An Industrial Outlook on Challenges of Hardware Security in Digital Economy—Extended Abstract—

Bhasin, Shivam; Lomné, Victor; Tobich, Karim

2017

Bhasin, S., Lomné, V., & Tobich, K. (2017). An Industrial Outlook on Challenges of Hardware Security in Digital Economy—Extended Abstract—. 2017 International Conference on Security, Privacy, and Applied Cryptography Engineering, 1-9.

https://hdl.handle.net/10356/88921

https://doi.org/10.1007/978-3-319-71501-8_1

An Industrial Outlook on Challenges of Hardware Security in Digital Economy —Extended Abstract—

Shivam Bhasin[1], Victor Lomné[2], and Karim Tobich[3]

[1] Temasek Laboratories, Nanyang Technological University, Singapore,
sbhasin@ntu.edu.sg
[2] NinjaLab, Montpellier, France,
victor@ninjalab.fr
[3] UL Transaction Security, Basingstoke, United Kingdom,
karim.tobich@ul.com

Thanks to the seminal works of Kocher on side-channel attacks [1,2] and Boneh et al. on fault injection attacks [3] in the 1990s, the domain of physical attacks has emerged as an active research domain as well as a potential threat on commercial devices. Practical hacks using physical attacks have been demonstrated on commercial products like NXP MiFare [4], KEELOQ [5], Sony PlayStation etc. The threat becomes even bigger with the emergence of the Internet of Things (IoT), digital economy and identity. Digital economy is a push towards cashless society, encouraging digital banking with use of modern payment methods based on smartcards and now smartphones. Digital identity now uses biometric data, like fingerprints, to authenticate people. Several governments are giving a push for digital economy and identity. This has lead to rapid adoption of mobile payments, cashless solutions, biometric identities. Often biometrics are linked to payment solution.

However, the deployed systems must be secure and trusted to avoid frauds and malicious exploitation. This is even more relevant now as the attackers have cyber as well as physical access to the devices (credit cards, passports, smartphones etc ...) and almost unlimited attack time (as the lifetime of banking cards and passports are of several years). The objective of this work is to give a high-level overview on how manufacturers, evaluation laboratories and certification schemes are assessing the security of such products. The overview is divided in two distinct parts: *payment solution* and *biometric passport*.

The first part will present the certification process of a Secure Element (SE) in banking evaluation context. It will start with a review of the banking transaction flow, based on a contact protocol. Then a practical banking evaluation process will be described from an evaluation lab, by giving concrete examples of assessment on some EMVCo [6,7], VISA [8] or MasterCard applications [9]. The concept of successful evaluation will be discussed as well.

The second part will present the certification process of a Common Criteria evaluation of a biometric passport. First some basics about Common Criteria certification will be given, explaining how it works, and how the different stakeholders interact with each other (manufacturer, evaluation laboratory, certification scheme). Then a concrete example of a biometric passport certification will be described, explaining the different tasks performed to assess its security.

1 A *successful* evaluation of a banking transaction

1.1 Three parties' process

To reduce the risk of bribery or corruption and keep independence between certification body and client, the industry pushed to have a three party process with the creation of evaluation labs. These labs are paid by customers to assess their products but they are under the authority and agreement of the certification body. This mean without agreement there is no work for them and without customers there is no revenue. A service based on a trust and a business to business model (B2B) became a reference, since quite a while now at least in the security domain. As a main role, the certification bodies are leading the industry by setting consortium and creating specifications and reference documents. They are assessing labs to give them the accreditation, or getting it back. They are reviewing the evaluation labs reports and guiding them about any new attack techniques that need to be used within these evaluations. The evaluation labs need to please to customers to get revenue but are watched by the certification body to do a proper assessment. They have to innovate by following the scheme recommendation but as well based on their own expertise and their own proper R&D and innovation strategy.

1.2 Banking transaction flow

As any industrial process, a strong flow was implemented and has been updated over the time to meet the market demand. The security was the main concern and is still the case over all these updates. A global view of this transaction flow is given in Fig.1 (a).

