Is Hardware Security prepared for unexpected discoveries?

Sergei Skorobogatov
Department of Computer Science and Technology, University of Cambridge
15 JJ Thomsov Avenue, Cambridge, CB3 0FD, UK
Email: sps32@cam.ac.uk

***Abstract*- Hardware Security of semiconductor chips is in high demand these days. Modern electronic devices are expected to have high level of protection against many known attack aimed at the extraction of stored information. This is especially important for devices used in critical areas like automotive, medical, banking and industrial control applications. This leads to a constant arms race between attackers and developers. Usually new attacks are disclosed in a responsible way leaving time for chip manufacturers and system engineers to develop countermeasures. However, there is always a chance that mitigation technology is not developed in time, or worse, not practical to implement. Are the engineers in semiconductor community prepared for such an outcome? This paper looks at the history of similar discoveries in different areas and gives some results on memory extraction from an old smartcard and approaching highly secure embedded memory – battery-backed SRAM. Finally this paper elaborates on possible discoveries in attacks aimed at stored information. The aim of this paper is to raise awareness of emerging attacks to inspire new mitigation techniques to be developed in appropriate and timely way.**

***Keywords** – **Hardware Security, Invasive attacks, Embedded memory, Decapsulation, Data extraction, Battery-backed SRAM, EEPROM, Flash memory**.*

I. INTRODUCTION

Modern semiconductor devices store sensitive and secret information in embedded memory. This could be passwords, encryption keys, user information or intellectual property. Therefore, devices are expected to protect both confidentiality and integrity of that information against extraction and modification. It was demonstrated many times in the past how various semiconductor devices could be attacked. In the old days it was mainly non-invasive attacks [1]. However, over time chip manufacturers learned the lesson and significantly improved the hardware security of their chips. This required more sophisticated methods to be used [2].

If we look at the history of attack and defence technologies one thing could be spotted – the defence is several years behind. This becomes more evident with modern advanced deep-submicron fabrication processes. From the early 90s a common memory protection technique for smartcards was in using "invisible" ROM for code and algorithms storage. This was achieved by encoding the information with different doping level in the channels of storage transistors. As this impurities do not affect the optical properties of material, data extraction under optical microscopes was unsuccessful. It served well until the point when new methods were developed in Failure Analysis. This allowed relatively inexpensive attacks to be carried out for code extraction [3]. When in late 90s power analysis attacks were introduced [4], the semiconductor community had to take it very seriously by implementing appropriate countermeasures and performing rigorous testing on secure microcontrollers as part of their security evaluation procedure. The discovery of the optical fault injection attacks in the early 2000s [5] and their powerful implementation in the form of the laser fault injection [2] forced many chip manufacturers to develop countermeasures, especially for security sensitive applications such as smartcards. The time it took the industry and evaluation labs to adopt their methodology and develop reliable testing procedures and equipment showed how much it took everyone by surprise. When the existence of a backdoor in highly secure ICs was discovered [6] in the form of secret test/debug interface capable of overriding chip security policy, it raised a lot of questions about hardware security of modern ICs. Recently demonstrated method for the direct imaging of EEPROM and Flash memory contents using easily accessible Scanning Electron Microscopes (SEM) [7] challenges the security of embedded storage. This is because non-volatile memory was always considered as being highly secure against most invasive attacks due to very small electrical charge accumulated beneath very thin barrier that cannot survive de-processing. Now the obvious question is: What could be the next in ground breaking and disturbing attack on hardware security?

In many cases new attacks were far from being something absolutely new. For example, structural analysis for impurities using chemical methods were known for decades and actively used in Failure Analysis. The fact that switching of each individual transistor contributes to the overall power consumption of the circuit was not new and was actively used by semiconductors development tools to predict power consumption and overheating. Even the photon emission was known, but was too expensive as common attack technology [8]. The fact that photons can interact with transistors was known since the development of transistors and was even used for communication. The ability of electron beam to detect buried charge was also known, but only with the development of more sensitive microscopes became practical to use. The main message of this paper is if the vast majority of attacks are based on already known facts, there must be a way to predict such attacks and develop mitigation techniques well ahead of the active use by attackers.

