SECURITY EXPLORATIONS

Gemalto Java SIM cards research

CALL FOR SUPPORT

INTRODUCTION

Security Explorations believes that Gemalto [1] SIM cards require a more in-depth and open security investigation.

The company successfully demonstrated a Java Card weakness can be used to completely compromise the environment of Gemalto SIM cards such as GemXplore3G and 3G USIMERA Prime. The company devised a novel method to read complete memory (256KB of FLASH and 384KB of ROM) of GemXplore3G card with the use of 16-bit JCRE references. Native code execution was also demonstrated for this card regardless of the Harvard RISC architecture of the underlying Samsung CalmRISC16 processor.

Yet, Gemalto referred to reported issue as potentially impacting Gemalto products and concludes it is "not applicable to products used in compliance with their user guidelines" [2].

Initial security analysis conducted with respect to GemXplore3G SIM card revealed several instances of preinstalled, proprietary SIM Toolkit applications from Gemalto with a dangerous functionality. At least one of them can be used for unauthenticated, over-the-air loading of arbitrary Java applet code into the SIM. Proper vulnerability report describing this (Issue 34) was submitted to Gemalto.

Additionally, SIM Toolkit security settings seem to be relying on the presence of some files (directly affecting STK MSL and signature checking).

In that context and with respect to Gemalto response received, we have reasons to suspect that security of Gemalto cards may rely on secrecy of the implementation (and secrecy of the keys), rather than quality and security of code ("*security through obscurity*"). Our experience with SAT TV ecosystem and "secure" STMicroelectronics chipsets (all broken to pieces in 2012 [3] and 2018 [4], all relying on secrecy of implementation for security of PayTV content) make us believe same situation may apply in Gemalto case.

The above makes independent security evaluation of Gemalto products even more important taking into account their wide market share.

At this point, Security Explorations is however unable to complete the project without external support.

SECURITY
EXPLORATIONS

CALL FOR SUPPORT

Security Explorations would like to proceed with the project aimed at an in-depth security analysis of Gemalto Java SIM cards.

The company offers the following sponsor packages to companies / organizations interested in Gemalto Java SIM cards research:

- *Platinum sponsor* (50K EUR)
- *Gold sponsor* (20K EUR)
- *Silver sponsor* (10K EUR)
- *Bronze sponsor* (5K EUR)

The following benefits are associated with all sponsor packages:

1) the name of the supporting company / organization is to be present in a dedicated Sponsors section of our Java Card research project (it can be anonymous if requested)
2) the name of the supporting company / organization is to be present in a dedicated Sponsors section of a technical report containing the results of the research that is made available to the public (it can be anonymous if requested)
3) exclusive access to the results of Gemalto SIM cards' research (technical report and associated Proof of Concept codes and tools) for 1 month before its public release.

The following benefits are available exclusively for *Platinum Sponsors*:

1) selection of a target Gemalto Java SIM card to analyze (the first *Platinum Sponsor* only, target card samples and associated keys might need to be provided by a Sponsor if not available in our cards repository),
2) reporting on the current progress of Gemalto Java SIM cards' research every two months.

Project goal

The goal of the project is to obtain more information about implementation, internals, security level and vulnerabilities pertaining to Gemalto Java based SIM cards.

As part of the research, the following analyses are planned to be conducted with respect to selected (we assume 2-3 of them) Gemalto Java based SIM cards (upon successful Java Card VM compromise and card's memory extraction):

- reverse engineering of card's internals
- verification if any remote (exploitable over the air / contactless interface) vulnerabilities could be found in various interfaces implemented by a card
- verification if any unpublished / dangerous APDU commands are implemented by a card
- verification if any unpublished / dangerous applications are preinstalled on a card
- verification if any "local" vulnerabilities could be found that would make it possible to gain access / install backdoor code onto a card upon physical access to it (while the card / phone is left unattended)
- verification if any backdoor like functionality was built into a card

- verification if any configuration / file system settings can jeopardize card's security
- verification of a feasibility to implement a stealth and persistent backdoor code in the environment of a specific card (such as SIM)

Deliverables

The following deliverable will be released to the public upon project completion:

- a technical report presenting the results of the security evaluation (details of all successful attack scenarios and weaknesses found),
- source and binary codes for any Proof of Concept codes and tools developed during the evaluation.

Please, refer to the research [5] section of our portal such as the one corresponding to NC+ SAT TV [4] project in order to get a better feel of the quality and nature of the deliverables we provide.

All project deliverables are to be published on Security Explorations' web pages dedicated to Java Card security (*Details* section).

Gemalto participation

Please, note that in order to provide unbiased and independent security analysis it would be natural to exclude Gemalto from this Call for Support. However, it would go against our core values to treat all vendors the same.

That said, Gemalto is always welcome to participate as long as the company sees a value in our proposal and accepts the usual non-commercial projects' rules (all project results to be released to the public).

Constraints

The Call for Support is valid till:	Apr 30 2019
The minimum funding required for the project to launch:	50K EUR
Project timeline and duration:	May 2019-May 2020 (12 months)

REFERENCES

[1] Gemalto
https://www.gemalto.com/

[2] Java Card project, Vendors status
http://www.security-explorations.com/javacard_vendors.html

[3] Security vulnerabilities of Digital Video Broadcast chipsets
http://www.security-explorations.com/materials/se-2011-01-hitb2.pdf

[4] SRP-2018-02 Exploitation Framework for STMicroelectronics DVB chipsets
http://www.security-explorations.com/ncplus_sat_general_info.html

[5] Security Explorations Research
http://www.security-explorations.com/research.html

About Security Explorations

Security Explorations (http://www.security-explorations.com) is a security company from Poland, providing various services in the area of security and vulnerability research. The company came to life as a result of a true passion of its founder for breaking security of things and analyzing software for security defects. Adam Gowdiak is the company's founder and its CEO. Adam is an experienced Java Virtual Machine hacker, with over 100 security issues uncovered in the Java technology over the recent years. He is also the Argus Hacking Contest co-winner and the man who has put Microsoft Windows to its knees (the original discoverer of MS03-026 / MS Blaster worm bug). He was also the first expert to present a successful and widespread attack against mobile Java platform in 2004.