Based on the Application Data Protocol Unit (APDU) the transaction is initiated by the terminal using a set of library command (see Fig.1 (b)). This step is used to SELECT the right payment application as the card may have different ones (credit, debit ...) followed by a GET PROCESSING OPTIONS to initiate the application by incrementing the *Application Transaction counter* (ATC). This is updated for each new transaction which make it unique and secure against any replay attack. A read application data is performed by using a READ RECORD command to get all these data related to the card capabilities such as the *Primary Account Number* (PAN), the *Card Risk Management* (CRM) and other details as the *Application Interchange Profile* (AIP) that might be needed for the transaction. The INTERNAL AUTHENTICATE command initiates the computation of the Signed Dynamic Application Data to perform an Offline Data Authentication. Depending on the capabilities of the card and the terminal, a *Static Data Authentication* (SDA) or a *Dynamic Data Authentication* (DDA) or a *Combined Dynamic Data Authentication/Application Cryptogram Generation* (CDA) will be performed to authenticate the application.

Next, a processing restrictions function is performed to determine the degree of compatibility of the application in the terminal with the application in the Integrated Circuit Card (ICC) and to make any necessary adjustments, including possible rejection of the transaction. The Cardholder verification is then performed to ensure that the person presenting the ICC is the person to whom the application in the card was issued. Based on the *Cardholder Verification Methods* (CVM) the terminal will ask for a paper signature or a PIN verification by using a VERIFY command. This one can be

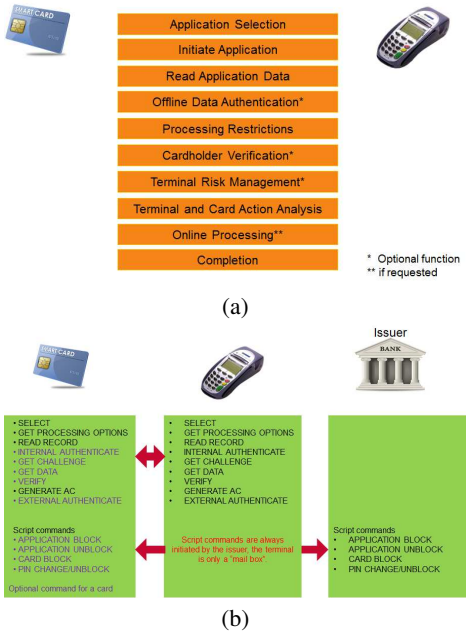

Fig. 1. (a) Transaction flow, (b) Command library

processed offline or online. A terminal risk management is then performed to ensure that transactions initiated from the ICC go online periodically to protect against threats. It consists of: A floor limits checking, a random transaction selection and usually a velocity checking. These checks will be performed by using GET DATA command.

Further, the terminal and card action analysis is performed. This starts with the terminal, which will make the first decision as to whether the transaction should be approved offline, declined offline, or transmitted online. Followed by the ICC that may decide to complete a transaction online with an *Authorisation ReQuest Cryptogram* (ARQC) or offline with a *Transaction Certificate* (TC) or reject it with an *Application Authentication Cryptogram* (AAC). This will be done by using a GENERATE AC (Application Cryptogram) command, commonly known as 1^{st} GAC. Online processing is performed to ensure the issuer can review and authorise or reject transactions that are outside acceptable limits of risk defined by the issuer, the payment system, or the acquirer. As a response the issuer may generate an *Authorisation Response Cryptogram* (ARPC) to validate the transaction. The terminal shall issue then an EXTERNAL AUTHENTICATE command to the card only if the card indicates in byte 1 bit 3 of the *Application Interchange Profile* (AIP) that it supports issuer authentication using the EXTERNAL AUTHENTICATE command. Followed by the generation of an AC using a GENERATE AC (Application Cryptogram) to complete and accept the transaction with a *Transaction Certificate* (TC) or reject it with an *Application Authentication Cryptogram* (AAC). This is usually called the 2^{nd} GAC. A completion step will be done with

a last variables update. It closes the processing of a transaction. A script processing may then be performed.