The outcome of ignorance in understanding the attacks directions could be devastating to many modern devices going online or wireless as part of the Internet-of-Things (IoT) initiative. Modern devices which have wireless connectivity could be attacked in many ways through software vulnerabilities and backdoors.

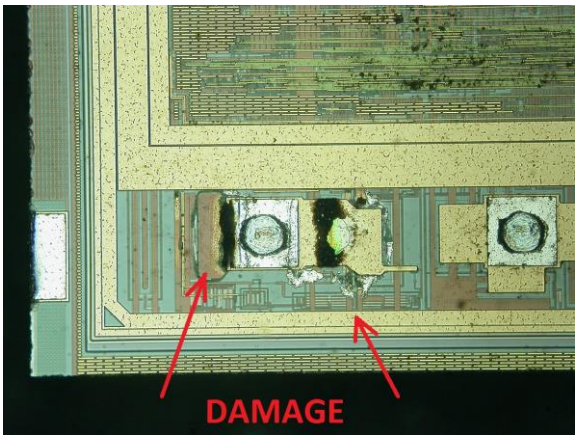

Fig. 1. Electrically damaged pin on the die of microcontroller

Sometime the research could even lead to impossible achievements. This happens when someone senior tells that certain things are not possible, but the research proves them wrong. This could result in a large outcry in the media like it was in the case of NAND mirroring attack on iPhone 5C [9]. There are some impossible challenges faced by Forensic Analysis engineers, for example, data extraction from electrically damaged (Fig. 1) and mechanically damaged (Fig. 2) chips. Although the contents of the on-chip non-volatile memory was fully preserved, conventional Failure Analysis methods are not only very expensive but would also require weeks or months of tedious work. However, it is very likely that Hardware Security would be able to come up with feasible and affordable solutions in the nearest future.

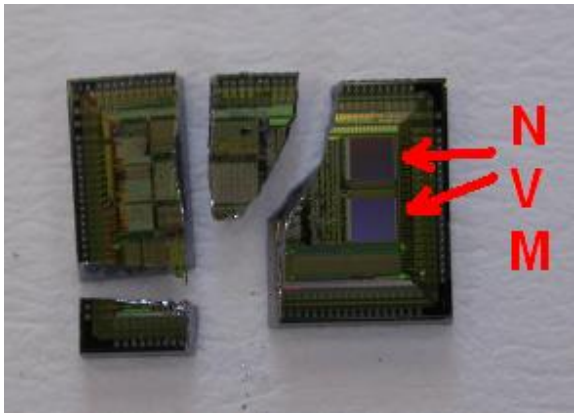

Fig. 2. Mechanically damaged die of microcontroller

As a contribution to the wide list of already known attacks this paper introduces two new attacks. One is about efficient microprobing of an old smartcard chip, another is about decapsulation of a microcontroller with battery-backed on-chip SRAM.

II. Experiments

As a first target to demonstrate the affordable memory extraction from a secure microcontroller, an early 2000s smartcard was chosen. It is based on the Hitachi HD6483102 chip fabricated with 0.8µm process with 2 metal layers and has embedded Mask ROM and EEPROM.

The Mask ROM is protected against optical reading with doping encoding. The Von-Newmann RISC 16-bit CPU with H8/300 architecture of this chip allows access to all resources in the linear address space and has a relatively simple instruction set [10]. The interesting property of this instruction set is if the most significant bit equals to 1 then the CPU will always execute single-cycle instructions without any branches. This can be achieved with a laser cutter [2] and the result is shown in Fig. 3.

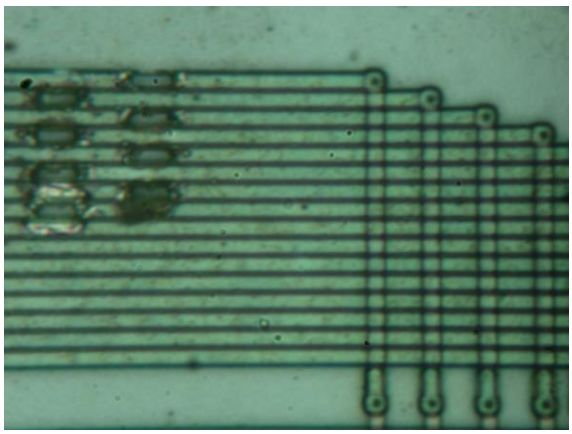

Fig. 3. Cuts in the data bus lines to modify instructions

In order to microprobe the data bus only opening in the passivation layer is required (Fig. 4). This cavity will help in holding the tip of the needle in place during the microprobing process.

