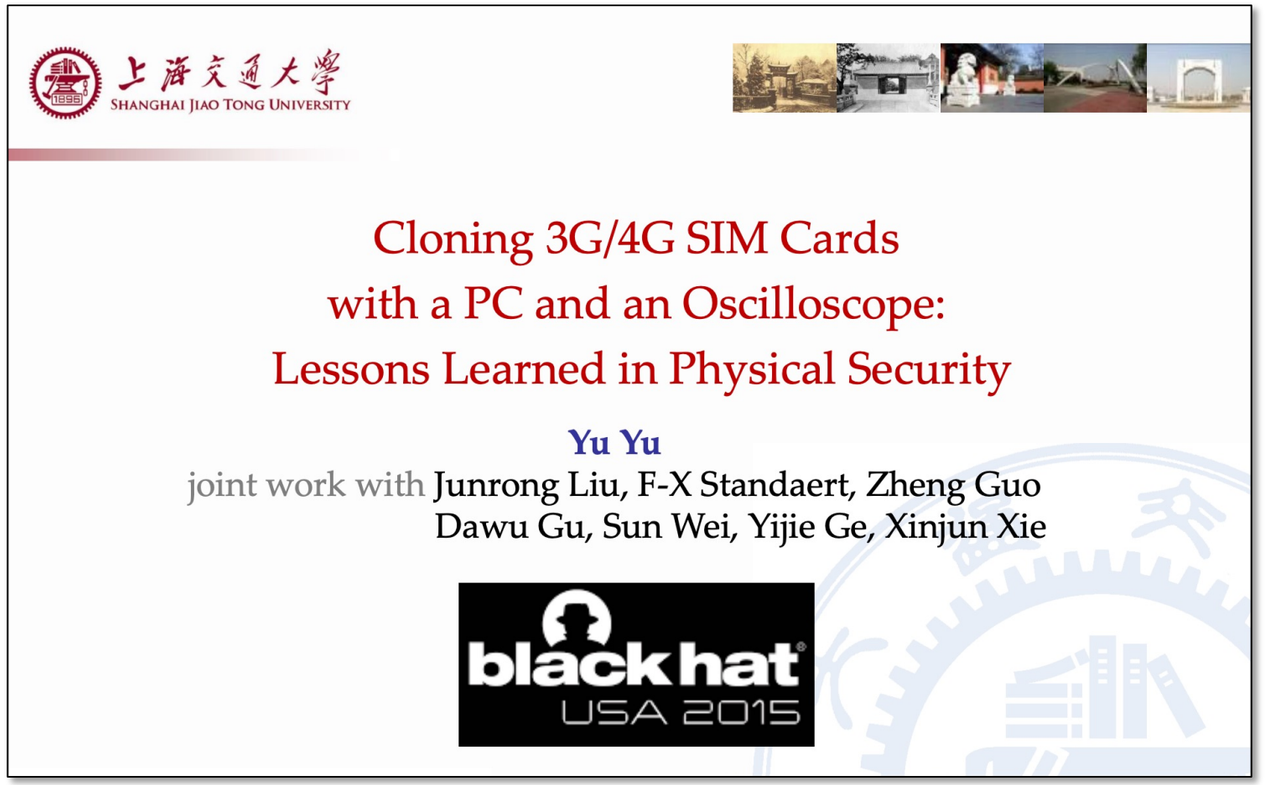


Programmable SIM

Only two very important parameters need to be read in order to copy them to a programmable card.

SIM cards 101 hacking

In 2015, a side channel attack vulnerability was discovered that allowed 3G and 4G SIM cards to be cloned using an oscilloscope.



SOURCE: 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

SIM Swaping fraud

In several countries, operators allowed numbers to be transferred from one SIM card to another (known as SIM replacement), originally intended as a service for customers who had lost their cell phones.

Criminals began to exploit this process as a form of fraud in which the attacker gets the victim's operator to transfer their phone number to a SIM card under their control (SIM swap).

Period	Key Milestone	Notable Countries
2007 – 2010	First cases of SIM duplication fraud	South Africa, Brazil
2011 – 2013	Large-scale incidents, start of SIM hijacking	U.S., Mexico, Spain
2014 – 2016	Term **"SIM swap fraud"** becomes popular	U.S., U.K.
2017 – 2019	Surge in cases due to cryptocurrency boom	U.S., Europe, LATAM
2020 – 2025	Global rise; stricter regulations introduced	Worldwide

Police warning after £250k sim-swap fraud

9 August 2025

Share Save

Stewart Whittingham BBC News, Manchester

SOURCE: *https://www.bbc.com/news/articles/cnv75pj4dlqo*

Home / South Africa / Mobile / SIM swap fraud leaves victims feeling helpless

SIM swap fraud leaves victims feeling helpless

SIM swap fraud leaves victims feeling helpless

SOURCE: *https://itweb.africa/article/sim-swap-fraud-leaves-victims-feeling-helpless/wbrpOqgPdxJvDLZn?utm_source=chatgpt.com*

SIM Cards

The SIM cards are elements that ensure identification and authentication with the network. To achieve this, different values are stored in the SIM card.

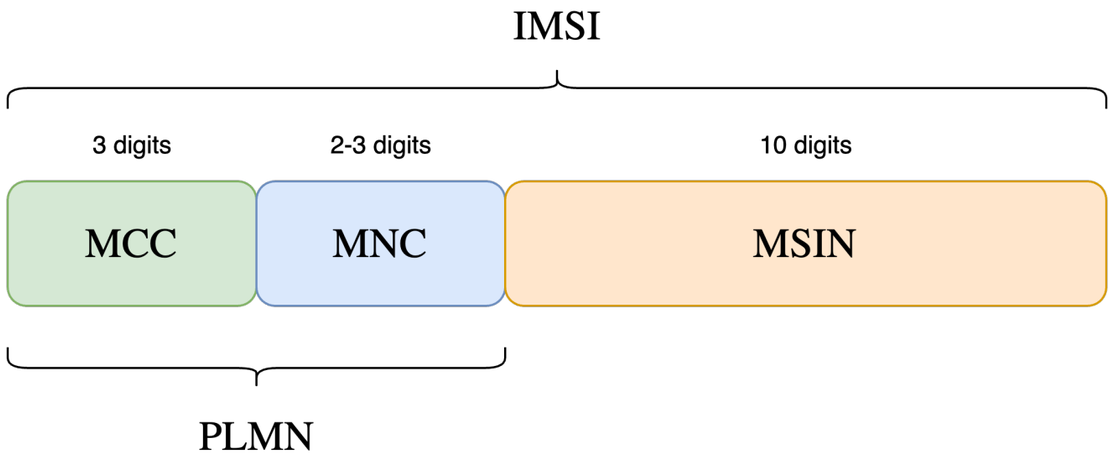
ICCID → SIM serial number

IMSI → International Mobile Subscriber Identity
UNIQUELY identifies a user.

Ki → Authentication Key

OP → Operator Code

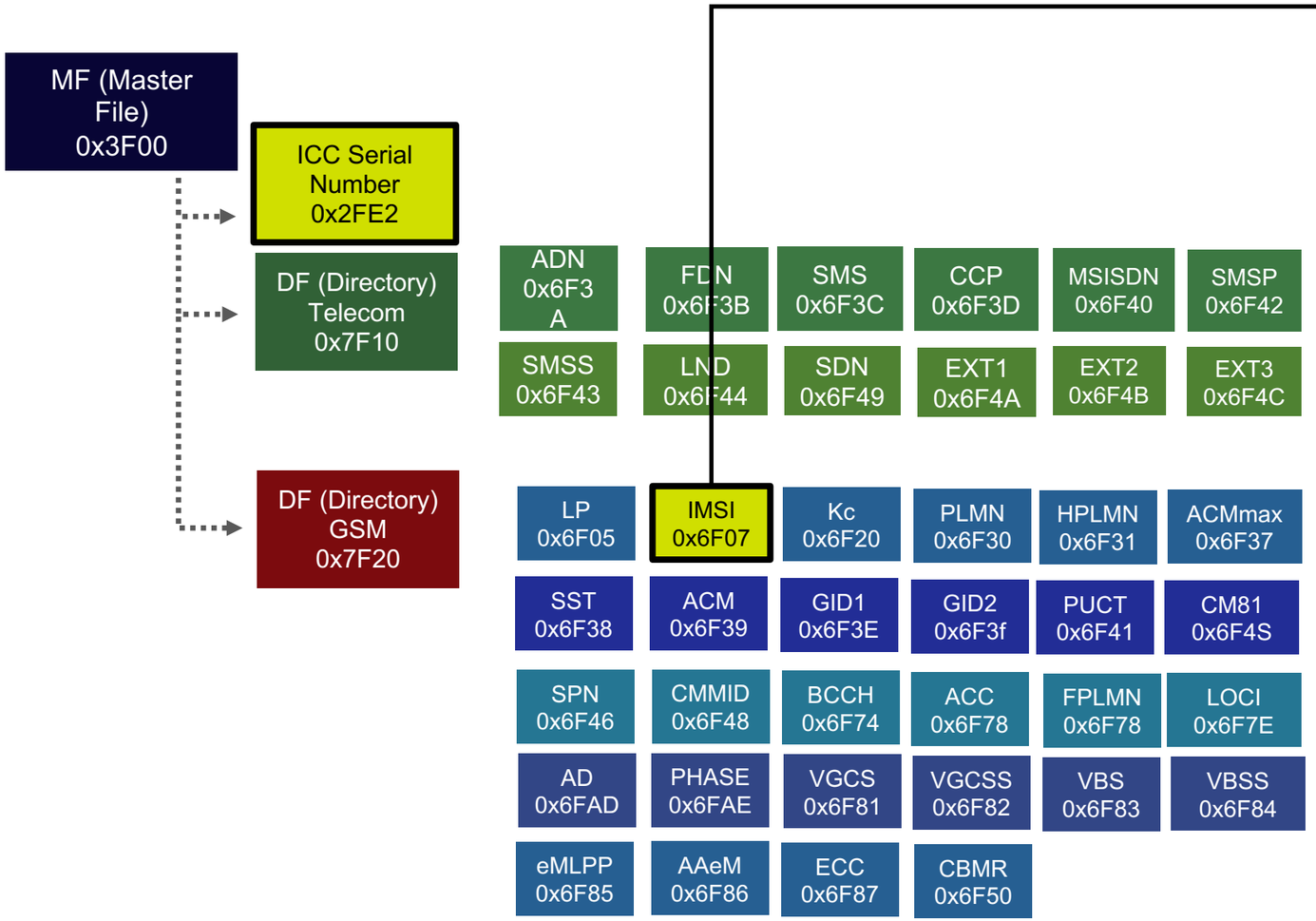
GSM 11.11: Specification of the SIM - ME interface



SIM Filesystem

SIM cards can be compared to a Linux filesystem, where you find directories and files.

