SECURITY RESEARCH PROGRAM

FREQUENTLY ASKED QUESTION

Last update: 30 Jan 2019

Why did you decide to launch SRP Program ?

For nearly 10 years, we refrained from commercializing the results of our security research. During that time, all of our own security investigation efforts have been done completely for free [1]. We shared our findings with vendors and contributed them to the public. We neither sold, nor provided any vulnerability information or Proof of Concept codes to anyone else prior to the public release. This in particular concerns, but is not limited to various nation states, defense contractors acting on their behalf or security vulnerability brokers.

SRP Program was born as a result of our observations of the changes and directions of vulnerability research and information security markets, inquiries from customers and 3rd parties along with our own experiences with various SW and HW vendors.

Does it mean that vendors of affected technologies do not have any choice than to pay you for vulnerability information ?

Vendors of affected technologies can either purchase access to our research material (SRP AO), acquire exclusive ownership rights to it (SRP EP) or they can completely ignore SRP and instead intensify their efforts aimed at improvement of the security of their products. While the latter does not warrant that vulnerabilities or exploitation techniques targeted by SRP get found or remediated, the net effect should be always positive: a vendor putting additional resources into security / new weaknesses being discovered and fixed / flawed products being recalled / replaced from the market.

This goes along our mission of bringing security research to a new level and continuously challenging SW / HW vendors, so that security of their products gets improved.

It's important to note that an introduction of SRP will not affect our Pro Bono mission. Security Explorations will continue its non-commercial security research and contribution to the field. This means that for our Pro Bono research, vendors will still receive vulnerability information and Proof of Concept codes completely for free (SRP is meant to fund our Pro Bono mission, so that we do not need to rely on SW / HW vendors for it).

Why did you decide to include STMicroelectronics tools as part of SRP ?

For the last 6 years, Security Explorations has been doing a courtesy to STMicroelectronics and a whole PayTV industry:

- the tools developed as part of SE-2011-01 project [2] have not been published,

- these tools have never been disclosed to any 3rd party,
- Security Explorations has never assisted any suspicious 3rd party (such as from a PayTV piracy scene) in the work aimed to reverse engineer ST DVB chipsets.

Regardless of the above:

- STMicroelectronics did not bother to provide us with any impact or status information regarding the addressing of the vulnerabilities found in their hardware [3] (no response to an inquiry from 11-Apr-2017) [4], this is in high contrast to major CPU vendors' response such as AMD, ARM or Intel to Spectre and Meltdown CPU flaws [5][6][7],
- the SAT TV operator (ITI Neovision) and set-top-box vendor (Advanced Digital Broadcast) have never responded to our inquiries regarding status updates / results of the analysis, they stopped responding to our messages a month following the reporting of the issues in 2012 [4],
- we have reasons to believe that PayTV industry did little to address the issues (as of 2018, vulnerable chipsets are still present in the field - STi7100 and STi7111 are main chipsets of "the refurbished" ITI-5800S, ITI-5800SX, ITI-2849ST and ITI-2850ST set-top-boxes that NC+ offers to its customers along the new boxes) and that the costs of vulnerable set-top-box devices' replacement are subsidized by an end user (a customer of a digital SAT TV paying a monthly fee for a new STB) [8][10].

Following on the above and our past experiences with the PayTV ecosystem (summary words of this paper [9]), we decided to challenge the PayTV industry that in our opinion:

- has been acting below the standards and in an indecent manner (avoiding the costs related to the replacement of vulnerable ST chipsets, pushing the costs to the user side),
- has been jeopardizing with full consent and for many years the requirements for high security of premium content expected by leading content providers, producers and Hollywood industry in particular (just to mention HBO),
- has been likely hiding from content providers, producers and Hollywood industry the fact that STBs with inadequate security level are still present in the field,
- has likely contributed to significant losses of the PayTV industry itself as industry's own negligence might have been the enabling factor for PayTV piracy.

What's so special about SRP-2018-02 Exploitation Framework for STMicroelectronics DVB chipsets ?