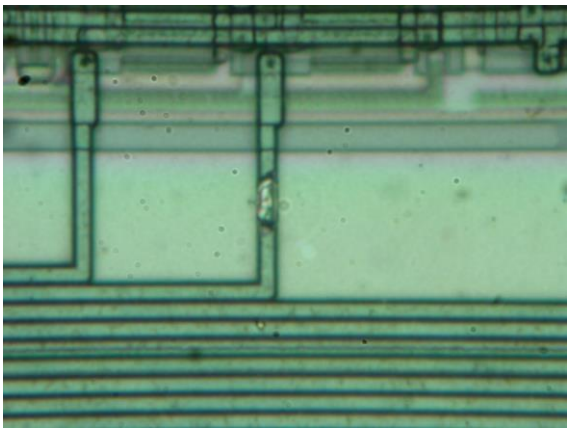

Fig. 4. Opening in passivation layer above the data bus line

Once the CPU is forced into execution of simple instructions it will access the whole memory by fetching all the addresses sequentially. This way the memory contents can be extracted by placing a microprobing needle over each bit of the data bus one at a time and recording the information on a digital storage

oscilloscope. After that all the acquisitions could be synchronised with the Reset signal.

As a target for verifying another kind of almost impossible attack a device with battery powered embedded SRAM was chosen – Vasco Digipass 270 – two-factor authentication token [11]. Although such devices do not have very high level of security protection like devices with tamper resistant enclosure, they offer adequate level of protection against all sorts of attacks. The reason for that is because the embedded SRAM is sensitive to the fluctuations of external power supply. Any interruption of the supply will cause the loss of data. In this case the signing key. Moreover, even the hardware reset of the device will make it inoperable, resulting in all keys and the user PIN being wiped off.

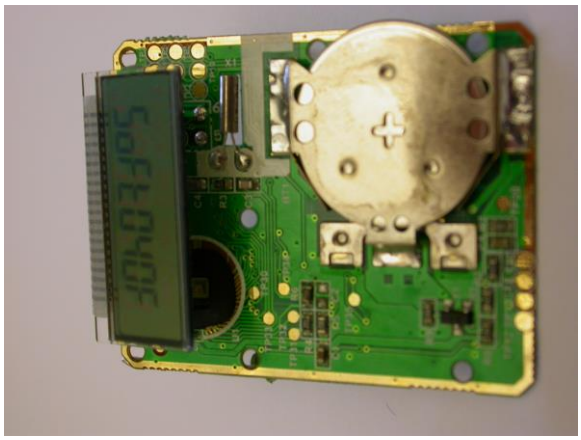

Fig. 5. PCB of the security token after normal decapsulation

The device is relatively easy to disassemble as the internal electronics is only covered with plastic sheets glued to its plastic case. The main component of the device is a specialised microcontroller which is bonded directly to the PCB and encapsulated with epoxy. Removing the battery for more than a few seconds results in the device going into internal test mode and no longer operational. The same happens if the Reset line of the microcontroller is shorted to 0. The result of the successful partial decapsulation of the microcontroller is shown in Fig. 5. However, because the battery was removed for that process, the microcontroller had no useful information inside.