These files can be accessed using open-source software.



3GPP TS 31.102 version 3.8.0 Release 1999 | 15 | ETSI TS 131 102 V3.8.0 (2001-12)

4.2.2 EF_{IMSI} (IMSI)

This EF contains the International Mobile Subscriber Identity (IMSI).

Identifier: '6F07'	Structure: transparent	Mandatory
SFI: '07'		
File size: 9 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Length of IMSI	M	1 byte
2 to 9	IMSI	M	8 bytes

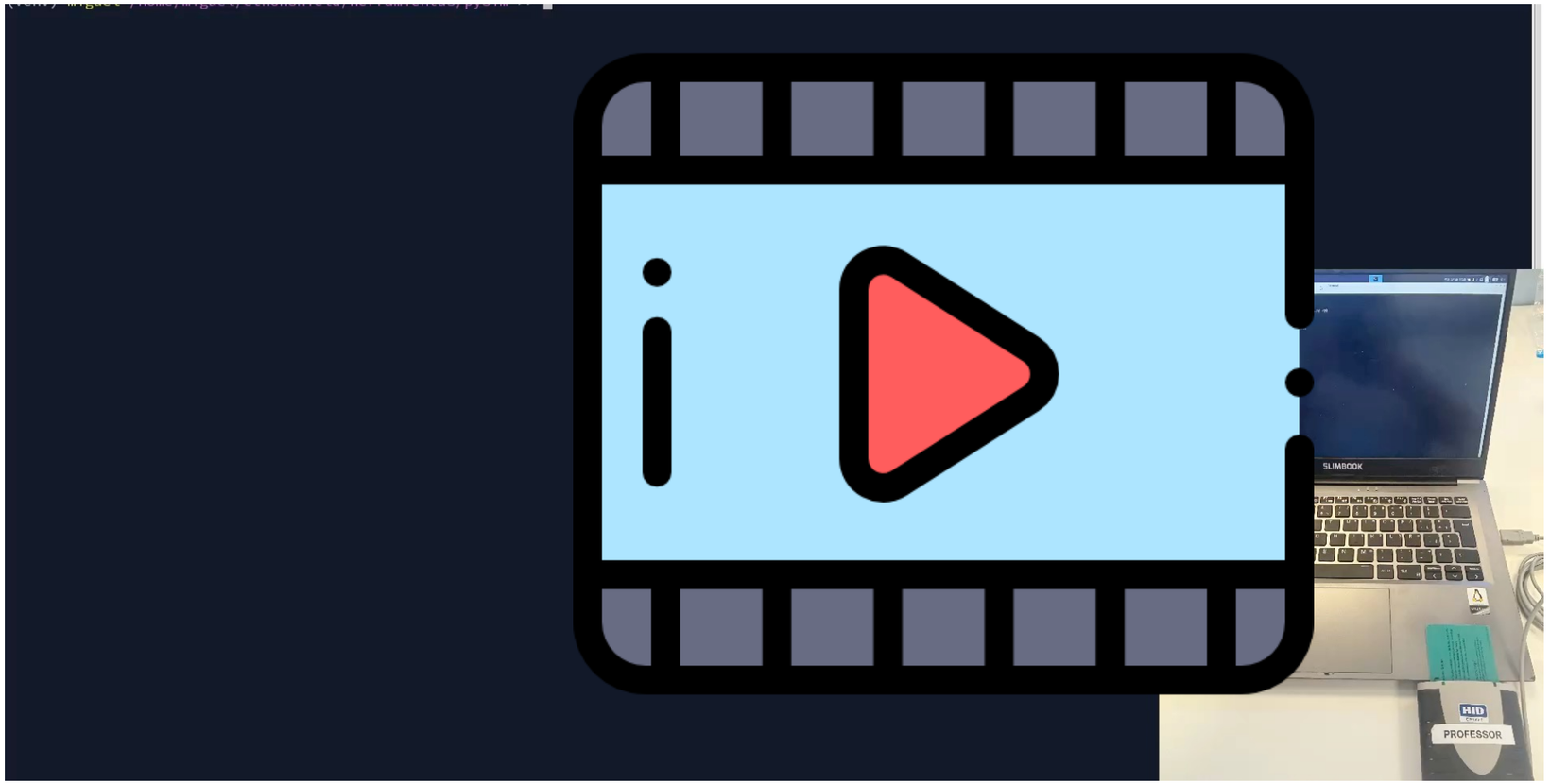
SOURCE:
https://www.etsi.org/deliver/etsi_ts/131100_131199/131102/03.08.00_60/ts_131102v030800p.pdf

Not all EFs involved in the attack will be described for obvious reasons.

Extract the essential SIM card information

Physical SIM card

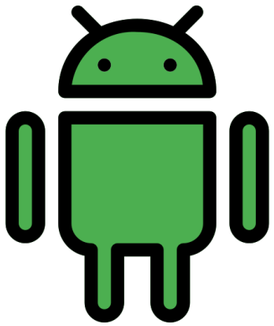
Extract the physical SIM card from the phone



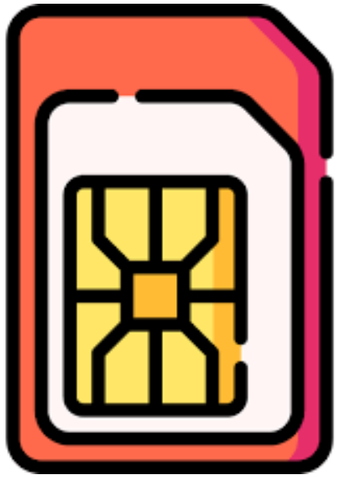
Smartphone Generic Architecture

How many operating systems does a terminal have?

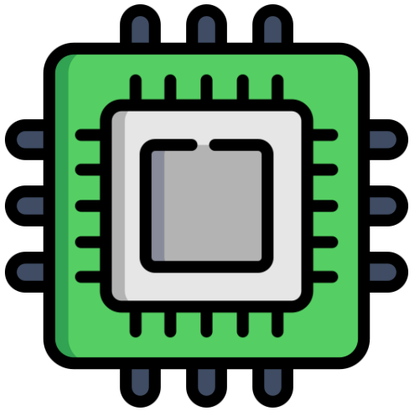
iOS



User O.S.