The framework and accompanying tools are key to both learning and discovering the operation of proprietary SlimCORE and TKD crypto cores of STi7111 DVB chipset. They are also crucial for a successful testing and exploitation of their security vulnerabilities.

The framework and accompanying tools already proved their usefulness as they were used to discover the new ST chipset design vulnerability (SRP-2018-02 Issue 7).

Where can SlimCORE processor be found ?

We know for sure that it is used by STi7111 SoCs to handle TKD Crypto core. It could be used by the whole Gen-2 of STMicroelectronics' STB H.264 chipsets though (the generation STi7111 is part of).

According to public sources, SlimCORE processor is the basis for various pieces of IP in STi chipsets [12]. For example, Flexible and Direct Memory Access (FDMA) controller is a slim core CPU with a dedicated firmware, which can be found in STi5197, STi5206, STi7100, STi7109c2, STi7109c3, STi7105, STi7111, STi7141 and STi7200 SoCs [14]. Additionally, Orly family of set-top-box SoCs such as STiH407 and STiH416 make use of a SlimCORE processor [13].

Who might benefit from getting access to SRP-2018-02 ?

ST DVB chipsets framework and reverse engineering tools might be helpful for companies and organizations willing to:

- verify the presence of vulnerabilities in target chipsets (specific models, chip cuts, customer modes, fuses configurations, etc.),
- verify the operation of vendor's patches and protection measures, develop custom patches and protection measures,
- proceed with further investigation of ST DVB chipsets security (such as SCK key extraction, STiH237 CARDIFF chip, other chipsets generations). There are still some ideas pertaining to TKD crypto core operation that are worth checking (potential vulnerabilities described in SRP-2018-01 technical paper).

Additionally, the material might be useful for parties considering to file a lawsuit against STMicroelectronics or a set-top-box vendor over the issues discovered in ST DVB chipsets (the material can be used as a supporting evidence in any legal claims filed against vendors to cover costs / repair damages occurred due to vulnerabilities). The latter seems to be a viable option considering that Intel faces 30+ lawsuits over security issues discovered in its CPUs [11].

What are the benefits of Exclusive Purchase (EP) ?

The party acquiring exclusive ownership and intellectual property rights to a given SRP material becomes the sole owner of it. As a result:

- no further sales nor disclosure to other parties is possible by Security Explorations,
- no further use of the information contained in a given SRP material is possible by Security Explorations (no further research or publication making use of or based on it is possible),
- all copies of the material along any accompanying Proof of Concept codes and tools are destroyed by Security Explorations (upon providing SRP material to the party acquiring exclusive ownership and intellectual property rights).

How do you make sure that the tools do not help PayTV pirates ?

The license terms of our SRP material forbid to use it for any criminal purposes that would violate any domestic or international laws.

We have no means to control whether these license terms are broken or not. If this is the case, the PayTV industry can:

- consider implementing Security Explorations' original idea for a rouge subscriber detection / deactivation at content distribution level [9],
- use its Intelligence, Anti-Piracy & Forensics resources along technical means (watermarking solutions, etc.) to fight PayTV piracy.

We would want to have a look at your findings and assess them prior to the purchase (e.g. through a meeting with our engineers). Could we imagine having one of our experts look at your work results to have a better idea ?

The AO price is exactly for the ability to have a look at our findings, evaluate and use them according to the license terms. We do not provide the results of our commercial security research for free.

What's the impact of SRP-2018-02 research ?

The impact of SRP-2018-02 research material is the following:

- it again exposes inadequate security level of ADB set-top-box devices [15][16]. Regardless of Security Explorations recommendation [17], security of investigated ADB set-top-boxes has not been hardened / improved much beyond the addressing of the issues reported 6 years ago,
- it proves that NC+ platform still relies on and has in its offer set-top-box devices vulnerable to STMicroelectronics flaws. This is in contrary to the requirements of the agreements signed by the operator with various providers of a premium PayTV content [10],
- it makes it possible to gain access to vulnerable set-top-box device (accompanying the material) and research security of SlimCORE / TKD Crypto cores of STi7111 DVB chipset in the environment of a real-life digital satellite TV platform (NC+),
- it proves that there are more security issues affecting STi7111 chipset such as the new design vulnerability (SRP-2018-02 Issue 7),
- the vulnerabilities found give the potential to investigate security of other ADB set-top-boxes such as those based on STiH237 CARDIFF chipset for Nagra / Conax CAS implementation,

What devices are vulnerable to SRP-2018-02 issues ?