1.3 Banking evaluation process

To be able to assess deeply the security of a product, a white box evaluation is considered since few years now. Under a Non-Disclosure Agreement (NDA), an evaluation lab can have access to the code source, analyses it and highlights the finding to the customer. This can be done in the client premise or in the evaluation lab. This vulnerability analysis will lead to a list of findings and different phase of attacks. These could be classified as software attack using malwares and *Application Protocol Data Unit* (APDU) command, or more hardware and firmware attacks using side-channel attack and fault injection techniques. A combined attack regrouping software and hardware attacks could be used as well to assess the security of a product. Each command may contain different assets and each asset is associated with a level:

- A primary level is: a successful attack on the asset breaks the core security level expected from the application and may lead to harmful consequences for the payment process. Compromising a primary asset leads to a security evaluation failure.
- A secondary level is: a successful attack on the asset may expose a primary asset. Compromising a secondary asset usually leads to a specific notice in the evaluation report.

The level of these assets varies from one application to another and from one scheme to another due to their specific implementation.

To maintain a high level of security, security architects and developers need to follow different guidelines. Some are more related to the core of the security, whereas some are more related to a performance issues to balancing between security and performance.

As an example of recommendation the following could be considered as generic guidance to protect assets against software attacks, side-channel attacks and fault injection attacks:

- Every time the platform or the application is run, raise security errors upon detection of a configuration not compliant with the functional specifications.
- Every time an APDU command is received by the platform or by the application, raise security errors upon detection of parameter combinations not compliant with the functional specifications.
- When possible, implement checks to any functions that have assumptions on parameters and execution context.
- Make all operations on sensitive data independent of the sensitive data value from the attacker's perspective: timing, power consumption level / electromagnetic emanation level.
- Avoid implementing two consecutive operations on sensitive data that provide exactly the same electrical or electromagnetic behavior, such as
  - Adding random masking

    - o Involving changing parameters in calculations (such as in counters)
- Reduce freedom on chosen input format on sensitive data with values known or unknown to the attacker.
- Make time synchronization with the targeted operation difficult for the attacker.
- Cross-check every sensitive operation, such as:
    - o Redundancy
    - o Complementary checks (such as RSA verification after signature)
- Cross-check every sensitive data value (such as integrity checking)
- Cross-check program execution, such as: sequence of instructions, function calls.
- Add hidden dummy operations with random timing
- Add global random execution time of operations

The evaluation laboratories will have the mission to assess the conformity of the implementation with these security guidelines and mainly the one related to the core security. This will be done using tools and techniques which are at the state of the art. Nowadays a laboratory who hasn't got these tools or equipments can be under surveillance process and can loose its accreditation. As well as the expertise of the evaluators and their skills sets need to be considered to keep an accreditation. In fact, to keep a consensus between evaluation labs, the certification labs, scheme are setting skills matrix and job specification to define a real expert in their accredited labs. From tools perspective, the major needed one are listed by the scheme or the certification lab, the following ones can be considered as an example are a generic one. The pattern recognition tool used to detect and find targeted timing area and avoid any random jitter, the tearing card mechanism tools to interrupt the saving process of the any fault detection counters and extend the sample live time, the bandwidth frequency analyser tool to reduce the noise and distinguish operations such cryptographic operations . . . these tools are common for side-channel and fault injection attacks.

Specific benches might be used to assess a product these could be based on Electromagnetic fault injections [10], glitching using the FBBI or RBBI technique[11], some recent research highlighted the use of X-ray tools to reprogram a circuit [12], some labs may use Infrared laser or blue laser instead, but the most common goal is to fire with 3 or 4 spots as the circuits are more and more based on multi-core architecture or on hardware redundancy security mechanism. The first 2 spots will be on the targeted area and its redundancy, while the 3^{rd} one on the cross-check operation (See figure 2 [13,14]). Side-channel technique are as well used to assess the code execution leakage different attack technique are used DPA, DEMA, HO, and recently the deep learning.