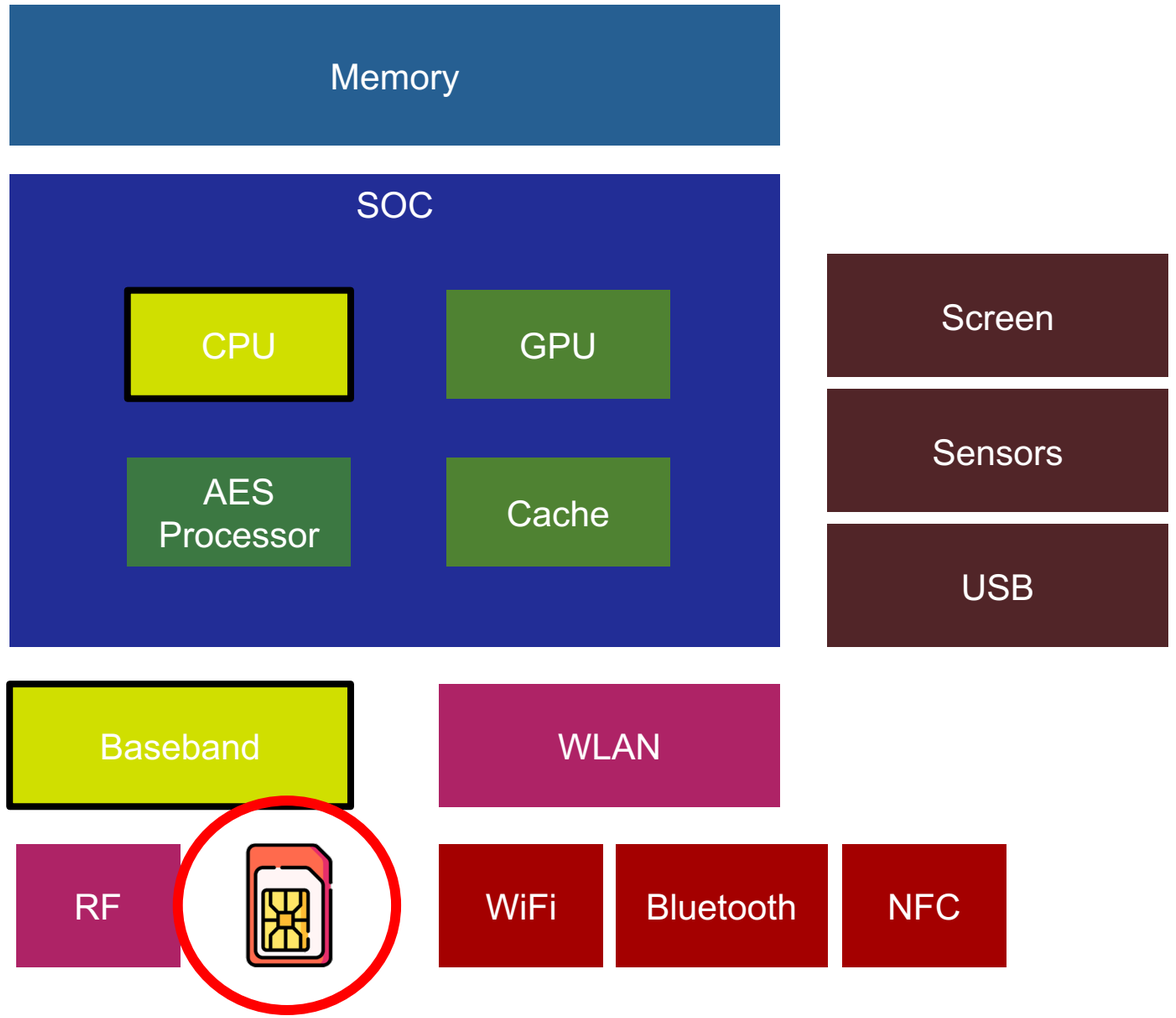
SIM cards

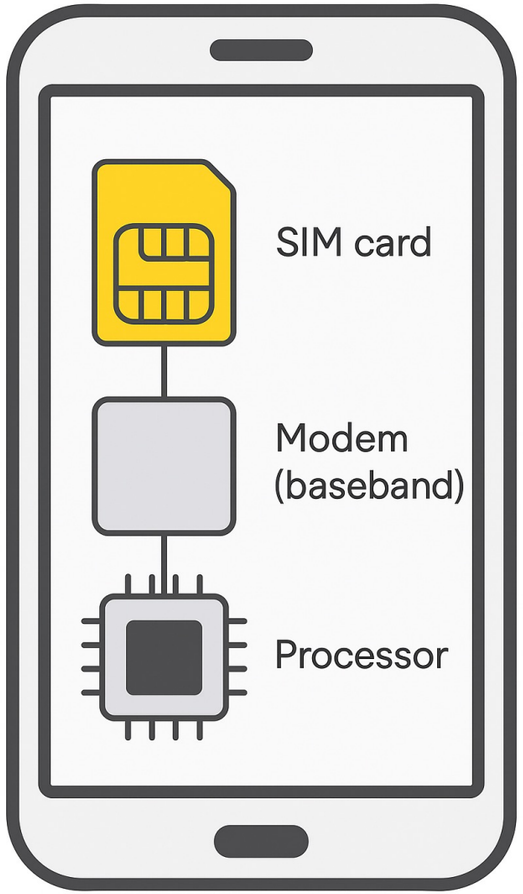


Baseband

Smartphone Generic Architecture

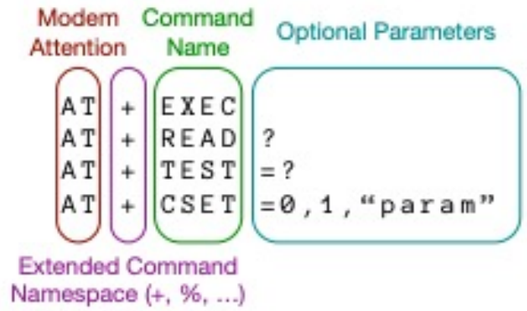
The objective is to explore different methods of accessing the SIM card when it is inserted in the smartphone.





Exploring AT Commands

The AT command set is a specific command language originally developed by Dale Heatherington and Dennis Hayes for the Hayes Smartmodem in 1981 (Wikipedia).



SOURCE:
https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-tian.pdf

Given their command architecture, they are susceptible to fuzzing and brute force attacks to find hidden commands or undocumented proprietary commands (secret codes).

Although historically they have been associated with modems rather than mobile phones, with the advent of the first smartphones, which already incorporated web browsing functions and allowed data-only use, they also began to incorporate AT commands.

SOURCE: Wikipedia

Exploring AT Commands

There are AT commands designed to cover very specific functions.

Looking through the documentation, we quickly found a set of **AT commands** designed to **interact** with the **SIM card**.

3GPP AT commands
Turn 3GPP AT commands on or off.

Basic commands to get information about the modem and SIM card

The below commands do not have a read or test command and no parameters - they only execute commands that return information.

Name	AT Command	Description
Get manufacturer	AT+CGMI	Returns string representation of the manufacturer
Get model	AT+CGMM	Returns the model of the modem.
Get firmware	AT+CGMR	Returns firmware revision
Get IMEI	AT+GSN	Retrieves the International Mobile Equipment Identity of the module
Get IMSI	AT+CIMI	Returns the current used IMSI

SOURCE: https://www.emnify.com/developer-blog/at-commands-for-cellular-modules#basic-commands

Exploring AT Commands

We highlight the work "*ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem*" which studies a large number of Android devices.

LILY HAY NEWMAN SECURITY AUG 29, 2018 7:00 AM

Exploiting Decades-Old Telephone Tech to Break Into Android Devices

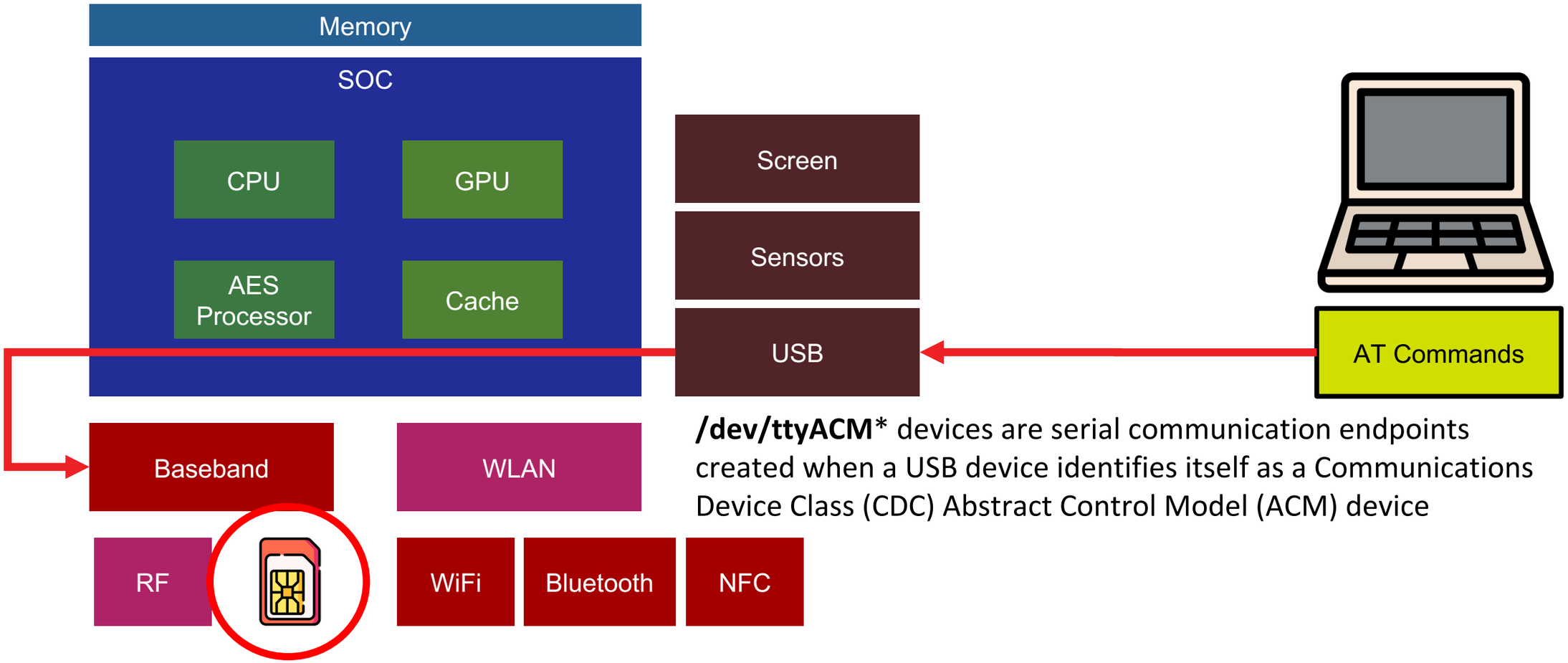
So-called Attention commands date back to the 80s, but they can enable some very modern-day smartphone hacks.

SOURCE: https://www.wired.com/story/at-commands-android-vulnerability

The study uncovers many undocumented AT commands with dangerous functionality, such as Android Lockscreen Bypassing & Event Injection (`LG G4, AT%KEYLOCK=0`), among many others.

Exploring AT Commands

We confirm a way to access the SIM card using AT commands, which will be processed by the baseband (modem).

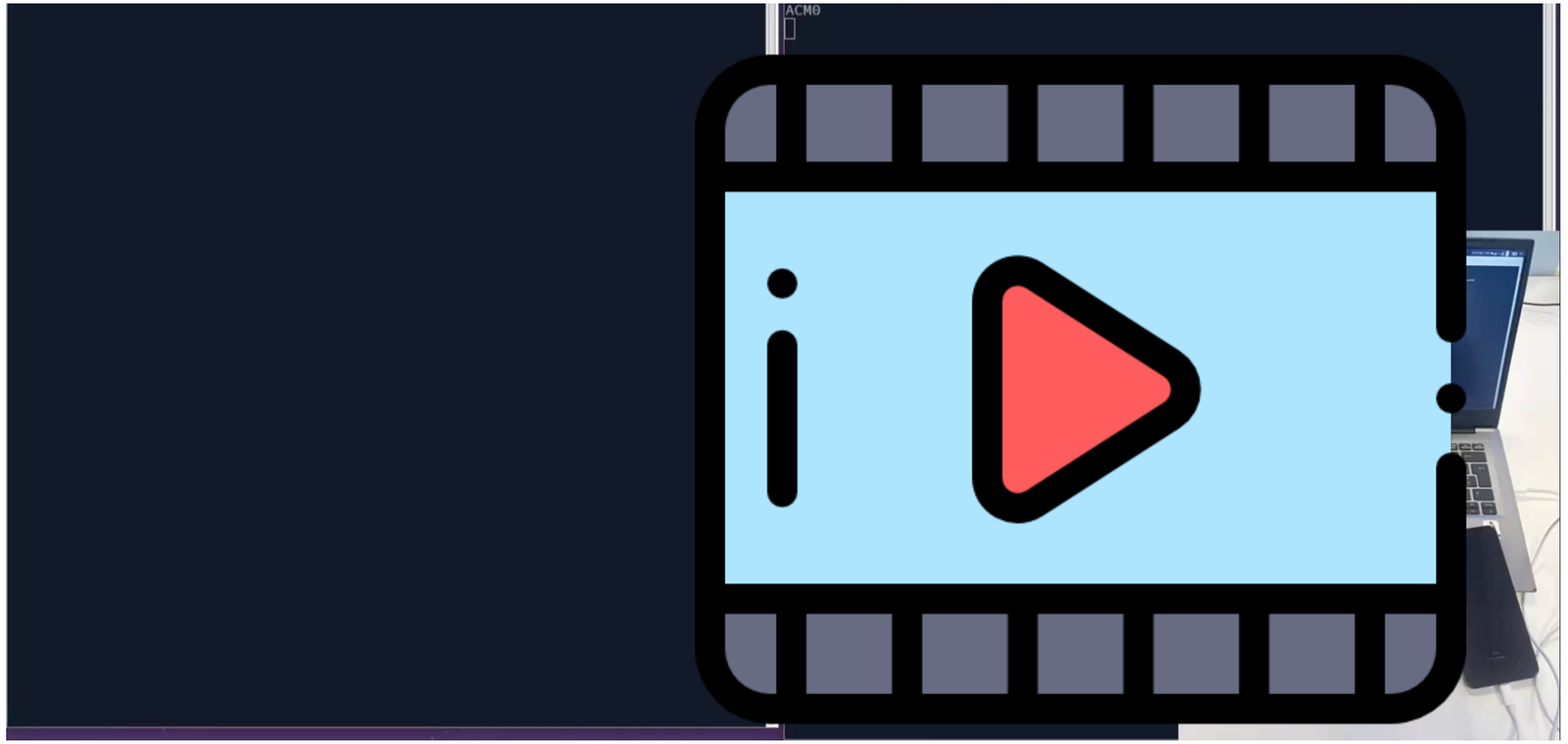


/dev/ttyACM* devices are serial communication endpoints created when a USB device identifies itself as a Communications Device Class (CDC) Abstract Control Model (ACM) device

