THE ORIGIN AND IMPACT OF SECURITY VULNERABILITIES IN ST CHIPSETS

SE-2011-01

[Security weaknesses in a digital satellite TV platform]

Last update: 20 Apr 2018

DISCLAIMER

INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW NEITHER SECURITY EXPLORATIONS, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE INFORMATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS, OR OTHER RIGHTS. THERE IS NO WARRANTY BY SECURITY EXPLORATIONS OR BY ANY OTHER PARTY THAT THE INFORMATION CONTAINED IN THE THIS DOCUMENT WILL MEET YOUR REQUIREMENTS OR THAT IT WILL BE ERROR-FREE.

YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION AND USE OF THE INFORMATION TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE INSTALLATION, USE, AND RESULTS OBTAINED FROM IT.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL SECURITY EXPLORATIONS, ITS EMPLOYEES OR LICENSORS OR AFFILIATES BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA, OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION, OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE, OR OTHER THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE INFORMATION CONTAINED IN THIS DOCUMENT, EVEN IF SECURITY EXPLORATIONS OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS.

INTRODUCTION

This document presents information related to security vulnerabilities discovered by Security Explorations in STMicroelectronics' chipsets [1][2].

Its goal is to provide all interested parties (chipset / set-top-box / CAS vendors and security researchers in particular) with a summary information pertaining to the origin and impact of the weaknesses found in ST SoC processors.

These vulnerabilities are still a mystery to many and we keep receiving inquiries about them regardless of the fact that almost 6 years had passed since the disclosure. STMicroelectronics, although out of set-top-box and DVB chipset business [3], has not provided us with any details regarding the impact of the issues found [4].

We have reasons to believe that vulnerable IP (TKD Crypto core of STi7111 SoC) might be part of other ST chipsets and/or part of other vendors' solutions, not necessarily related to PayTV industry (e-passports, banking cards and SIM cards).

We have reasons to believe that ST actions were aimed to hide the impact of the issues found, that company's shareholders were not aware of these vulnerabilities, their impact and associated liabilities. We have reasons to believe that the issues have not been resolved up to this day.

This document is a work in progress. As such, it will be updated once new information is acquired regarding the impact of the issues found in ST chipsets.

GENERIC IMPACT FOR PAY TV INDUSTRY AND CAS VENDORS

Security Explorations discovered several security weaknesses in the implementation of the chipset pairing functionality used in set-top-box devices. We discovered that for STi7100 / STI7111 DVB chipsets, it is possible to extract plaintext values of Control Word cryptographic keys - the keys that protect security of content in a digital satellite TV system. For STi7111 DVB chipset, we also discovered a way to extract the plaintext value of the pairing key itself. By doing so, we broke security of the pairing function and the cryptographic relationship between a subscriber's smartcard and a set-top-box' DVB chipset.

Chipset pairing technology was invented to protect against hacking satellite TV. Chipset pairing uniquely ties a given subscriber's smartcard with a corresponding set-top-box equipment. The pairing has a form of a cryptographic function. It is usually implemented in a silicon (DVB chipset). The goal of the latter is to prevent set-top-box hijacking and unauthorized sharing / distribution of a satellite TV programming.

The implementation of many modern CAS systems that are in use by PayTV industry is based on the idea of a Key Ladder [5] for chipset pairing functionality. Although the date of a datasheet for STi7111 SoC (2007) precedes the date of the Key Ladder specification (2010), we still find the latter helpful for describing the likely cause of ST flaws (the base security principles described in the spec hold for STi7111 SoC).

Key Ladder is a functional block implemented by a secure chipset such as STi7111. It makes it possible to securely deliver descrambling keys (Control Words) to the target set-to-box device as illustrated on Fig. 1.