1.4 Concept of *successful* evaluation

Concept of *successful* evaluation is a complex notion. In fact, as the evaluation is a three parties process, each of them will have his own goal and criteria of success. For sure the main goal will be to ensure that the product will not be hacked during its lifetime in the market. But this is an absolute goal shared by the three entities. In day to day work, the manufacture will push to spend less time on evaluation as the market is not going to wait for them. A successful evaluation will be a quick one with minor findings which will keep or set them as pioneer in the market with this product. From

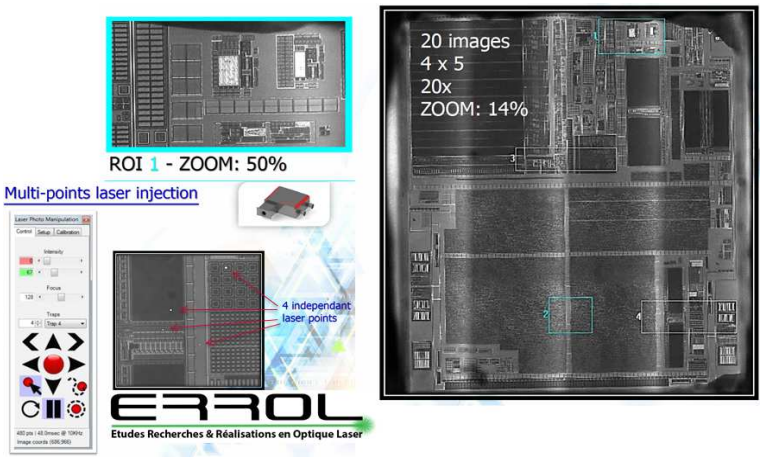

Fig. 2. Multi-Spot Laser System

an evaluation lab, a successful evaluation will be based on different findings which will induce proper break during the attack phase. These could be on primary assets or secondary assets. From a certification lab or scheme, a successful evaluation will be based on good report highlighting the findings and the patches that have been applied, along with the techniques and tools that has been used and deployed for that assessment.

2 Common Criteria Certification of a Smartcard - Application to Biometric Passport

Common Criteria is an international standard (ISO/IEC 15408) for IT products security certification. It is especially used for assessing the security of embedded devices like smartcards and similar products, e.g. biometric passport. More precisely, Common Criteria works as a framework in which:

1. Users specify their security requirements
2. Vendors implement the security requirements in their products
3. Evaluation laboratories evaluate the security of the products
4. Certification bodies certify the products security by checking the correctness of all steps

Among the key concepts, the *Target Of Evaluation* (TOE) is (a part of) the product that is the subject of the evaluation, e.g. the biometric passport and its environnment. The *Security Target* (ST) is a document that identifies the security properties of the TOE, and may refer to a *Protection Profile* (PP).

A PP is a document, typically created by a user or users community, which identifies security requirements for a class of security devices. For instance PP for biometric passport can be found at [15].

Common Criteria provides key documents defining an evaluation methodology where six different classes must be verified, each one being linked to a step of the product development or to its features. Whereas five classes check TOE conformity, one class checks the TOE security (AVA_VAN), in regards to the ST. Furthermore, for every Common Criteria certification, an *Evaluation Assurance Level* (EAL) is defined. EAL can be seen as a global rating of the classes, where each class has to reach a certain value.

For the certification of smartcards and similar devices like biometric passport, the final product usually follows several certification steps. First the security *Integrated Circuit* (IC) developed by an IC manufacturer is evaluated, in regards of the security of its hardware functionalities (e.g. CPU, RAM, non volatile memory, cryptographic co-processors, ...).

Once the security IC is certified, a smartcard vendor develops an *Operating System* (OS) and a dedicated application (in our case an biometric passport application) on top of the IC. The full product follows then a second evaluation procedure. This concept is called a composite evaluation, where an evaluation of a product relies on the certification of a part of the product.