Extract the essential SIM card information

USB

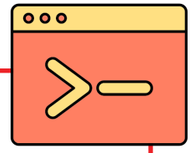
Interact with the phone's USB interface by sending AT commands



Android Debug Bridge

Android Debug Bridge (adb) is a tool for controlling Android from outside: it can be used to install apps, make backups, or debug the system.

AT commands, on the other hand, are used to control the phone's modem: make calls, send SMS messages, or check coverage.



AT Communications architecture

Protocol: Asynchronous serial communication (over USB)

Topology: Host ↔ Modem.

Destination: Does not pass through Android, but is sent directly to the baseband modem.

ADB Communications architecture

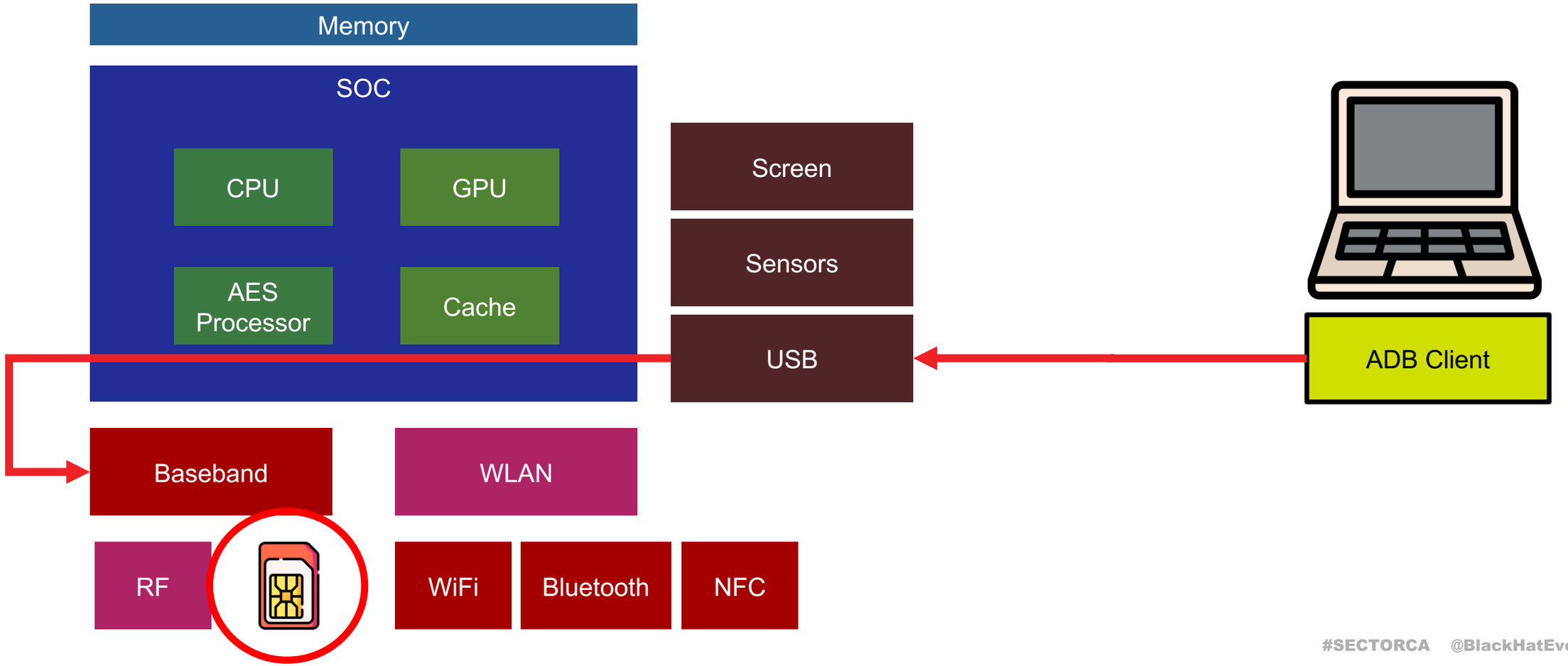
Protocol: USB or TCP/IP

Topology: Client ↔ Server ↔ Daemon

- ADB Client → usually on your computer
- ADB Server → local intermediary that listens on localhost:5037
- ADB Daemon (adbd) → process within the Android device

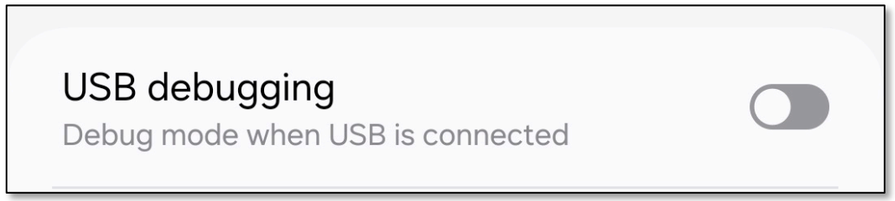
Android Debug Bridge

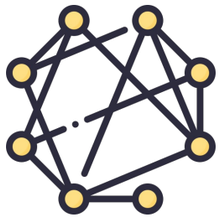
An Android RIL (Radio Interface Layer) SMD device refers to the physical radio hardware on an Android smartphone or tablet that handles cellular network communications, such as calls, SMS, and mobile data. The "SMD" likely refers to a Surface Mount Device component on the printed circuit board (PCB) that serves as the radio modem, while RIL is the software abstraction layer that allows the Android OS to communicate with this hardware.



Android Debug Bridge

From an ADB shell, AT commands can also be sent to the modem from the Android operating system.



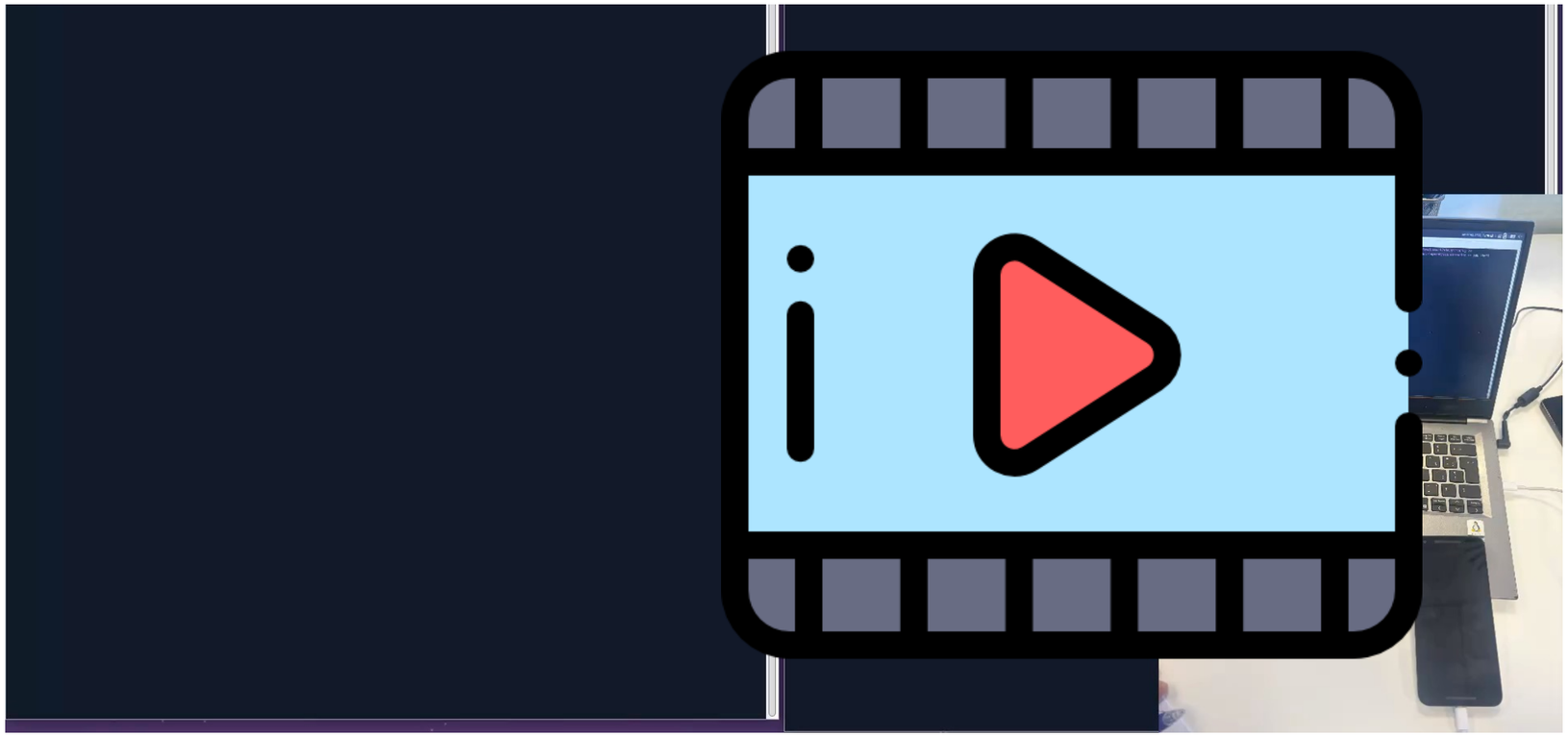


This allows another method of interacting with the modem, which may have different security requirements depending on the operating system version.