The Proof of Concept code and the Exploitation Framework for STMicroelectronics DVB chipsets were verified to work in the environment of ITI-2849ST, ITI-2850ST and ITI-2851S devices.

We would not be surprised to learn that other ADB satellite / cable TV set-top-boxes devices such as ITI-3740SX from NC+ or TNR-2850ST used by Canal Digital in Scandinavia are also vulnerable though.

I can't find any information about your successful hacks of ADB and NC+ (Multiroom, set-to-boxes, etc.) in any Polish media. What's the reason for that ?

While in 2012, some Polish media outlets found it interesting that we successfully broke security of a major digital SAT TV provider in Poland, this was not the case in 2018. This is regardless of the fact that some media outlets such as SAT Kurier [18] have been informed about the following:

- the correlation of the announcement of STB replacement by NC+ operator with the availability of reverse engineering tools for ST chipsets, the fact that NC+ subscribers partially subsidize the replacement costs of set-top-box devices vulnerable to ST flaws (Jan 2018)
- the security bypass of a Multiroom service of NC+, the negligence of a set-to-box vendor to fix the issues from 2012 (Feb 2018),

- complete security bypass of NC+ devices, proving that NC+ operator relies on vulnerable chipsets 6 years following the disclosure and contrary to the security requirements of the agreements signed with content providers (Jun 2018),
- publication of a 120+ pages report exposing insecurities of NC+ SAT TV platform along associated risks to NC+ subscribers such as abuse of their subscriptions for unauthorized NC+ GO access / unauthorized ordering of VOD movies and collections (Jan 2019).

SAT Kurier informed us that it avoids "hack" related topics due to the fact that their portal is visited by many subscribers of SAT TV platforms and publication about possible ways to circumvent security would promote SAT TV Piracy.

The problem with that point of view is that by ignoring topics related to the abuse, negligence and incompetence of a SAT TV industry, the media automatically put themselves on a one side of the equation[1].

If the whole IT / tech media industry had adopted such an approach, we could hardly learn about security vulnerabilities in a fear this would promote "hacking", OS / web browser vendors would not feel the pressure to patch these issues, inform the public about the fixes and do anything to improve security of their systems. They would enjoy the comfort of a SAT TV ecosystem.

Why did you decide to publish SRP-2018-01 material ?

The release of SRP-2018-01 is a direct consequence of the following:

1) no response to our inquiries regarding the impact of ST issues from a SAT TV ecosystem (STMicroelectronics, NC+, Canal+, Vivendi),
2) no will to provide assistance to obtain information pertaining to the impact and addressing of the issues from STMicroelectronics, we asked for help CERT-FR (French governmental CSIRT), IT-CERT (CERT Nazionale Italia) and US-CERT (US government CERT), but all of them stopped responding to our messages,
3) a statement received from a major vendor in a SAT TV CAS / security field indicating that its "goal is to remove the marketplace from our materials",
4) us completely breaking security of ADB set-top-boxes in use by NC+ SAT TV platform (Canal Digital makes use of same boxes) and gaining access to vulnerable ST chipsets again (we verified that 6 years following the disclosure Canal+ owned NC+ still relies on / offers to customers STBs vulnerable to ST flaws, which likely violates security requirements of agreements signed with various content providers).

What's included as part of a commercially available SRP-2018-02 material ?

The complete version of SRP-2018-02 report includes nearly 30 pages dedicated solely to the new ST issue. Among other things, it contains detailed technical description of the vulnerability, its origin and exploitation technique along detailed explanation of an exploit code implementation.

