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, Singapore
sbhasin@ntu.edu.sg
[2] NinjaLab, Montpellier, France
victor@ninjalab.fr
[3] UL Transaction Security, Basingstoke, UK
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

S.S. Ali et al. (Eds.): SPACE 2017, LNCS 10662, pp. 1–9, 2017.

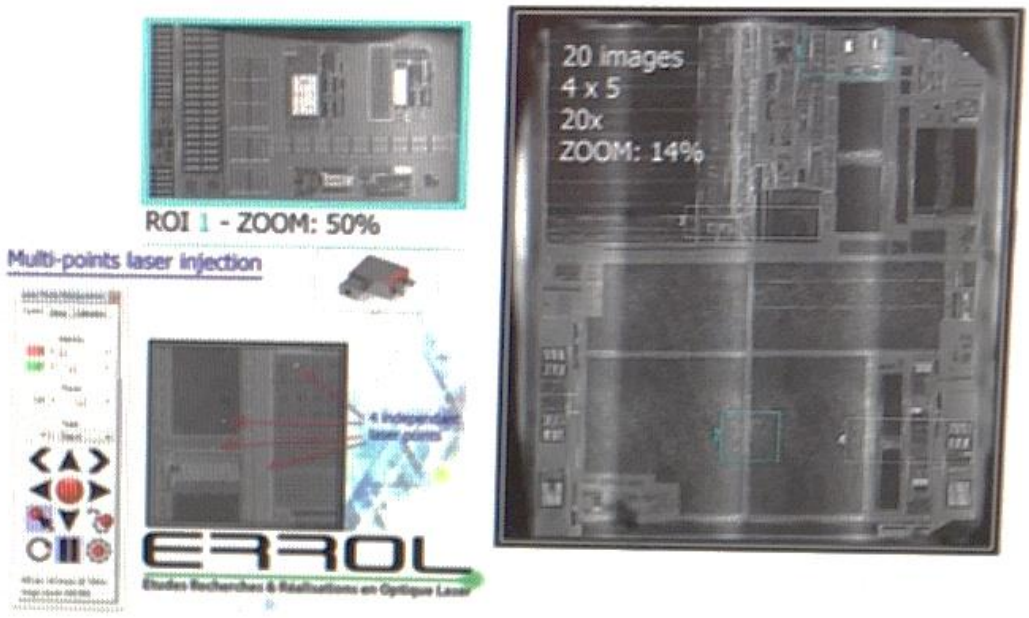

Fig. 2. Multi-spot laser system

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 Fig. 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 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