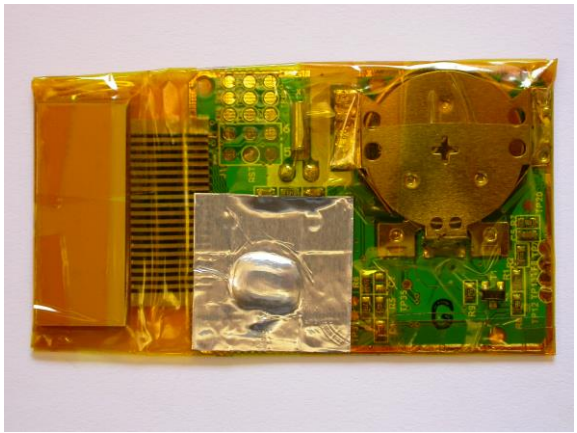

Fig. 6. PCB of the security token prepared for live decapsulation

In order to verify the idea of live decapsulation, the PCB of the fully working token was first wrapped in an insulation tape, while the potted chip was covered with aluminium tape (Fig.6). Then the whole setup was wrapped into aluminium tape before creating a cut in the tape where the decapsulation was desired.

The device was then decapsulated using 100% Nitric acid heated to 60°C. It was added in small drops and washed away with acetone after a few seconds. This process was repeated for several minutes until the surface of the chip die was exposed. Although the bonding wires were also exposed, this did not create any short circuits because of the high concentration of the acid. Once the decapsulation was finished, the whole sample was cleaned in acetone using ultrasonic bath. That removed the remaining of the acid and particles of resin. As a result the surface of the chip became clean. After careful removal of the tapes and testing the device demonstrated full functionality (Fig. 7).

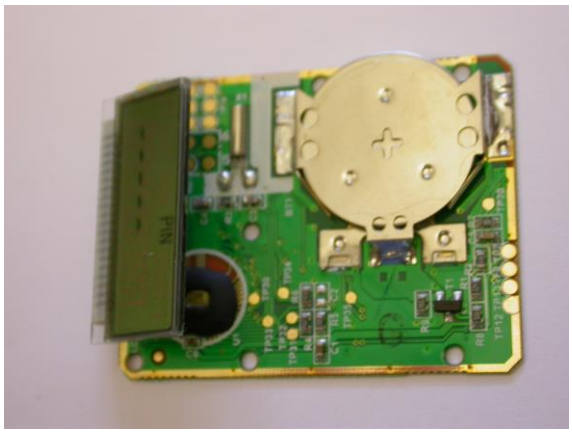

Fig. 7. PCB of the security token after live decapsulation

It is very important to make sure that the chip is not over-decapsulated. This would result in the acid going into contact with PCB traces made of copper. They react very actively with acid and this will quickly result in loss contact with bonding wires.

The device with live battery connection could then be used for further extraction of the embedded SRAM using microprobing attacks.

III. Results and Discussion

The microprobing experiments showed how easily a microcontroller with wide data bus could be probed and its memory contents extracted. The fact that only a single bit in the instruction set could defeat branch instructions could pose some security implications. Also, the presence of a weak pull-up in the data bus results in the cut bus lines to stuck at logic 1. However, if a memory encryption was used this would require more sophisticated approach, for example, by injecting random data and observing the response from the CPU [12]. Nevertheless, high orthogonality of instruction sets in most RISC CPUs could help the attacker in finding the right combination to influence the code execution.

Live decapsulation experiments proved the possibility of opening up battery powered devices without interrupting their constant power supply. This might have some consequences for highly secure applications where such devices are used. This could be medical devices or hardware security modules (HSM) used in banking or industrial applications.

Once the surface of the chip with battery-backed SRAM is accessed, the contents of the memory could be microprobed either by microprobing exposed data bus lines [12] or by exploiting test points. Both approaches though would require the use of a laser cutter to cut through passivation layer [2]. For devices fabricated with deep submicron process a Focused Ion Beam (FIB) machine will be required to establish a connection with internal data bus. However, such machines are available in many places for rent at a price below $100 per hour.

IV. Conclusion

Hardware Security of semiconductor chips is in high demand these days. Modern electronic devices are expected to have high level of protection against many known attack aimed at the extraction of stored information. This is especially important for devices used in critical areas like automotive, medical, banking and industrial control applications. This leads to a constant arms race between attackers and developers. Usually new attacks are disclosed in a responsible way leaving time for chip manufacturers and system engineers to develop countermeasures. However, there is always a chance that mitigation technology is not developed in time, or worse, not practical to implement. Are the engineers in semiconductor community prepared for such an outcome?