Extract the essential SIM card information

ADB

Interact with the phone's modem via *adb* shell by sending AT commands

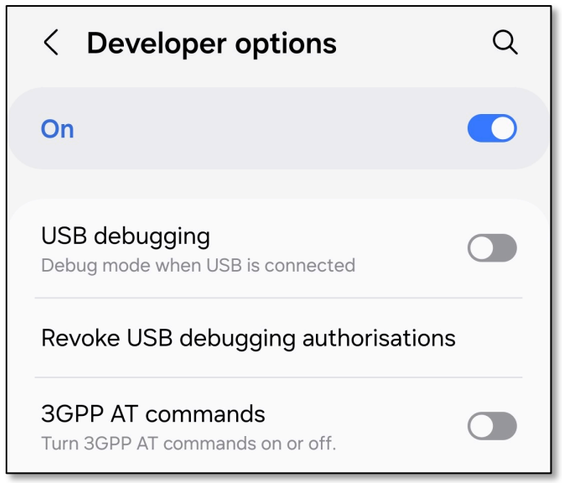


Summary Android security features

AT commands and security

Google does not directly control this attack surface, as it depends on how manufacturers expose the modem.

Android base did not introduce a specific restriction for AT commands, and security here depends on the manufacturer.



Android Debug Bridge security

It has had security issues. For example, until Android 2.2, there was a vulnerability (RageAgainstTheCage) that allowed root shell access if ADB was enabled

Over time, ADB was protected with RSA authentication (the device must authorize the connected computer) and whitelists to prevent unwanted access.

Screen lock: PIN, pattern, and biometrics

Since early versions, Android has supported locking via PIN, pattern, or password.

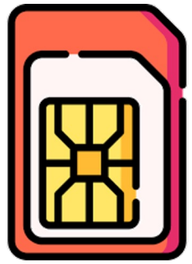
Biometrics (fingerprint and face)
-Android Marshmallow introduces native support for fingerprint, with standard API for unlocking and secure authentication.
-In Android Pie, the API is improved to adapt to new types of biometrics (facial recognition, on-screen sensors).

Identity Check (Android 15 and later)
-With Android 15, Identity Check arrives: outside of trusted locations, only biometrics are accepted to access sensitive settings (change PIN, passwords, reset device, etc.).

Summary Android security features

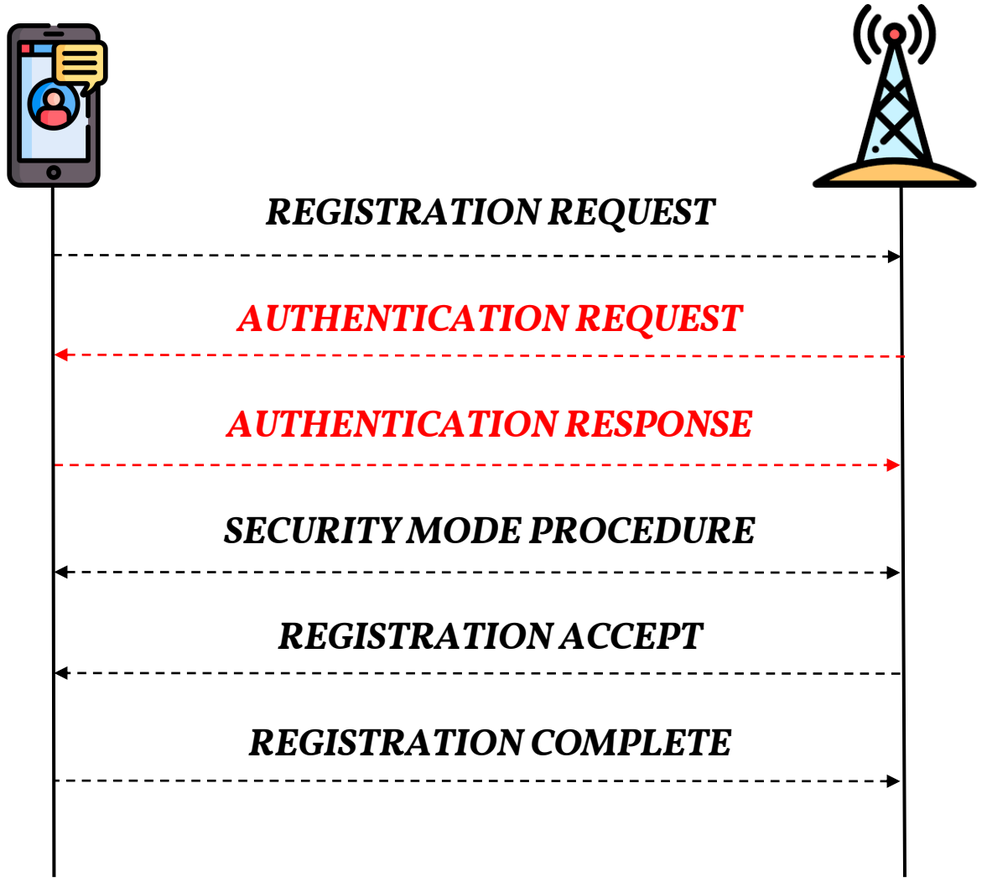
Function	Before Android 4.4.2	Android 4.4.2 – Android 10	Android 11+	Android 15+ (Identity Check)
Enable ADB	No unlock required	Unlock + accept **RSA key** required	Same as 4.4.2	Requires **unlock + biometric authentication**
Use ADB (authorized host)	Full access even if locked	Partial access when locked	Some **critical operations** require unlocking	Same as Android 11
AT commands via USB	Almost always accessible, even if locked	Some OEMs blocked them, Google didn't enforce yet	Since **Android 9 Pie**, most commands are blocked when locked	Same as Android 11
Biometric authentication	Not available	Optional for screen unlock	**Lockdown mode** allows disabling biometrics temporarily	**Mandatory biometrics** for sensitive settings

SOURCE: ChatGPT



Mobile Network 101: Authentication Procedure

The authentication is the procedure that ensures that both the network and the client are who they claim to be.



To prevent fraudulent activities, the network ensures the user intending to use the network is who it claims to be.

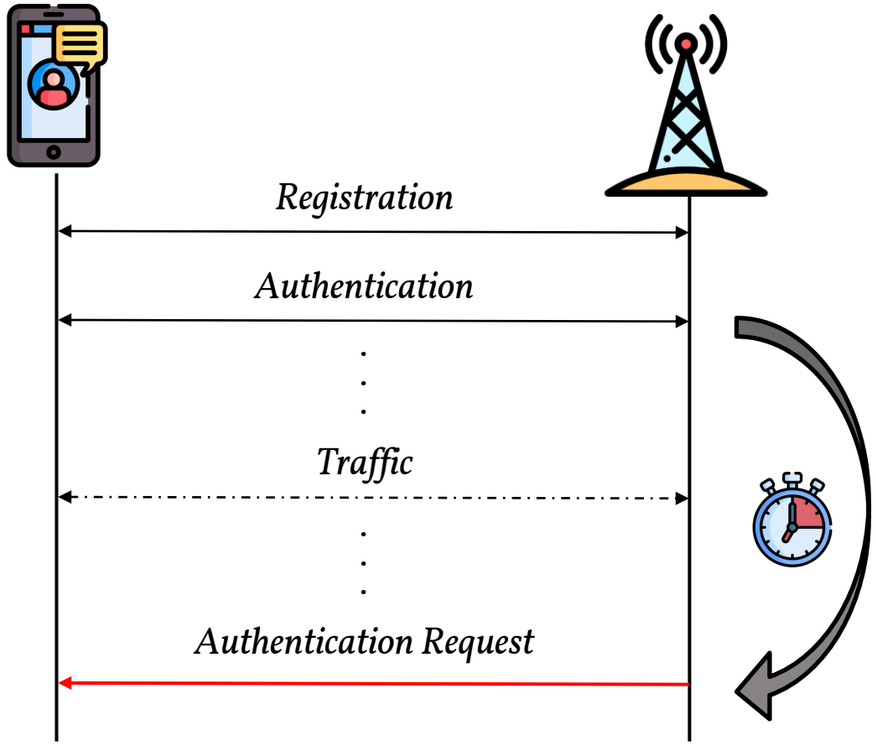
From 3G onwards, the SIM card also ensures the network is legitimate, preventing fraudulent networks (fake stations). There is **mutual authentication**.

Authentication Policy

The authentication policy defines how often and under what conditions the authentication procedure should be triggered.