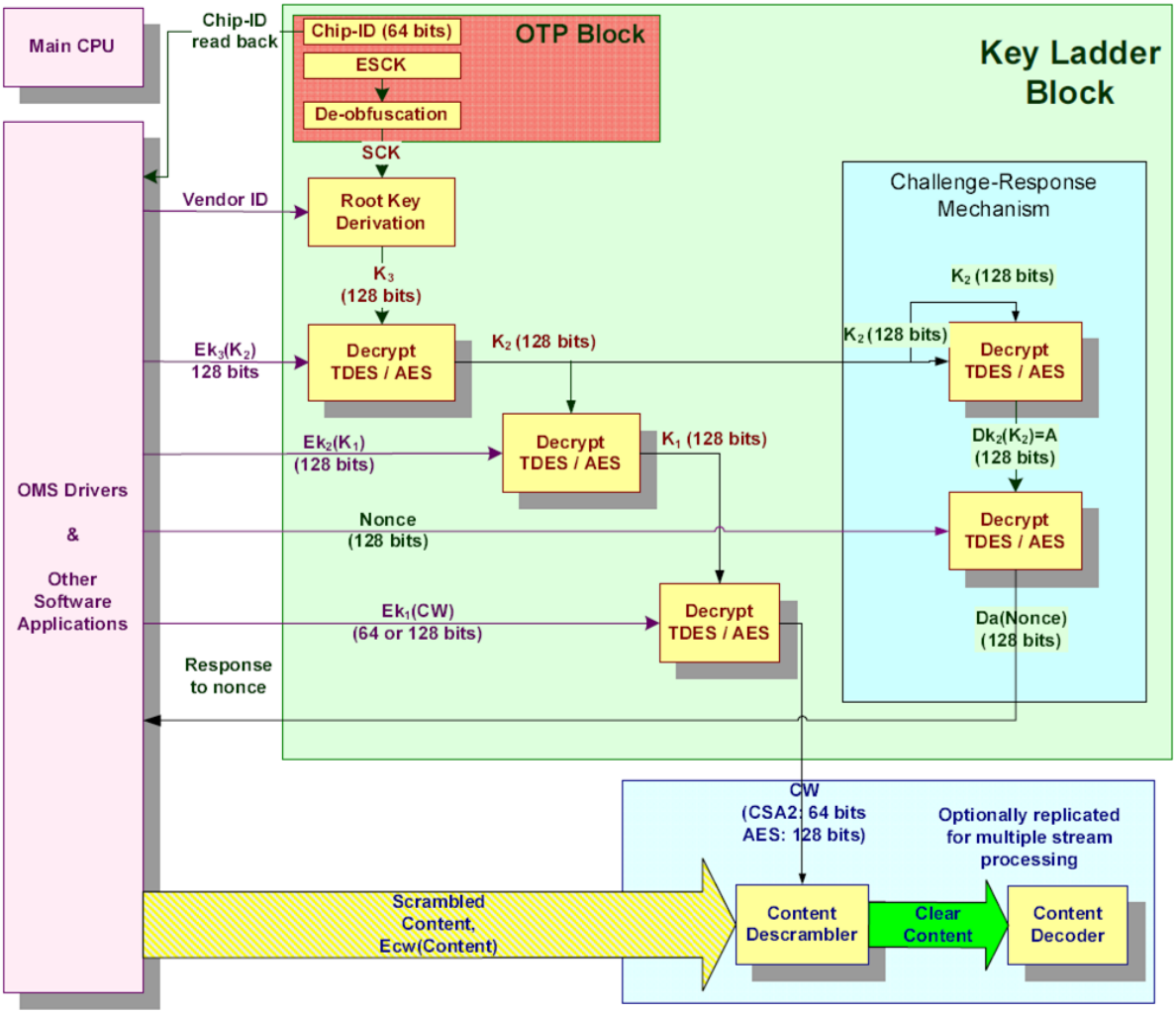

Image source: ETSI TS 103 162 V1.1.1 (2010-10)

Fig. 1 Key Ladder functional diagram (the case for 2 pairing keys).

Each chipset contains a unique secret SCK key. It is used directly (or indirectly by the means of a derived root key K3) to decrypt encrypted (and unique to each chipset) value of key K2. This key is further used to obtain a plaintext value of any other pairing key as they form a ladder like structure (key *Kn+1* is used to decrypt the value of key *Kn*). The final key (such as K1) is used to decrypt the encrypted Control Words. These are further used to obtain descrambled A/V content.