This paper raised a discussion on how well the semiconductor community is prepared for something unexpected in attack technology. From the previous history it was clear that not all discoveries are easy to predict or even mitigate when fully learned. This means that new approaches will be required to tackle the problem. As an example, this paper demonstrates how easily the microprobing attacks could be applied even on 16-bit secure microcontroller. It also shows that the expectation of battery-backed SRAM to be highly secure against invasive attacks is not quite true. It was commonly believed that decapsulation of a powered up chip is not possible, therefore, the fact that it could be successfully decapsulated was totally unexpected. The consequence could be in the review of the security requirements for battery-backed devices which hold secret information.

Another area of possible concern could be in unpredictability of the new attacks, especially if they would be based on some methods previously thought to be impossible. There were many examples when some new attacks were discovered based on already known facts. This requires the chip manufacturers and developers to find ways of predicting such attacks and developing mitigation techniques well ahead of any active use by attackers.

Recently demonstrated methods for the direct imaging of EEPROM and Flash memory contents using SEM pose big challenges to the hardware security. Not only because non-volatile memory was always considered as being highly secure against invasive attacks, but also because there are no mitigation techniques to defeat this unless new methods of storage are developed. Now the obvious question is: What could be the next in ground breaking and disturbing attack on hardware security?

In case of attacks disclosure there is always a dilemma for the best way of responsible disclosure. There are no strict rules on that, hence, both chip manufacturers and researchers could be affected. On one hand, the researchers want to tell everyone about their findings and make sure they found something important ahead of anyone else. On the other hand, developers want to avoid large recall of their products for updates or, worse, replacement. The solution could be in working together on the development of mitigation techniques.

References

[1] Ross Anderson, Markus Kuhn: Low Cost Attacks on Tamper Resistant Devices, in M. Lomas et al. (ed.): Proceedings of Security Protocols, 5th International Workshop, Paris, France, April 1997, LNCS 1361, Springer-Verlag, pp. 125-136, ISBN 3-540-64040-1

[2] Sergei Skorobogatov: Semi-invasive attacks – A new approach to hardware security analysis. Technical Report UCAM-CL-TR-630, University of Cambridge,Computer Laboratory, April 2005

[3] Oliver Kömmerling, Markus G. Kuhn: Design Principles for Tamper-Resistant Smartcard Processors, Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard '99), Chicago, Illinois, USA, May 1999, USENIX Association, pp. 9–20, ISBN 1-880446-34-0

[4] Paul Kocher: Differential Power Analysis. Advances in Cryptology – Crypto 99, Springer LNCS, vol 1666, pp 388–397

[5] Sergei Skorobogatov, Ross Anderson: Optical Fault Induction Attacks. CHES 2002, August 2002, LNCS 2523, Springer-Verlag, ISBN 3-540-00409-2, pp.2–12

[6] Sergei Skorobogatov, Christopher Woods: Breakthrough silicon scanning discovers backdoor in military chip. CHES 2012, September 2012, Leuven, Belgium, LNCS 7428, Springer, ISBN 978-3-642-33026-1, pp.23–40

[7] Franck Courbon, Sergei Skorobogatov, Christopher Woods: Direct charge measurement in Floating Gate transistors of Flash EEPROM using Scanning Electron Microscopy. ISTFA 2016, Fort Worth, USA, November 2016

[8] Sergei Skorobogatov: Using Optical Emission Analysis for Estimating Contribution to Power Analysis. FDTC 2009, September 2009, Lausanne, Switzerland. IEEE-CS Press, ISBN 978-0-7695-3824-2, pp.111–119

[9] Sergei Skorobogatov: The bumpy road towards iPhone 5c NAND mirroring. arXiv:1609.04327, September 2016

[10] H8/300 Programming Manual. Renesas Electronics.

[11] Vasco Digipass 270.

https://www.vasco.com/images/DIGIPASS-270_tcm42-47392.pdf

[12] Sergei Skorobogatov: How microprobing can attack encrypted memory. In Proceedings of Euromicro Conference on Digital System Design, AHSA 2017 Special Session, Vienna, Austria. IEEE Computer Society, 2017