Texplained
Arep Center
1, Traverse des Brucs
06560 Valbonne
France

Texplained

HARDWARE SECURITY INSIGHT

Security Analysis Methodology

Item	Description
Document	Security Analysis Methodology
Revision	1.0

SUMMARY

1. INTRODUCTION

Security is thought to mostly rely on software and networking solutions. Software can not work by themselves and are executed by Integrated Circuits. Therefore, security equally relies on hardware and software. As a system is as secure as its weakest point, all of its components have to be evaluated.

Hardware security is a vast topic which extends from board level down to the embedded Integrated Circuit. Secure elements are made to store embedded software, cryptographic keys and user data in a safe way that prevents hackers from dumping any of them. They are a good solution for security demanding applications.

Those security devices are designed to offer protection against the 3 main categories of attacks. State of the art secure elements are evaluated regarding Non-Invasive and Semi-Invasive Attacks and may offer :
- A good protection against Non-Invasive fault injection (VCC and Clk glitch),
- Some dedicated features to prevent side-channel attacks (Anti SPA-DPA),
- Protection against Semi-Invasive Attacks (light detectors, ...)
- Protection against Invasive Attacks (Meshes / Shields)

Different strategies can be derived to attack secure elements. One can try to extract secrets by applying Non-Invasive techniques but the guarantee of success is fairly low. Semi-Invasive Attacks may seem more powerful but they do not increase the attacker success rate by a significant factor and are usually more effective on larger devices such as SOCs.

Integrated Circuits piracy deeply evolved over the last decade. Attackers were individuals willing to get access to Pay-TV for example with very little equipment. Nowadays, groups and companies use professional Failure Analysis equipments to extract the secrets from devices in order to produce off-branded compatible devices that are reaching the mass market. From this point, the ability of attackers reached a high level and puts complete industry segments such as banking, e-Gov applications, authenticating devices, etc, at risk.

Professional Integrated Circuit pirates have privilege over the year the use of fully Invasive Attacks as it has several advantages among which a higher success rate for memory dumps.

This is where, one has to distinguish several scenarios. An attacker can extract the embedded software and keys from a device to produce clones or emulations to establish a counterfeit or off-branded mass market business.

On the other hand, extracting software from a chip can be an ideal starting point for finding a vulnerability that could be exploited through a simple attack, ideally Non-Invasive. This way, a pirate could for example steal data from people without stealing the device itself.

2. THREAT LANDSCAPE

Security is a major concern for the semiconductor industry. Bad security can compromise user personal data and safety, can result in market loss and can also damage the image of vendors.