For Conax CAS [6], the following holds:

- K3 is likely the SCK key itself,
- K2 is the pairing key (CWPK),
- K1 equals K2 (there is only one pairing key for Conax CAS),
- TDES algorithm is used for decryption in the environment of NC+ operator in Poland.

For Nagra CAS [7], it seems there are more CWPK keys [8]. The number of keys used by the Key Ladder block does not seem to matter from a point of view of the exploitation of ST chipset vulnerabilities such as Issue 19. Once a plaintext value of a key higher in the Key Ladder hierarchy is obtained, all other keys below it can be decrypted. As a result, the given CAS can be successfully compromised in the environment of a vulnerable ST chipset. We have successfully proven this for Conax CAS [9].

The Key Ladder specification does seem to contain some security guidelines for the vendor willing to implement a chipset pairing functionality:

a) *The components in yellow in Fig. 1 shall all be in a single silicon chip* (fulfilled for STi7111, TKD Crypto core, OTP Block and SCK are all part of one SoC),

b) *The interface from applications that run on the CPU, even if the CPU is located on the same silicon as the key ladder, are permitted to input and output data only according to the interfaces that appear in the diagram* (not fulfilled for STi7111, the interfaces available for an application that run on SlimCORE CPU are permitted to input and output data in a manner other than according to the interfaces),

c) *The main CPU shall have absolutely no read/write access to the registers that store ESCK, SCK, Kn,…,K3, K2, K1 and A* (fulfilled for the main SH4 CPU of STi7111, but not SlimCORE CPU)

d) *There shall be write, but no read, access to CW* (not fulfilled for STi7111).

It is clear that 3 of the 4 abovementioned guidelines are violated in the environment of STi7111 SoC. While ST might have missed the weaknesses prior to the publication of the Key Ladder spec in 2010, the company should have implemented proper measures to mitigate the issues revealed by it in future SoC generations.

ORIGIN OF THE VULNERABILITIES

Issues 18 and 19 have their origin in TKD Crypto core, a hardware component of STi7111 DVB chipset SoC [10] (Fig. 2). Taking into account the nature of the flaws and the actual hardware component they affect, we conclude this is a hardware vulnerability.

As for the actual cause of the issues, the following hypotheses are considered by us among others:

1) the issues are simply implementation or configuration[1] flaws. The security of the chip did not take into account some potentially insecure combinations of source and targets for TKD commands (i.e. CWPK key being the source of / DMA key being the target of a given crypto operation). During our meeting with STMicroelectronics[2], the company indicated that its engineers did not take into account an attack conducted purely through software means as its engineers were solely focused on hardware based attacks (i.e. fault injection, glitches, side-channel, etc.),

[1] understood as configuration of security fuses.

[2] the meeting in Paris on Feb 13, 2012 attended by ST Platform Security Solution Director, Corporate System Security Roadmap and Lab Director, Product Security Group VP and Legal Affairs person.

2) the issues are the result of a possibility to use SCK key for operations different than CWPK key decryption (i.e. crypto DMA required for encrypting / decrypting FLASH memory with a chipset specific key),