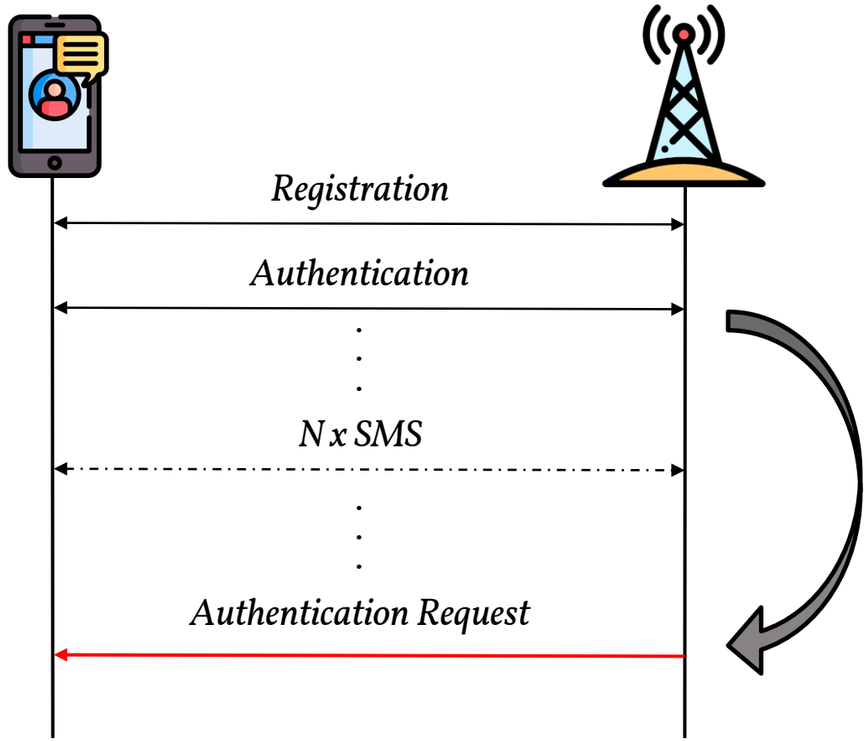
Time based

Subscribers are authenticated after a predetermined duration



Event based

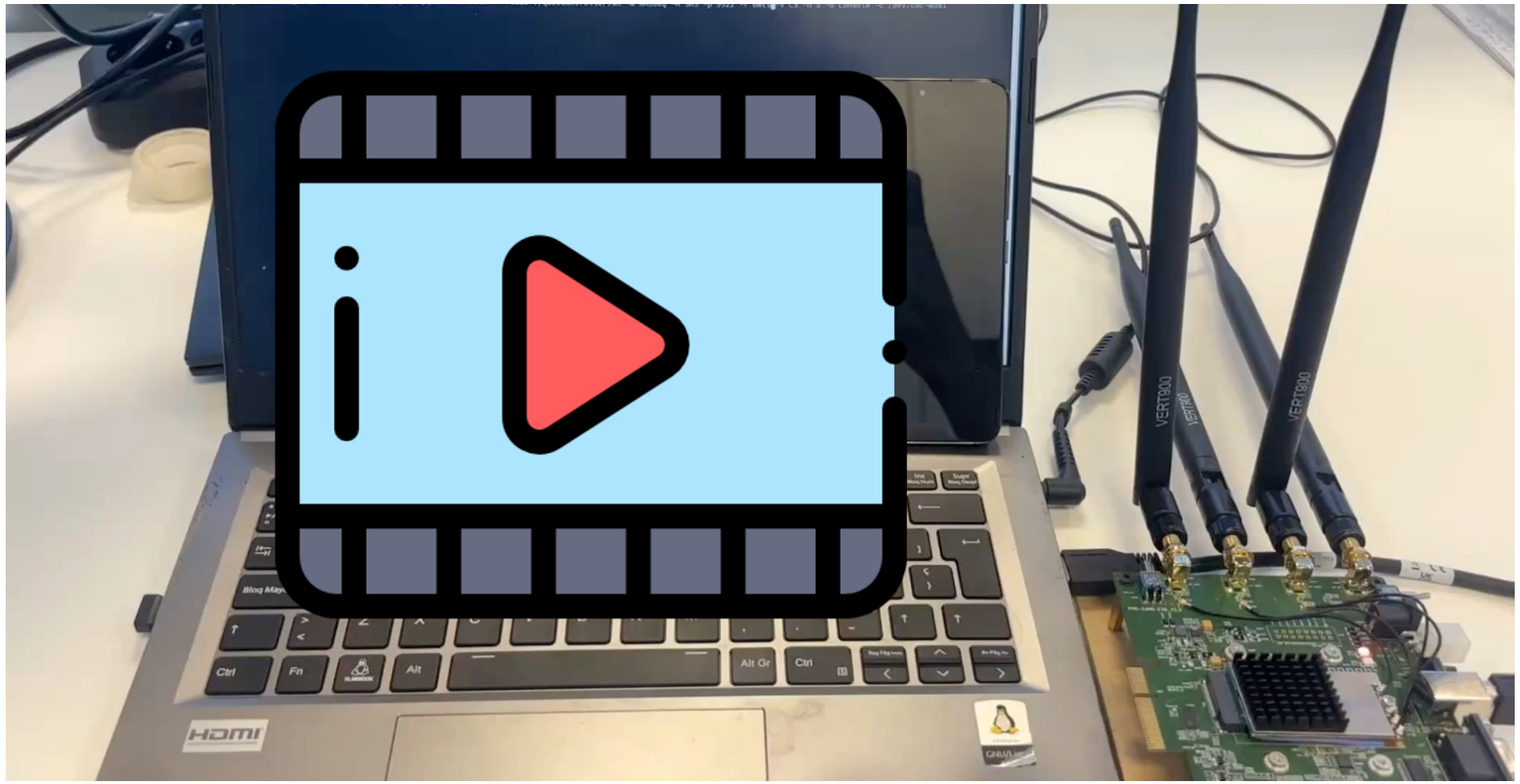
Generally, include calls, registration requests, mobility updates or SMS.



What is a “weak” authentication policy?

Authentication Policy

The authentication policy can be determined through automated tasks, generating events that trigger an authentication procedure.



Authentication Policy

This example Wireshark shows the result of the previous automated task

Source	Destination	Protocol	SMS text	Info
127.0.0.1	127.0.0.1	GSMTAP		(DTAP) (MM) Location Updating Request
127.0.0.1	127.0.0.1	GSMTAP		(DTAP) (MM) Location Updating Accept
127.0.0.1	127.0.0.1	GSMTAP		(DTAP) (MM) Authentication Request
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
127.0.0.1	127.0.0.1	GSMTAP		(DTAP) (MM) Authentication Request
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
127.0.0.1	127.0.0.1	GSM SMS	Hello\n	(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)

16 SMS

Authentication Policy

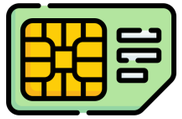
Example of authentication policy results from different studied operators in 2G technology

	Op. A	Op. B	Op. C	Op. D
Registrations CS	20	20	20	20
Authentication Procedures	1	1	**15**	**13**
Registrations PS	20	20	19	21
Authentication Procedures	**20**	**20**	**15**	**20**
SMS	20	20	14	23
Authentication Procedures	1	2	1	**17**
Phone Call	20	20	14	9
Authentication Procedures	2	1	2	1

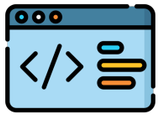
Ghost SIM attack

By extracting critical information from a legitimate SIM card and copying it to a fraudulent one WITHOUT needing the secret key (Ki), the attacker will impersonate the victim and successfully register with the mobile network, provided that no authentication procedure is triggered.

Have **physical access** to victim's phone



Extract the essential SIM card **information**



Copy SIM card **information** into programmable SIM card

Insert the programmable SIM card into a mobile device

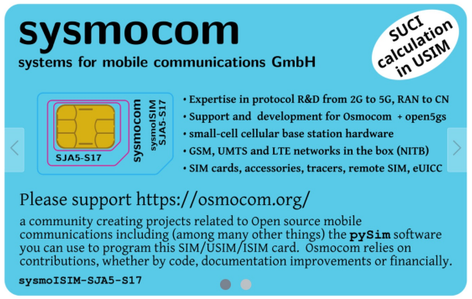
Successfully connect to network

↓

For this, NO authentication procedure must be triggered

Copy information into programmable SIM

The information will be copied to a programmable SIM card



To be able to modify the different parameters in the programmable SIM card, we need the **ADM** PIN.

Connection to the network

To be able to successfully connect to the legitimate network, NO authentication procedure should be triggered

Authentication procedure triggered - FAILURE

(gsmtap and not icmp) && (gsm_a.dtap.protocol_discriminator == 5)

No.	Time	Source	Destination	Protocol	Info
174	22:17:42,563282382	127.0.0.1	127.0.0.1	GSMTAP	(DTAP) (MM) Location Updating Request
190	22:17:43,668211870	127.0.0.1	127.0.0.1	GSMTAP	(DTAP) (MM) Authentication Request
192	22:17:43,717313000	127.0.0.1	127.0.0.1	GSMTAP	(DTAP) (MM) Authentication Failure
194	22:17:43,917594535	127.0.0.1	127.0.0.1	GSMTAP	(DTAP) (MM) Identity Request
196	22:17:43,918238730	127.0.0.1	127.0.0.1	GSMTAP	(DTAP) (MM) Identity Response
202	22:17:44,169173323	127.0.0.1	127.0.0.1	GSMTAP	(DTAP) (MM) Location Updating Reject

Authentication request message

Rejected by the network

```
▸ Frame 174: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface lo, id 0
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ User Datagram Protocol, Src Port: 48918, Dst Port: 4729
▸ GSM TAP Header, ARFCN: 0 (Uplink), TS: 0, Channel: UNKNOWN (0)
▾ GSM A-I/F DTAP - Location Updating Request
  ▾ Protocol Discriminator: Mobility Management messages (5)
      .... 0101 = Protocol discriminator: Mobility Management messages (0x5)
      0000 .... = Skip Indicator: No indication of selected PLMN (0)
    00.. .... = Sequence number: 0
    ..00 1000 = DTAP Mobility Management Message Type: Location Updating Request (0x08)
  ▸ Ciphering Key Sequence Number
  ▸ Location Updating Type - IMSI attach
  ▸ Location Area Identification (LAI)
  ▸ Mobile Station Classmark 1
  ▾ Mobile Identity - TMSI/P-TMSI (0x5cbec7ac)
      Length: 5
      1111 .... = Unused: 0xf
      .... 0... = Odd/even indication: Even number of identity digits
      .... .100 = Mobile Identity Type: TMSI/P-TMSI/M-TMSI (4)
      TMSI/P-TMSI/M-TMSI/5G-TMSI: 1556006828 (0x5cbec7ac)
  ▸ MS network feature support
```