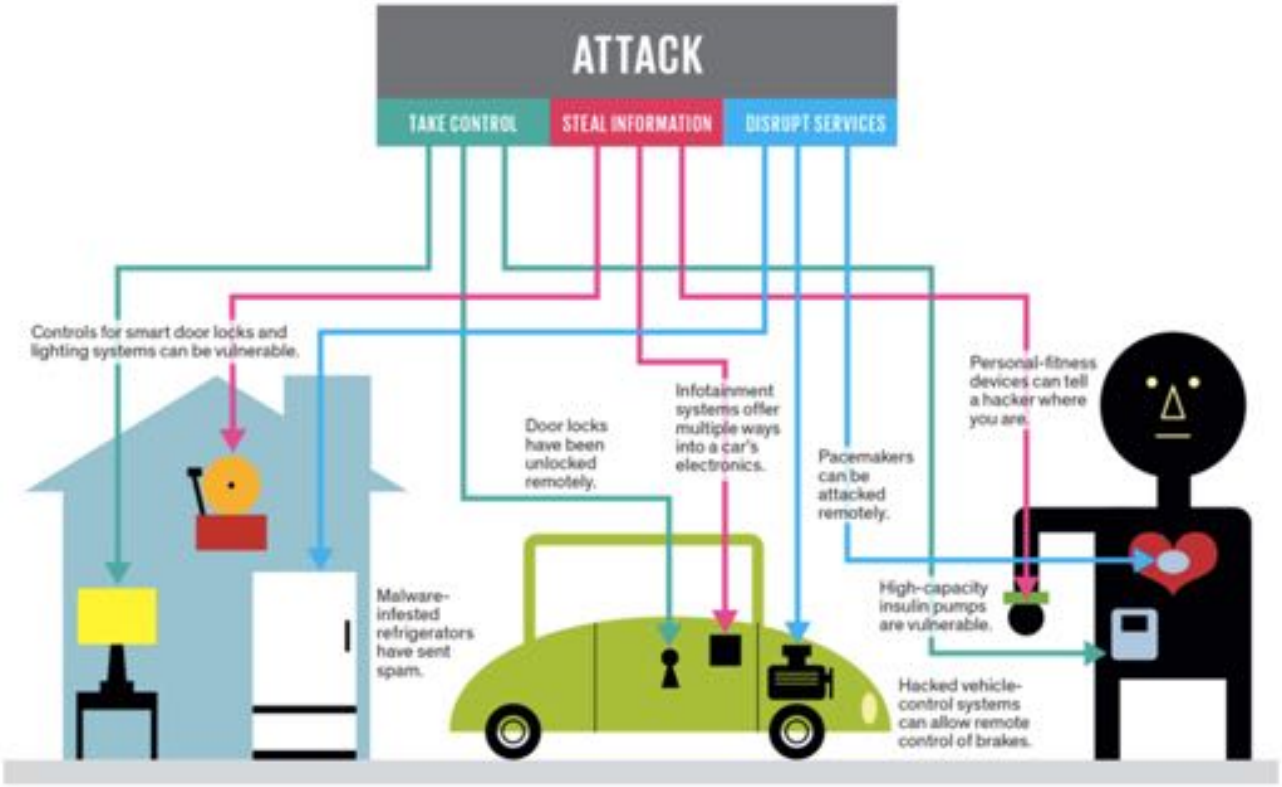


Illustration: J. D. King

Hardware piracy consists in different types of abuse:

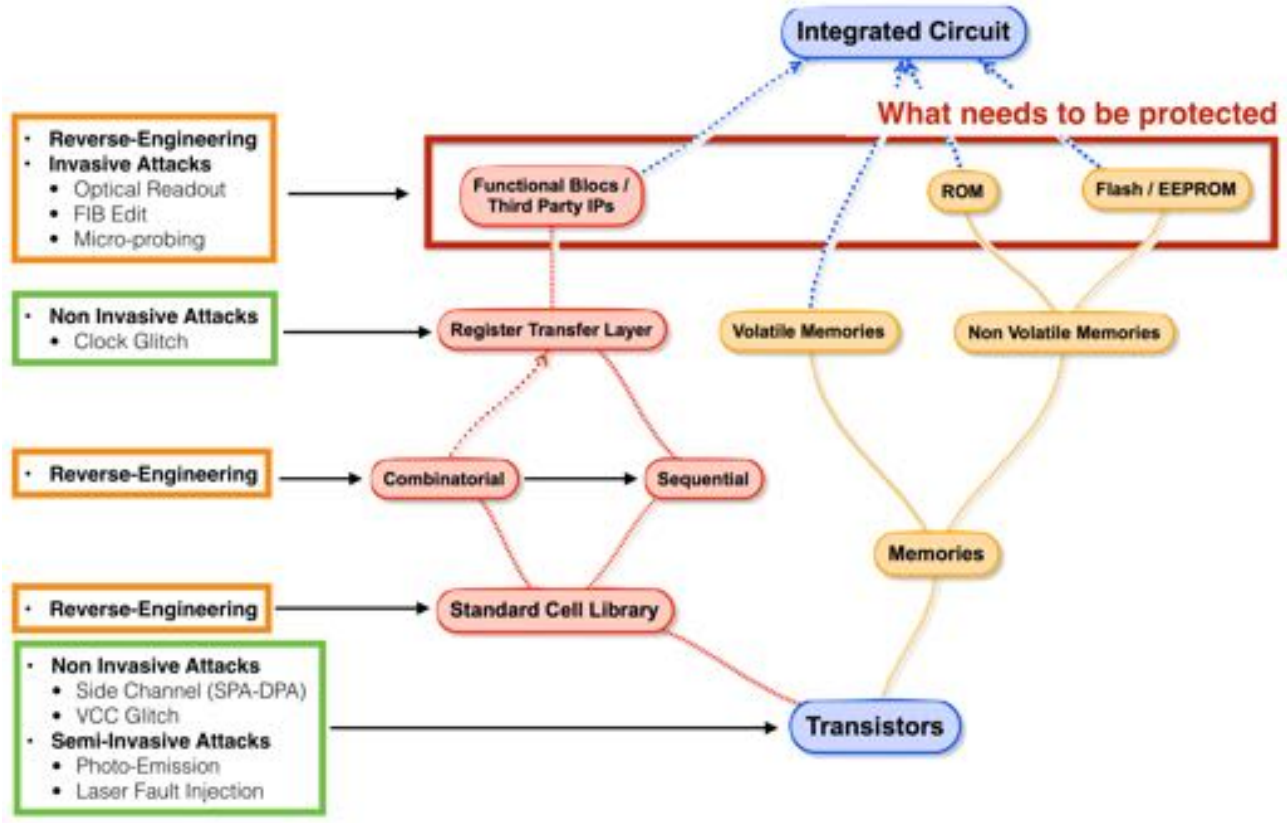
- Counterfeiting
- Intellectual Property Theft
- Mask, Chip and Circuits Theft
- Illegal Copy and Cloning
- Functionalities Modification (unlocking, DRM, etc)
- Trojans Implementation