[1] in a period of 2018-02-19 to 2018-06-26, SAT Kurier published 20 news articles related to a fight with SAT TV piracy, but none regarding insecurities of ADB / NC+ set-top-box devices making PayTV piracy possible.

The report is accompanied by source and binary codes for a Proof of Concept Code exploiting vulnerabilities for STB and STi7111 chipset access (for ITI-2849ST, ITI2850ST and ITI2851S set-top-boxes). This includes an exploit code for the new ST vulnerability.

Finally, source and binary codes for the 2 tools described in SRP-2018-02 report (Compiler Stubs Generator and SlimCORE assembler) are also included as part of a commercially available SRP-2018-02 material.

Why do you claim SRP-2018-02 Issue 7 is a design vulnerability ?

Because, it's related to the design of STi7111 chipset. The detailed reasoning behind this thesis is included in the report.

Can SRP-2018-02 Issue 7 be fixed ?

It probably cannot be fixed due to the origin of the vulnerability (chip design issue). It could be only mitigated.

Can other ST chipsets be vulnerable to it ?

We would not be surprised if this was the case. STi7111 alone is available in many variants and there are other ST chipsets (including chipsets of other manufacturers) that could follow the same flawed chip design.

How do I know that the new ST chipset vulnerability is real ?

Here is a proof for that:

```
- chip id                   21933b24
- encrypted CWPK            1a ef 59 70 90 0d 45 30 3a d0 73 43 4b 8c 44 99
- plaintext CWPK            8f 19 2c 5d 97 54 d0 34 6b f4 7c 98 64 3d 79 3d
```

NC+ SAT TV operator can confirm that the above corresponds to the plaintext value of CWPK in use by STi7111 chipset of ITI-2851S set-top-box device indicated by a given chip id.

REFERENCES

[1] Security Explorations in a Nutshell
http://www.security-explorations.com/materials/se-nutshell.pdf

[2] SE-2011-01 Security weaknesses in a digital satellite TV platform
http://www.security-explorations.com/tv_platform_general_info.html

[3] SE-2011-01 Issues #17-19
http://www.security-explorations.com/materials/se-2011-01-st.pdf

[4] SE-2011-01 Vendors status
http://www.security-explorations.com/tv_platform_vendors.html

[5] Arm Processor Security Update
https://developer.arm.com/support/security-update

[6] AMD Processors: Google Project Zero, Spectre and Meltdown
`https://www.amd.com/en/corporate/speculative-execution`

[7] Speculative Execution and Indirect Branch Prediction Side Channel Analysis Method
`https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr`

[8] WYMIEŃ SWÓJ DEKODER NA NOWY!
`http://ncplus.pl/wymiana-dekodera`

[9] Ideas regarding vulnerabilities in ST DVB chipsets
`http://www.security-explorations.com/materials/se-2011-01_ideas.pdf`

[10] Screenshot of NC+ operator web page advertising STB replacement to a new model
`http://www.security-explorations.com/materials/ncplus_screenshot.png`

[11] Intel hit with 32 lawsuits over security flaws
`https://www.reuters.com/article/us-cyber-intel-lawsuit/intel-hit-with-32-lawsuits-over-security-flaws-idUSKCN1G01KX`

[12] Add support for FDMA DMA controller and slim core rproc found on STi chipsets
`https://lwn.net/Articles/690158/`

[13] Debugging Embedded Multimedia Application Execution Traces through Periodic Pattern Mining, Patricia L´opez Cueva
`http://www.theses.fr/2013GRENM029.pdf`

[14] STLinux, Linux 2.6.32 kernel source code (linux-2.6.32.10_stm24_sh4_0201.patch)
`http://stlinux.com`

[15] SE-2011-01 Issues #5-16,#25-32
`http://www.security-explorations.com/materials/se-2011-01-adb.pdf`

[16] NC+ Multiroom service bypass
`http://www.security-explorations.com/materials/se-2011-01-33.pdf`

[17] Security vulnerabilities of Digital Video Broadcast chipsets, slide 73
`http://www.security-explorations.com/materials/se-2011-01-hitb2.pdf`

[18] SAT Kurier
`http://www.satkurier.pl`