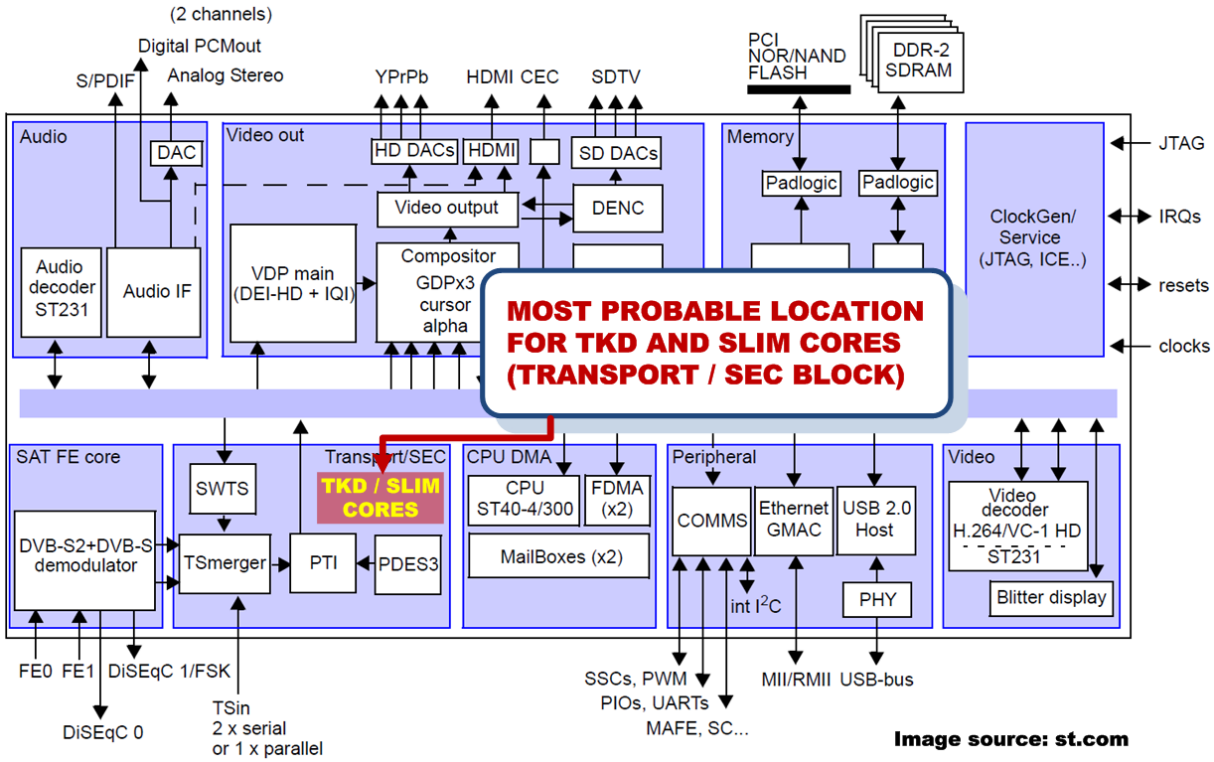

Fig. 2 STi7111 SoC architecture.

3) the issues are the result of implementing Key Ladder computation in a non-atomic fashion, Issue 19 allows to obtain CWPK key by executing 2 sequential operations (decrypt and encrypt) issued on a secret CWPK key value. The Key Ladder is shown in the specification as one block and it is solely composed of decrypt operations. Thus, it is reasonable to assume that the Key Ladder should produce an output (CWPK key) in a more atomic way (without the possibility to use any intermediate CWPK key in the middle of the computation and for any other operation than CW decryption),

4) the issues are the result of a compromise between the features of a crypto chip (generic crypto functionality vs. generic chipset pairing functionality such as a Key Ladder in particular) and/or the requirements of the Key Ladder specification itself (Nonce feature). As such ST choice might have been to provide means for implementing Key Ladder block and Nonce computation by the means of sequences of basic crypto operations (encrypt / decrypt and load key slot) issued to the crypto core from the outside.

From a perspective of a Key Ladder specification, we see a potential for similar attacks against other chipsets used in PayTV industry (Broadcom, HiSilicon, Ali). The more generic given chip's functionality and API implementing chipset pairing (Key Ladder) is, the more risk it may be vulnerable to attacks abusing sequences of specially crafted / key manipulation operations.

VULNERABLE CHIPSETS

The list of chipsets confirmed to be vulnerable to the issues found in STMicroelectronics SoCs is presented in Table 1.

VENDOR	VULNERABILITY	AFFECTED CHIPSET
STMicroelectronics http://www.st.com	Issue 17	STi7100
	Issue 18	STi7111
	Issue 19	STi7111

Table 1 Impact information.