Hardware attacks can also be used in order to take control of different systems, disrupts services or gather personal data. It is also a threat for individual safety. For those reasons, the threat must be taken seriously with security being at the center of the design stage for components that are used in critical systems as well as for mass production devices.

3. TEXPLAINED RISK ASSESSMENTS & BENCHMARKS

A. INTRODUCTION

Texplained specializes in Integrated Circuit Reverse-Engineering and Security.



The above diagram shows the construction of an Integrated Circuit starting at its transistors. On the left side, attacks are placed at the location which represents the abused parts of the IC. For most of the attacks, transistor physics is the base for the attack creation.

It is noticeable that Reverse-Engineering and Invasive Attacks are much higher level attacks that target the system instead of abusing its elementary components. The goal of such work is to extract secrets and the attacks are not based on empirically finding a glitch but rather on fully understanding the circuitry to modify it and then bypass any security.

Reverse-Engineering and Invasive Attacks are usually under-estimated and sometimes stated as a residual threat. This might be due to the barrier of entry that equipments and skills are creating. But this statement has to be properly counter-balanced :

- Can an attack be qualified as a residual threat when it can defeat a device in a couple of months when the component remains in the field for 10 years ?
- Lab equipments are expensive but there is no direct link with the attack price. A plane ticket is not the same price as the plane itself, is it?
- Service labs can be used for the laboratory work. Equipments can also be rented.
- The skills exist and pirates are using invasive attacks to create off-branded products (printer cartridges, video game controller), to abuse Control Access Systems, extract passwords and other protection keys, etc.
- Invasive Attacks can also be used to strategize simpler attacks such as Non-Invasive and Semi-Invasive.

Non- and to some extent Semi- Invasive attacks are of concern for chip designers and evaluators. Invasive Attacks and Reverse-Engineering are mostly left aside. The too few counter-measures are generally not efficient and evaluation are left aside to minimize costs.

B. TEXPLAINED OFFER

Texplained conducts risk assessments regarding Reverse-Engineering based Invasive Attacks on Integrated Circuits in black box situation to avoid being oriented in a way that would make us miss important weaknesses. Our approach is to look at the IC as if we were attacking it.

Our analysis is made with the help of our proprietary software suite called FlagChip that reconstructs the layout and netlist of the target device from Scanning Electron Microscope pictures. Using dedicated tools such as FlagChip allow us to make deep analysis in a time and cost efficient manner.

This, combined with our black box approach, is reflecting our mindset: half engineer, half hackers. FlagChip is providing coherent and complete datasets that are analyzed by our hardware team who benefits from more than 20 years combined experience in IC attack and evaluation.

This approach ensures that the complete digital core can be studied at different levels. Weaknesses will be looked for inside the netlist and will then be analyzed to strategize attacks.

Layout information are not left aside and are used to assess the attack difficulty. As an example, if an attack requires to modify 100 internal signals on a surface smaller than a 10 micrometers square, the number of potential attackers is getting close to zero.

In that context, our security risk assessments on Integrated Circuits aim at finding potential weaknesses but also rank those regarding their potential exploitation and their feasibility level.

The risk assessment is delivered as a report containing the different findings which are accompanied with the used pictures.

As an option and if applicable, the attack can be tested in real life which gives some more elements regarding the difficulty of the circuit edit, the associated micro-probing or the potential processing of the acquired signals.