When assessing the security of smartcards and similar products, a specific methodology has to be used [16], where several attack paths have to be considered. More precisely, physical attacks (microprobing, FIB attack, memory reading attack, ...), perturbation attacks (glitch, laser, electromagnetic injection), fault based cryptanalysis, side-channel attacks and software attacks are applied to the TOE.

When an attack is successful, its rating is computed by considering two steps:

1. Identification: effort required to imagine, develop and apply the attack to the TOE for the first time
2. Exploitation: effort required to apply the attack to the TOE by knowing the methodology developed in the identification step

An attack is divided in attack factors, allowing to evaluate the difficulty of the different attack aspects. The more an attack factor is difficult to apply, the more its rating is high. The full rating of an attack is obtained by summing the rating of all attack factors of both steps.

If one successful attack has a rating higher than the one defined by the EAL the TOE has to reach, then the evaluation is not successful. In this case, the developer can patch its product, and the evaluation laboratory has to perform once again the attack to check that the patch corrects the vulnerability previously discovered.

Finally, when no attack is successful, or has a rating higher than the one defined by the EAL, then the TOE can be certified.

3 Conclusion

A brief overview of process followed by industry and challenges faced to evaluate a secure product. In particular, the overview covers two key components of a digital economy, payment and identity. The first part discusses aspects of certifying a SE in context of banking and payment evaluation. Next, the role of Common Criteria is discussed in evaluation of a smart card oriented for biometric passport. Owing to these certification and trusted processes, the foundation of a safe and secure digital economy can be realised.

References

1. P. Kocher, J. Jaffe, & B. Jun,(1999). Differential power analysis. In Advances in Cryptology-CRYTO 99 (pp. 789-789). Springer Berlin/Heidelberg.
2. Kocher, P. (1996). Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Advances in Cryptology-CRYTO 96 (pp. 104-113). Springer Berlin/Heidelberg.
3. D. Boneh, R.A. DeMillo, & R. J. Lipton, (1997, May). On the importance of checking cryptographic protocols for faults. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 37-51). Springer Berlin Heidelberg.
4. G. de Koning Gans, J. H. Hoepman, & F.D. Garcia, A practical attack on the MIFARE Classic. In International Conference on Smart Card Research and Advanced Applications(pp. 267-282). Springer, Berlin, Heidelberg.
5. S. Indesteege, N. Keller, O. Dunkelman, E. Biham & B. Preneel. A practical attack on KeeLoq. Advances in Cryptology EUROCRYPT 2008, 1-18.
6. EMV Book 2 - Integrated Circuit Card Specifications for Payment Systems - Security and Key Management v4.2 2011. https://www.emvco.com/
7. EMV Book 3 - Integrated Circuit Card Specifications for Payment Systems - Application Specification v4.3 2011. https://www.emvco.com/
8. VISA - https://technologypartner.visa.com/Library/
9. PayPass-M/Chip Requirements - https://www.paypass.com/PP_Imp_Guides/PayPass-MChip-Requirements-2013.pdf
10. F. Poucheret, K. Tobich, M. Lisart, L. Chusseau, B. Robisson, and P. Maurine. Local and direct em injection of power into cmos integrated circuits. In FDTC, 2011.
11. K. Tobich, P. Maurine, P-Y. Liardet, M. Lisart & T. Ordas.Voltage spikes on the substrate to obtain timing faults. In 2013 Euromicro Conference on Digital System Design, DSD 2013, Los Alamitos, CA, USA, September 4-6, 2013, pages 483-486, 2013.
12. S. Anceau, P. Bleuet, J. Clédière, L. Maingault,J-L. Rainard, R. Tucoulou. Nanofocused x-ray beam to reprogram secure circuits. In Conference on Cryptographic Hardware and Embedded Systems 2017, 2017.
13. https://www.errol-laser.com/
14. http://www.alphanov.com/
15. biometric passport Protection Profile: https://www.sogis.org/uk/pp_en.html
16. Application of Attack Potential to Smartcards: https://www.sogis.org/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v2-9.pdf