Although the STi7111 chip alone is available in many variants [10] (STI7111-SUC, SGC7111BIUC, STI7111-LUC, STI7111BNUCT, STI7111-FUC, STI7111BFUC, STI7111-KUC, STI7111BOUC, STI7111BMUC, STI7111BHUCT, STI7111-SUCT, STI7111NUB, STI7111-NUC, STI7111-BUC, STI7111BNUC, STI7111BSUC, STI7111-KUCT, STI7111BIUC, STI7111BOUCT, STI7111BAUC, STI7111-DUC, STI7111-YUC, STI7111ZUC and STI7111BDUC), we don't know which of these models are vulnerable / which are not.

The vulnerabilities could potentially affect the whole Gen-1 (STi7100, STi7103, STi7109, STi5202) and Gen-2 (STi7104, STi7105, STi7111, STi7141, STi7200, STi5211, STi5206) of DVB chipsets from STMicroelectronics of which STi7100 and STi7111 are respective parts of. The rationale for this is that these generations share the same SoC architecture.

Additionally, as it is common to include given IP in other products of a given hardware vendor[3], vulnerable IP (TKD Crypto core of STi7111 SoC) could be part of other ST chipsets (not-related to PayTV) or chipsets from other vendors (in case of IP licensing).

RATIONALES FOR FURTHER INVESTIGATION

Over the last 20+ years, we have been dealing with various vendors and ecosystems (desktop, cloud, mobile). The case of STMicroelectronics vulnerabilities is however truly unique as we have never met with such a persistent and long-term refusal to provide information pertaining to the impact and addressing of security vulnerabilities found.

The more resistance we experience from the vendor, PayTV ecosystem and arbitrary 3rd parties regarding requests for information, the more strange and suspicious the whole case starts to look.

The above along the following rationales are an indication for us to dig further into the case of ST chipsets' vulnerabilities :

- Since 2012, ST has been persistently refusing to provide information pertaining to the impact and addressing of the issues found in its chipsets [4]

[3] SlimCORE processor is a good example o that. According to public sources, SlimCORE processor is the basis for various pieces of IP in STi chipsets [20]. 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, STi7109, STi7105, STi7111, STi7141 and STi7200 SoCs [22]. Additionally, Orly family of set-top-box SoCs such as STiH407 and STiH416 make use of a SlimCORE processor [21].

  - this is regardless of the fact that STi7111 is still an active product (product is in volume production as of Apr 20, 2018) [10],
  - this is in high contrast to major CPU vendors' response such as AMD, ARM or Intel to Spectre and Meltdown CPU flaws [11][12][13],
  - ST stance has not changed a bit even though 6 years has passed since the disclosure.
- Public sources indicated that there could be hundreds of millions of flawed chips released to the market (STMicroelectronics own sources mentioned 541 millions as the number of these chipsets released to the market in 2008, with ST market share at 68% [14]).
- As of 2018, vulnerable set-top-boxes (based on vulnerable chipsets) are still deployed in the field (just to mention NC+ operator in Poland of which French Canal+ Group holds a majority of stake).
- ST is one of the major chipset vendors in the world
  - the company delivers solutions for Wireless, Automotive, Consumer, Computer, Telecom Infrastructure and Industrial markets,
  - among ST customers there are many big companies [15], just to mention Apple, Dell, HP, Cisco, Microsoft and DirecTV,
  - vulnerable IP (TKD Crypto core of STi7111 SoC) might have been licensed and become part of other vendors' solutions, not necessarily related to PayTV industry (e-passports, banking cards and SIM cards),
  - in our WWW server logs, we have observed an interest in ST vulnerabilities from various vendors, IP addresses indicating[4] R&D of Oberthur Technologies (a major smartcard / identity card / SIM card vendor) are of a particular interest here - public sources from 2010 indicate that ST and Oberthur teamed up for NFC SIM card development [16]),
- ST tried to achieve a non-disclosure / limited disclosure of the vulnerabilities (a vague proposal of a business relationship in exchange for a limited vulnerability disclosure, carefully worded statements indicating that publication or disclosure on the process we followed to extract control word from ST devices will damage ST and other vendors in the ecosystem [17]),
- ST noted a significant net income loss at the end of 2012 (a year of the disclosure) [18],
- ST announced its exit from the STB chipsets business in 2016 [3]
- In Mar 2018, we asked CERT-FR (French governmental CSIRT) and IT-CERT (CERT Nazionale Italia) for assistance aimed at obtaining information from STMicroelectronics regarding security issues found in their chipsets (ST is a French-Italian company and both French and Italian governments hold 13.8% of its stake each). For some unknown reason, both CERTs have stopped responding to our messages. This could indicate a potential conflict of interest.

