SECURITY RESEARCH

IDEMIA EXCHANGE

On trust and certifications

This document contains excerpts from a follow up e-mail conversation[1] with IDEMIA representative around the following question asked during Java Card Forum Webinar in 2023:

From a point of view of a person that has significant experience in discovering real life vulnerabilities in Java card and SIM cards, I am afraid all those certifications (CC or ENISA) do not matter. While vendors might pass or follow various certifications (such as CC or ENISA) this will not do the magic and will not make their products immune to hacks.

Certification scheme doesn't exclude flaws at the implementation and even design level (unknown attacks).

The key problem is with the vendors themselves. SIM / UICC card security relies on a security through obscurity scheme. As such, no information is available for any SIM card vendor regarding security vulnerabilities that got fixed in their cards / to which their cards were affected. No card samples are available for security companies to conduct independent evaluations (my experience).

This alone creates a false illusion of security. This also limits innovation for better security (response to newly discovered attacks).

On what basis should customers (MNOs, GOVs) trust that SIM / UICC are secure ? IMHO certifications are not enough and do not matter with current closed approach to security by vendors.

[1] with original text preserved and only occasional spelling errors corrected

From IDEMIA to AGSR (Nov 02, 2023, 09:57)

As I understand, one part of your statement / question is, that certification does not provide guaranteed security. And here I believe I answered this question.

On the part of your question or more request to get more information about security countermeasures, I must state, that no manufacturer will provide this in detail, as this is the core of the knowledge of a company providing secure products.

Then, there are also different aspects and it is not clear to me to which of these your statement refers. I mean, on the one side there are the algorithms and cryptographic functions that are specified. Meanwhile all of these that are used in 5G systems are public algorithms. If there are any vulnerabilities to these algorithms or crypto functions, these are normally also made public (e.g. publications) or e.g. made to be known by Vulnerability Disclosure Programs e.g. to GSMA.

Certification can just provide a proof of that all the measures being known to be necessary to fulfill the requirements of the certification program are fulfilled.

I hope that these answers do better respond to your questions / statements.

From AGSR to IDEMIA (Nov 02, 2023, 10:55)

I personally do not trust any of the certifications or claims made by any of the SW / HW vendor by default. This is based on 28 years of experience gained while investigating security of various (mostly closed source) products (including certified).

Certifications are more about checking whether when building a house you put the doors / windows in right places, have a good (safe) plan for electricity and gas installation, etc.

These are like checklists, and do not get under the hood...

The implementation is where the devil lies. Let me bring the case of crypto as I know SIM card vendors tend to stick to crypto as a panacea for everything...

I once read some nice summary about it. It is expected that only a small percentage (actually a few) of the world's crypto-experts can implement the crypto they perfectly understand in code in a secure way. There are so many cases one can mess when writing crypto code (overflows, insecure RNGs, padding, oracles, etc.).

Let me also clarify. I do not expect any SIM / UICC card vendor to provide details of the security measures used. I got methods to find these on my own (see 2). I would however expect a vendor to:

1) publish information about fixed vulnerabilities and the strength of introducing new countermeasures. Please, note that no details are needed, it is sufficient to say that given products were affected to either DoS, local privilege elevation or a remote attack.

   Such an information provides a better perspective on the real life security of a target product though (existing / future customers can immediately evaluate quality of your processes, how many bugs and of what impact get missed during internal evaluations, etc.). No information provides the illusion that your product is bullet-proof (which I expect is not true).
2) not be afraid of having an independent security company evaluate its stuff. If you are, this basically immediately carries the following message:
   a) we are not confident of the security of our product,
   b) we base the security of the product on secrecy (security through obscurity). Please, note that security through obscurity is different from having security of a product being based on a secret crypto key. One can have complete knowledge of a product operation and algorithms used (such as in SSL / TLS). In security through obscurity you base security of the product on a belief that it is bullet-proof because:
      - the outside world doesn't know how it works (the implementation is secret),
      - the algorithms are secret.

IMHO the closed policy:

- limits your innovation in the area of security improvements (think about Microsoft, Intel, Apple and all the things these companies did in the security area as a response to learning about new vulnerabilities and attack techniques, I mean new security features at SW, compiler, and HW levels).
- creates false illusion of security for vendors (our product was awarded N certifications, it successfully passed M security reviews, we barely get any external vulnerability reports - we did such a great job then)
- increases the risk of a major, devastating hack (my experience is that secret implementations are riddled with security flaws).

To end this overlong message. What I mean in the context of certifications is that they cannot be perceived in terms of having a real impact on the security of your product. The progress is made elsewhere and by many other parties. The overall progress in many sciences is a sum of the contributions of various parties, in your case this contribution is artificially limited to your in-house teams and external contractors.

Finally, security through obscurity model is valid till someone shows that your card can be completely hacked from a remote. In the best case scenario it could be reported to you by some security company / researcher (you can assume some control over disclosure, have time for patching and preparing a response to media). In the worst case, you could learn about it when some massive attack is found in the wild...