SECURITY RESEARCH

SIM CARD VENDORS' QUESTIONNAIRE

Last update: 11 Feb 2024

INTRODUCTION

While most SIM card vendors' claim that privacy and security is their top-priority, real-life verification of that claim is not possible. This is primarily due to the following:

1) vendors do not publish / do not announce to the public security advisories regarding SIM card products [1][2]
2) vendors stick to certifications[1] and evaluations gained by their product such as those assigned by Common Criteria [3]
3) vendors tend to claim that their products are regularly audited and certified by third-party private and public organizations [4]
4) vendors do not let arbitrary independent 3rd parties conduct security analysis of SIM card products, some vendors introduced no sale policy to security companies [5].

The above approach has significant consequence.

First, arbitrarily parties may gain a completely false sense of security as no public vulnerability data may lead to the conclusion that no vulnerabilities are present in given vendor's SIM card products and that SIM card vendors QA / security processes are perfect (leaving technological companies such as Apple, Microsoft and Oracle far behind as each of these companies tend to fix dozens of security issues in their products each year).

Second, it is impossible for 3rd parties to verify if vendor's claims have any grounds. The know-how of vendors and their trusted evaluation labs (or contractors) is limited in some way. In a security field, many significant contributions are made by external parties. This is due to the unbiased, alternative perspective into a target product. SIM card vendors demonstrating a

[1] Unfortunately, the certifications do not add any data to the equation. While they may carry valuable information pertaining to whether a given product provides / implements certain security features (crypto algorithms, auth mechanisms, OS / user/ domains isolation, HW security features, etc.), they do not provide any valuable information about the actual security / quality of a target product, vendor's know-how and quality of its security processes. The reason is simple. Security vulnerabilities and attack techniques have been present in products with top-notch security features. Certified products are no exception here (Conax security evaluation case [6]).

closed approach are never to benefit from such contributions (they also instantly limit their own innovation in the area of security). As such, they risk getting caught by surprise when a 3rd party finds a bug and releases it to the public (when they become a victim of a major, devastating hack – our experience shows that this is usually the case for closed and secret implementations).

Third, it is impossible to verify if vulnerabilities found in SIM cards have been actually fixed (and if so, if they have been fixed properly).

As a result, it is impossible to say anything about the state of security of a target SIM card product. It is impossible to say anything about vendor's QA and security processes either. As such, SIM card security should be perceived in terms of a "security through obscurity".

THE QUESTIONNAIRE

The questions below should be treated as guidelines for 3rd parties sharing similar security concerns about SIM cards as we do. This especially, concerns telecom and government actors which are responsible for the privacy and security of whole societies or nations.

We believe these questions are worth to ask any SIM card vendor at any time (not necessarily prior to making a decision about the purchase of a given SIM card product). The answers may help evaluate the quality of products and security processes of the vendor. They can potentially reveal SIM card vendors that do a questionable job in the security area too.

The questions:

1. Is information about security vulnerabilities affecting your SIM card products (security advisories, security bulletins) available to the public ?
2. Is information about security fixes available for your SIM card products available to the public ?
3. Do you notify your customers about all security vulnerabilities found in your products of which your company was made aware of ?
4. Do you always fix all security vulnerabilities found in your SIM cards ?
5. Do you allow unfixed SIM cards (SIM cards vulnerable to security issues) to be present in the field ? If so, are your customers (such as MNOs) always made aware of that ?
6. Can independent 3rd parties (such as security companies) purchase SIM card samples from your end without any restrictions (such as without the requirement for NDA, minimum volume purchase, etc.) in order to conduct their independent security evaluation ? If no, what are your concerns ? How these concerns fit your security claims ?
7. Can you provide statistic data from the last 5 years period regarding the number of security vulnerabilities found and fixed in your SIM card products ? The statistics data is understood as data per each year consisting of the following:
   a) product name / model (optionally version)

b) the number of security issues found internally (by the SIM card vendor's security / engineering team)
c) the number of security issues found externally (by 3rd parties and SIM card vendor's contractor)
d) the impact of the issues, which should distinguish between the following:
    - unauthorized card access (access to card memory or its secrets)
    - code execution access (execution of code on the card)
    - privilege elevation access (elevation of privileges for the code running on the card such as Java VM)
    - remote card access (compromise of the card from the network)
    - full chains (complete card compromise from the remote)

SAMPLE QUESTIONAIRE TEMPLATE

PRODUCT	SOURCE	IMPACT	2019	2020	2021	2022	2023
Product name	*Internal issues*	*Card access*					
		Code exec					
		Priv elevation					
		Remote					
		Full chain					
	External issues	*Card access*					
		Code exec					
		Priv elevation					
		Remote					
		Full chain					

Additionally, the following could be taken into account in case some concerns arise:

e) the prerequisites for the issues, which should take into account the following:
    - physical SIM card access (attack through ISO-7816 command interface)
    - close proximity (attack through NFC interface)
    - network actor (attack conducted by any user of the mobile network)
    - rogue operator (attack limited to the operator)
f) fixing status
    - fixed in SIM card SW
    - impossible to fix in SIM card SW, fixed only through mitigation
    - not fixed
g) technical details of the vulnerability along Proof of Concept code[2] for threat and/or vendor's fix evaluation (whether the fix is complete / has been done properly).

[2] Such access shouldn't constitute a problem due to the usual NDA covering any information / material exchanged between SIM card vendor and a target customer (such as MNO).

SECURITY RESEARCH

REFERENCES

[1] Thales Security Center
https://supportportal.thalesgroup.com/csm?id=security_center_home_page

[2] IDEMIA Vulnerability information
https://www.idemia.com/vulnerability-information

[3] Common Criteria
https://commoncriteriaportal.org/

[4] Gemalto presents the findings of its investigations into the alleged hacking of SIM card encryption keys by Britain's Government Communications Headquarters (GCHQ) and the U.S. National Security Agency (NSA)
https://www.thalesgroup.com/en/markets/digital-identity-and-security/press-release/gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-sim-card-encryption-keys

[5] Java Card project – FAQ
https://security-explorations.com/java-card.html#faq

[6] "Security vulnerabilities of Digital Video Broadcast chipsets" (slide 17)
https://security-explorations.com/materials/se-2011-01-hitb2.pdf