FINAL WORDS

The usual "crisis management" conducted by vendors for disclosures of high impact flaws involve carefully-worded statements indicating that the issues affect older products only or in case of low / limited impact flaws, a vendor usually publishes a list of vulnerable products to clearly emphasize the low nature of the issues found.

[4] according to `http://ip-tracker.org`.

ST refusal to provide any information pertaining to the impact of vulnerabilities found in its chipsets can be perceived in terms of intentionally hiding the impact of a much larger magnitude than anticipated by the reporting party, customers or the public. It could be that these actions are aimed at avoiding the liabilities associated with manufacturing flawed products, the costs of their recalls and/or replacements.

ST has all the means to end any speculation pertaining to the nature of the issues found in its chipsets and their impact by simply delivering clear impact information to general public (vulnerable chipset models, whether vulnerable IP is used in other products, remediation steps, etc).

Security Explorations will continue engaging various entities such as US-CERT in a goal to acquire accurate information pertaining to the impact and addressing of ST vulnerabilities. This document and our SE-2011-01 Vendor Status page [4] will reflect any new information acquired and our steps taken to obtain it.

The company is also ready to release to the public all unpublished bits pertaining to its research of ST chipsets such as SRP-2018-01 [19] material if deemed necessary.

REFERENCES

[1] "Security vulnerabilities of Digital Video Broadcast chipsets", HITB Talk#2
http://www.security-explorations.com/materials/se-2011-01-hitb2.pdf

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

[3] STMicro to exit STB chip business
https://www.broadbandtvnews.com/2016/01/27/losses-force-stmicro-to-end-stb-chip-business/

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

[5] ETSI TS 103 162 V1.1.1 (2010-10), K-LAD Functional Specification
http://www.etsi.org/deliver/etsi_ts/103100_103199/103162/01.01.01_60/ts_103162v010101p.pdf

[6] Conax CAS
http://www.conax.com

[7] Nagra CAS
https://dtv.nagra.com/secure/casdrm

[8] Post by R.e.L.o.A.D.e.D
http://www.sat-universe.com/archive/index.php?t-143361-p-3.html

[9] SE-2011-01 Proof of Concept Code
http://www.security-explorations.com/materials/se-2011-01-codes.zip

[10] STi7111, STMicroelectronics
http://www.st.com/en/digital-set-top-box-ics/sti7111.html

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

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

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

[14] Multimedia, Philippe Lambinet, STMicroelectronics
http://zxevo-files.perestoroniny.ru/datasheets/www.st.com/internet/com/CORPORATE_RESOURCES/COMPANY/COMPANY_PRESENTATION/9_breakout_multimedia_lambinet.pdf

[15] STMicroelectronics slides
http://phx.corporate-ir.net/External.File?item=UGFyZW50SUQ9NTg3MHxDaGlsZElEPS0xfFR5cGU9Mw==&t=1&usg=AOvVaw2ZPtwMnZIlgjKupUi36qMf

[16] Oberthur Technologies and STMicroelectronics Team Up for NFC(1) MIFARE DESFire™ SIM Card
https://www.prnewswire.com/news-releases/oberthur-technologies-and-stmicroelectronics-team-up-for-nfc1-mifare-desfire-sim-card-111375934.html

[17] Security Explorations - Frequently Asked Questions
http://www.security-explorations.com/materials/se-faq.pdf

[18] STMicroelectronics NV ADR
http://financials.morningstar.com/direct/ratios/r.html?t=XNYS:STM&region=usa&culture=en-US&productcode=MLE&cur=

[19] SRP-2018-01 Reverse engineering tools for ST DVB chipsets
http://www.security-explorations.com/materials/SRP-2018-01.pdf

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

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

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