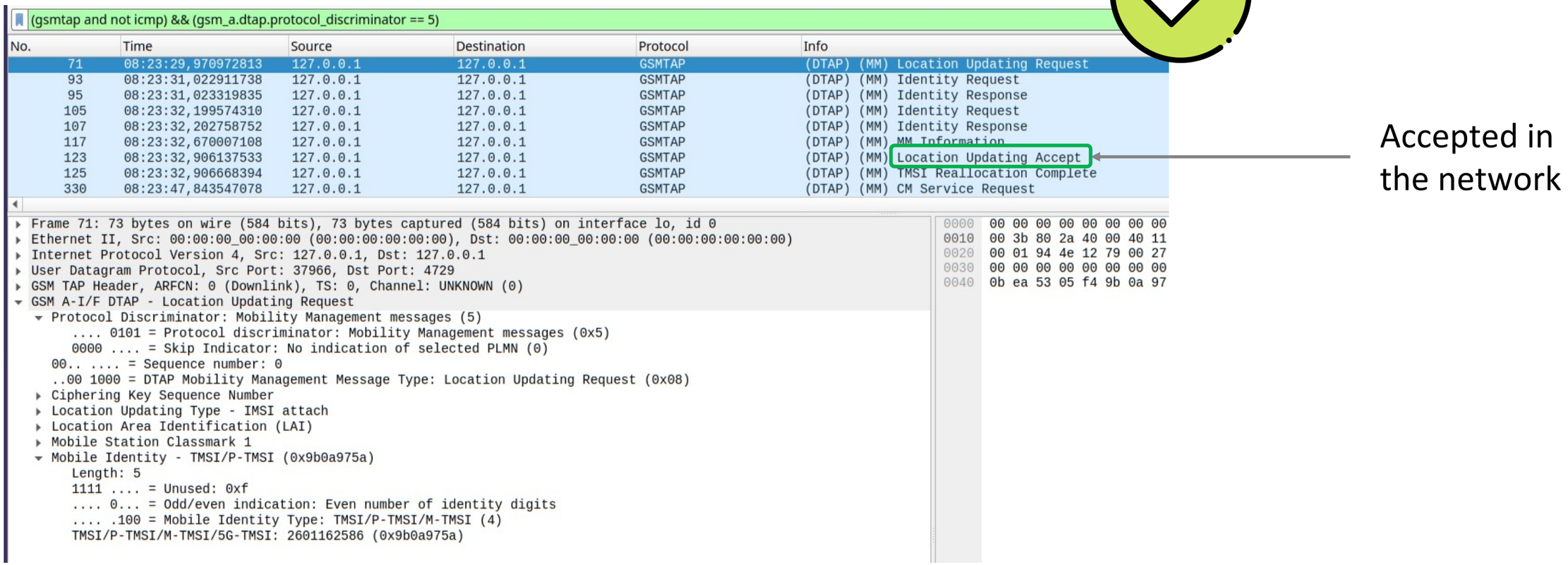
```
0000  00 00 00 00 00 00
0010  00 3c f0 95 40 00
0020  00 01 bf 16 12 79
0030  00 00 00 00 00 00
0040  01 34 53 05 f4 5c
```

We don’t have the secret key Ki

Connection to the network

To be able to successfully connect to the legitimate network, NO authentication procedure should be triggered

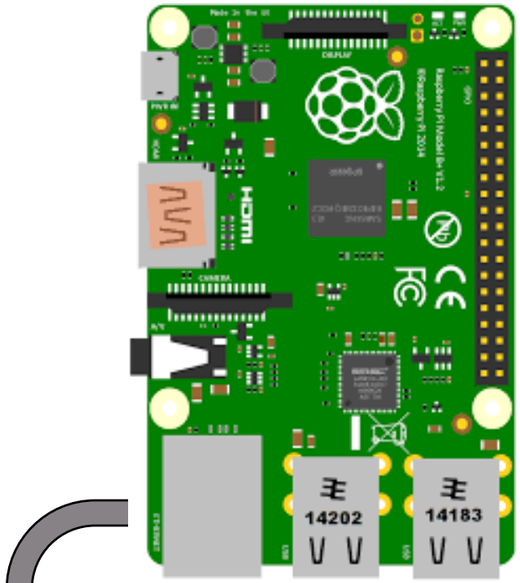
Authentication procedure NOT triggered - SUCCESS

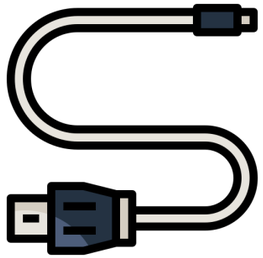


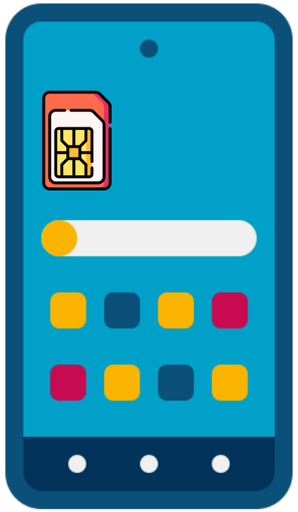
Accepted in the network

Ghost SIM Attack

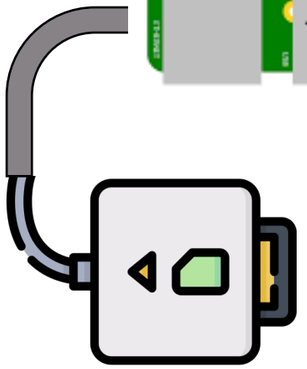
Raspberry Pi 3







Legitimate mobile device



Programmable SIM card

Fraudulent mobile device

Ghost SIM attack

LIVE DEMO

Ghost SIM attack: Results over the World

How robust should the authentication policy of an operator be to prevent the "ghost" SIM from successfully connecting to the network?

	2G		3G		4G	5G
	CS	PS	CS	PS	PS	PS
[EUR Country #1] Operator #1	Vulnerable	Not Vulnerable	Vulnerable	Not Vulnerable	Vulnerable	Vulnerable
[EUR Country #1] Operator #2	Vulnerable	Not Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable
[EUR Country #2] Operator #3	Vulnerable	Not Vulnerable	NA	NA	Vulnerable	NA
[EUR Country #2] Operator #4	Vulnerable	Not Vulnerable	NA	NA	Vulnerable	NA
[EUR Country #3] Operator #5	Not Vulnerable	Not Vulnerable	NA	NA	Vulnerable	NA
[ASIA Country #1] Operator #6	NA	NA	NA	NA	Vulnerable	NA
[ASIA Country #1] Operator #7	NA	NA	NA	NA	Vulnerable	NA

We haven't been able to conduct 5G SA tests in foreign countries, as all operators require a contract with a physical address and bank account in the country to be eligible. What it's sell as 5G prepaid cards is NSA technology; access to technologies marketed as "5G+" or "5G Ultra" requires a contract.

Ghost SIM attack: Post Exploitation

What can we do after we successfully register on the network?

Can we receive or make calls?

Can we receive or send SMS?

Can we use internet?

If we receive SMS, could we bypass 2FA?

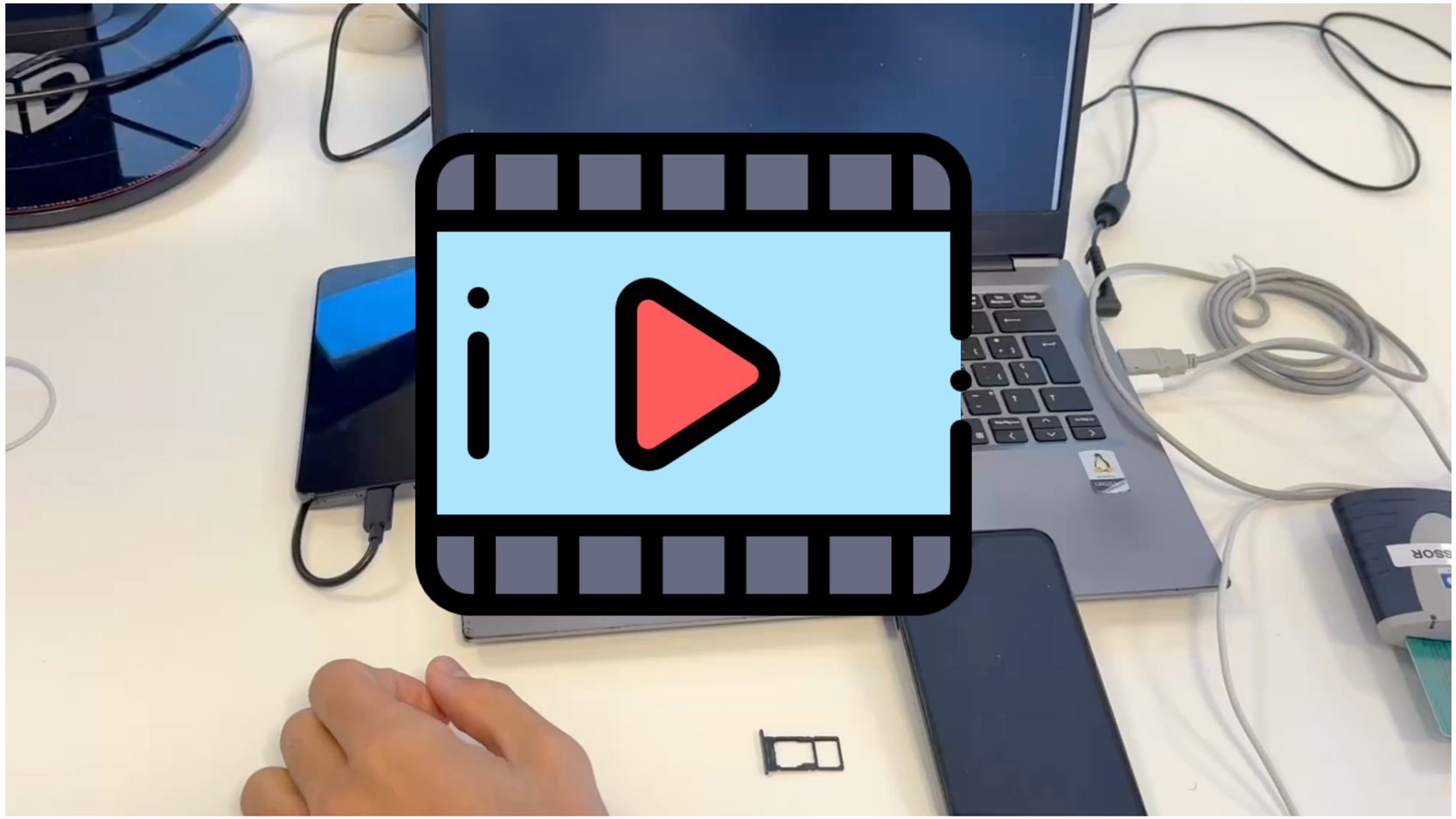
How long will I be registered on the network?

Can we use VoLTE?

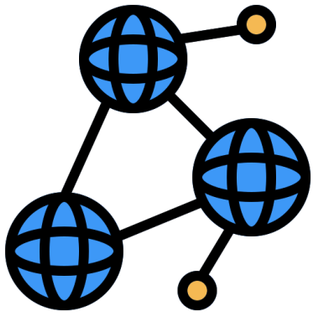
Is the legitimate user under a DoS attack?