A typical secure element Risk Assessment is composed of the different sections:

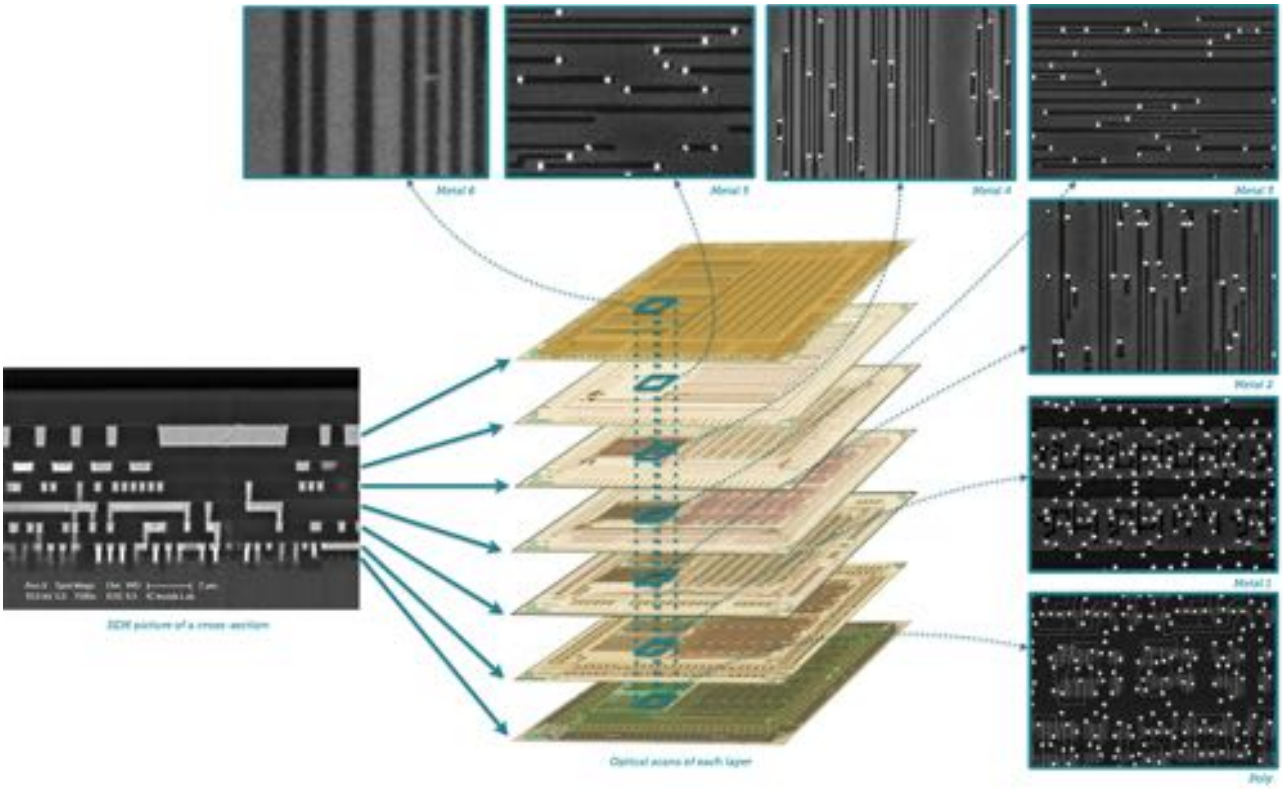
Phase 1: Physical Construction Analysis

Here we Reverse-Engineer the construction of one Integrated Circuit. During that preliminary phase:

- Optical pictures of the top and substrate layers are taken so as to map the(s) core(s), memories, etc
- A cross section is performed to count the number of layers and get their physical dimensions
- A SEM scan of the substrate sample is also done to measure the technology node and check the memory sizes

This phase is also used to determine the time and number of samples needed to perform the risk assessment laboratory work.

(Nb_samples ; lab_time) = f(Nb_layers, technology_node, surface_of_the_Region_Of_Interest).



Phase 2: Picture Acquisition

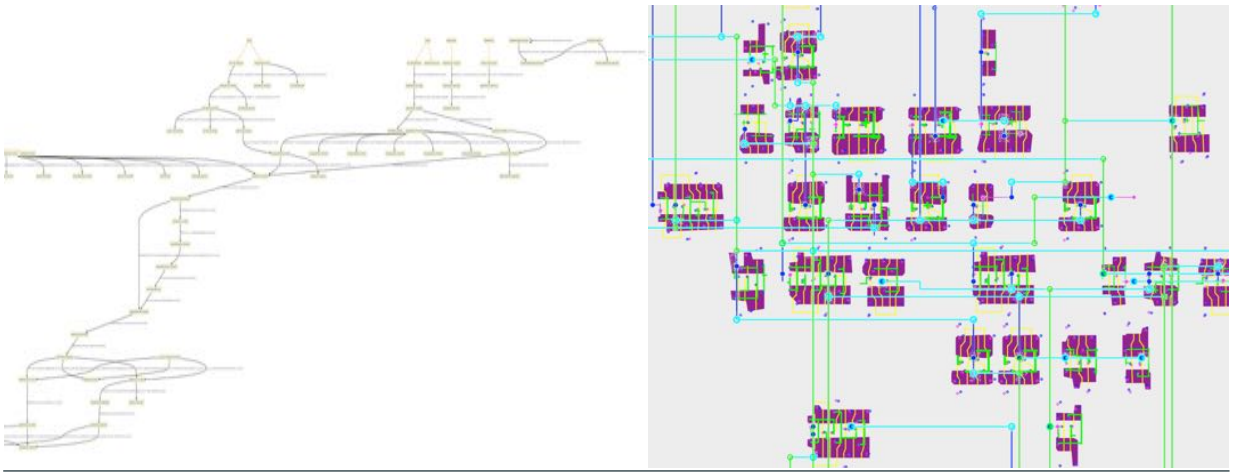
This phase is entirely done inside our laboratory. It consists in depackaging and delayering samples. Wet and dry chemicals are used in combination with polishing techniques to access the different chip layers. Each layer is then imaged using a Scanning Electron Microscope.

Phase 3: Physical Netlist Extraction

When pictures are ready, they are imported inside our Integrated Circuit Reverse-Engineering software, FlagChip, to convert the pictures into a netlist of the device. We call it physical netlist as every net is localized inside the chip. These localization information are helpful to find out where to perform the found attacks and to assess the difficulty of actually performing them.

Phase 4: Netlist Analysis

Our hardware team reviews the netlist at this stage to find exploitable weaknesses. We focus on finding ROMs and looking at their encryption, finding ways of dumping flash and EEPROM memories or key data, evaluating embedded counter-measures such as shields, etc.



Phase 4_b: (optional) Attack Assessment

When an attack has been strategized, this optional step can be performed to assess its difficulty at different levels, including FIB modification, micro-probing, data-processing, etc.

Phase 5: Reporting

The audit is delivered as a report including data from all phases. The results are also presented during a final meeting.

Results include technical findings but also the attack feasibility assessment so the study can be used for a larger risk assessment where the found vulnerabilities can be compared to the application characteristics such as time on the market, market specific risks, etc.

Risk Assessment reports can also be used to compare chips inside a benchmark. Benchmarks are conducted the same way as risk assessments but the results are compared to classify the devices by security level.

Phase 6: (optional) Extending the Analysis

Non- and Semi- Invasive Attacks are generally evaluated separately from Invasive Attacks. This approach can prove successful. For example, evaluating the resilience of the IC against side channel attacks can be made as part of a white box evaluation. Finding usable glitches (VCC / clk / laser / ...) is also feasible during that same white box evaluation.

But those approaches do not take into account the combination of software and hardware that characterize an embedded design. Random delays, use of an internal oscillator, light detectors can make the use of a glitch very difficult. Software verifications can also be used to detect certain attacks. At the same time, those counter-measures do not prevent Invasive Attacks.

On top of that, Invasive Attacks may be used to get access to the internal details of a product in order to find more simple attacks. This learning curve can make it possible to find well hidden vulnerabilities that can be exploited with simple equipments in a very short time. This makes it possible for example to extract data from a device without having the user find out about it.

For that reason, it can be useful to combine a Reverse-Engineering and Invasive attack evaluation with other type of attacks assessments in order to assess the security of the chip against memory dumps.

This evaluation method is designed the following way:
- IC Reverse-Engineering
- Invasive attacks evaluation
- Memory dump evaluation and / or debug chain unlocking
- Code review and / or scan chain analysis
- Identification of potential weaknesses / Non- and Semi- Invasive Attacks strategy creation
- Non- and Semi- Invasive Attacks evaluation

This type of evaluation is made to assess the full system and can still be performed in a black box situation to mimic a real attack scenario and avoid looking at only a fraction of the system.