Ghost SIM attack

If we successfully connect to multiple technologies, it is possible to bypass SMS/Calls 2FA in messaging applications



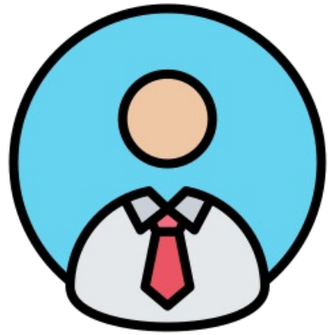
Ghost SIM attack: Limitations



The operator authentication policy robustness depend greatly on each operator and are influenced by the culture of each country.

For example (this is not an exhaustive list):

- Functionality provided by network manufacturers
- Aspects established in the mobile network design, as:
- Traffic volume received by the nodes responsible for authentication vectors
- Mobility configuration
- Control plane traffic volume between CORE nodes



Attacker requires:

Physical access to Android smartphone:

- Screen unlocked
- Screen unlocked + USB Debugging enabled
- Screen unlocked + 3GPP AT commands enabled

OR

Physical access to SIM:

- PIN disabled

Ghost SIM attack: Key Facilitators

Android is an operating system with significant heterogeneity across versions implemented by the major manufacturers. Vulnerabilities related to bypassing the screen lock, the ADB client, or undocumented AT commands are common.

Identifier	CISA Kev Info	Published Date	CNA	Description
CVE-2025-26428	✖	2025-09-04	Android (associated with Google Inc. or Open Handset Alliance)	In startLockTaskMode of LockTaskController.java, there is a possible lock screen bypass due to a logic error in the code. This could lead to physical escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.
CVE-2025-26421	✖	2025-09-04	Android (associated with Google Inc. or Open Handset Alliance)	In multiple locations, there is a possible lock screen bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2025-22434	✖	2025-09-02	Android (associated with Google Inc. or Open Handset Alliance)	In handleKeyGestureEvent of PhoneWindowManager.java, there is a possible lock screen bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2025-0077	✖	2025-09-04	Android (associated with Google Inc. or Open Handset Alliance)	In multiple functions of UserController.java, there is a possible lock screen bypass due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2023-40094	✖	2023-12-04	Android (associated with Google Inc. or Open Handset Alliance)	In keyguardGoingAway of ActivityTaskManagerService.java, there is a possible lock screen bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2021-0688	✖	2021-10-06	Android (associated with Google Inc. or Open Handset Alliance)	In lockNow of PhoneWindowManager.java, there is a possible lock screen bypass due to a race condition. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 A...

SOURCE: NIST National Vulnerability Database, Keyworks “lock screen bypass”

Ghost SIM attack: Key Facilitators

Android is an operating system with significant heterogeneity across versions implemented by the major manufacturers. Vulnerabilities related to bypassing the screen lock, the ADB client, or undocumented AT commands are common.

CVE-2019-16273 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

DTEN D5 and D7 before 1.3.4 devices allow unauthenticated root shell access through Android Debug Bridge (adb), leading to arbitrary code execution and system administration. Also, this provides a covert ability to capture screen data from the Zoom Client on Windows by executing commands on the Android OS.

CVE-2023-43488 Detail

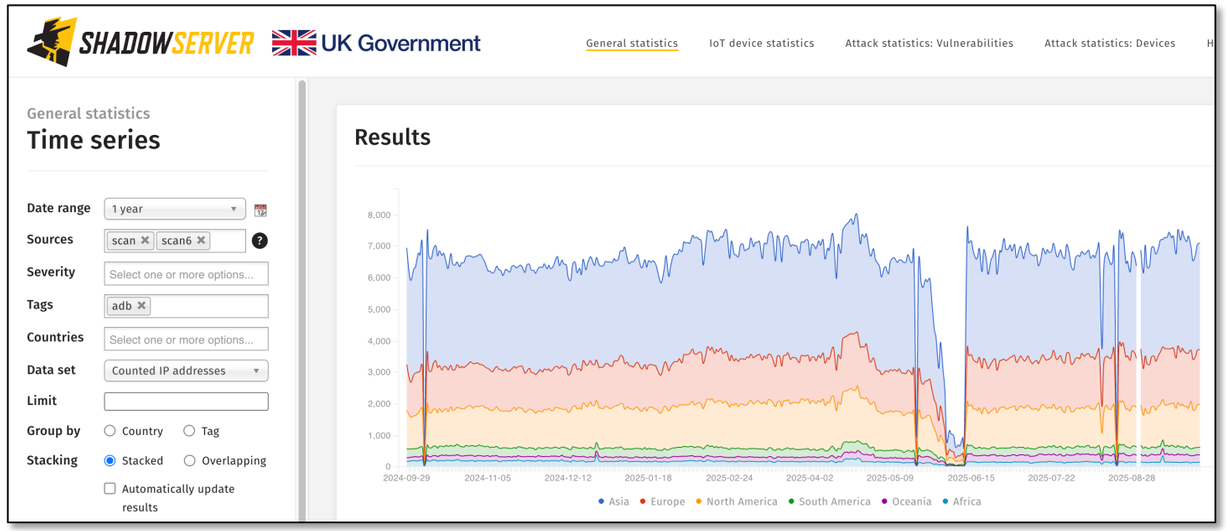
MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

The vulnerability allows a low privileged (untrusted) application to modify a critical system property that should be denied, in order to enable the ADB (Android Debug Bridge) protocol to be exposed on the network, exploiting it to gain a privileged shell on the device without requiring the physical access through USB.

SOURCE: NIST National Vulnerability Database



SOURCE: https://www.shadowserver.org

Ghost SIM attack: Key Facilitators

Android is an operating system with significant heterogeneity across versions implemented by the major manufacturers. Vulnerabilities related to bypassing the screen lock, the ADB client, or undocumented AT commands are common.

CVE-2025-26412 Detail

AWAITING ANALYSIS

This CVE record has been marked for NVD enrichment efforts.

Description

The SIMCom SIM7600G modem supports an undocumented AT command, which allows an attacker to execute system commands with root permission on the modem. An attacker needs either physical access or remote shell access to a device that interacts directly with the modem via AT commands.

CVE-2016-4030 Detail

DEFERRED

This CVE record is not being prioritized for NVD enrichment efforts due to resource or other concerns.

Description

Samsung SM-G920F build G920FXXU2COH2 (Galaxy S6), SM-N9005 build N9005XXUGBOK6 (Galaxy Note 3), GT-I9192 build I9192XXUBNB1 (Galaxy S4 mini), GT-I9195 build I9195XXUCOL1 (Galaxy S4 mini LTE), and GT-I9505 build I9505XXUHOJ2 (Galaxy S4) devices have unintended availability of the modem in USB configuration number 2 within the secure lockscreen state, allowing an attacker to make phone calls, send text messages, or issue commands, aka SVE-2016-5301.

CVE-2016-4032 Detail

DEFERRED

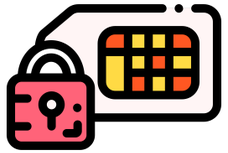
This CVE record is not being prioritized for NVD enrichment efforts due to resource or other concerns.

Description

Samsung SM-G920F build G920FXXU2COH2 (Galaxy S6), SM-N9005 build N9005XXUGBOK6 (Galaxy Note 3), GT-I9192 build I9192XXUBNB1 (Galaxy S4 mini), GT-I9195 build I9195XXUCOL1 (Galaxy S4 mini LTE), and GT-I9505 build I9505XXUHOJ2 (Galaxy S4) devices do not block AT+USBDEBUG and AT+WIFIVALUE, which allows attackers to modify Android settings by leveraging AT access, aka SVE-2016-5301.

SOURCE: NIST National Vulnerability Database

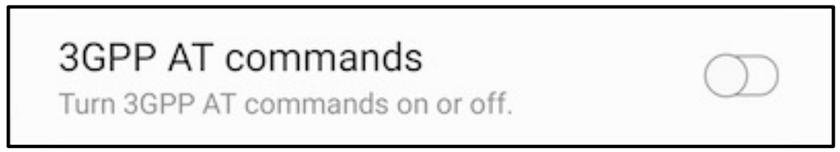
Users Countermeasures



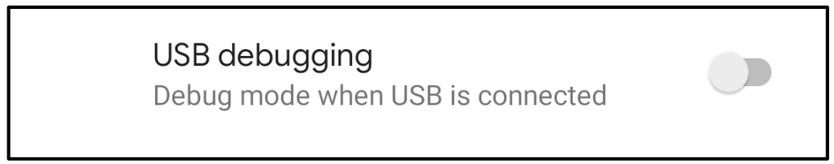
Always activate the PIN in you SIM card

Never leave your phone unattended

Paranoid screen lock



Have 3GPPAT commands deactivated (default)



USB Debugging disabled (default)

Operators Countermeasures

A feasible fine-tuning must be found (without causing traffic oversizing) but at the same time ensuring that conditions are avoided in which a potential attacker could gain network benefits without being authenticated.

Mandatory authentication of initial attachments and initial registrations on both circuit and data domains

Review of time counters (in VoIP, automatic registration is common every 3600 seconds, never more than 24 hours)

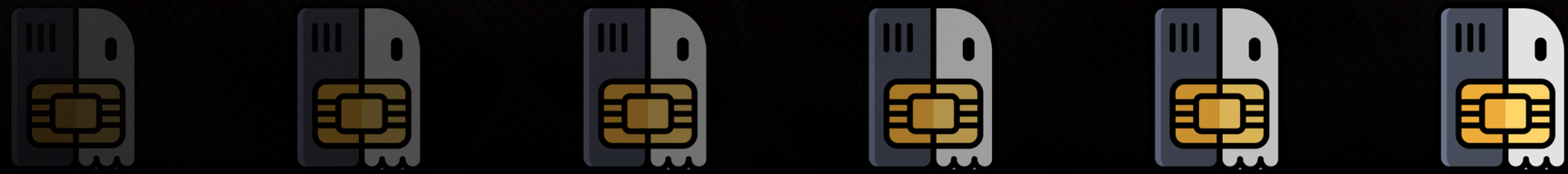
Review of counters based on "1 of n" events

PUBLISHED ON RESEARCH GATE

SECTOR
BRIEFINGS
October 1-2, 2025
METRO TORONTO CONVENTION CENTRE

Thank you

ETHON SHIELD



#SECTORCA @BlackHatEvents