5-2021

Malicious Hardware & Its Effects on Industry

Gustavo Perez

Malicious Hardware & Its Effects on Industry

An Undergraduate Honors College Thesis

Department of Computer Science and Computer Engineering

College of Engineering

University of Arkansas

April 2021

By Gustavo Perez

Abstract

In recent years advancements have been made in computer hardware security to circumnavigate the threat of malicious hardware. Threats come in several forms during the development and overall life cycle of computer hardware and I aim to highlight those key points. I will illustrate the various ways in which attackers exploit flaws in a chip design, or how malicious parties take advantage of the many steps required to design and fabricate hardware. Due to these exploits, the industry and consumers have suffered damages in the form of financial loss, physical harm, breaches of personal data, and a multitude of other problems.

Many are under the impression that such damages and attacks are only carried out at a software level. Because of this, flaws in chip design, fabrication, and the large scale of transistors on chips have often been overlooked as a means of exploitation. However, as is the trend in cyberattacks when one door is locked attackers look to gain an entrance with any possible means. Fortunately, strides have been made in closing those doors, however now that malicious attackers have been made aware of these openings the aim is to mitigate or even abolish the damage that has been dealt.

Contents

1. Introduction

1.1 Motivation

The malpractice of malicious hardware is spread throughout many stages in the life cycle of a chip. For many years the general expectation was that cyberattacks would be carried out at a software or firmware level. We largely ignored the risk imposed upon the very machines that execute the software we focused our security efforts on. As a former intern with Centauri, I gained a firsthand look at the design flow of an SoC design and was made aware of the need for an increase in hardware-level security. Through case studies and my work in physical implementation, I gained knowledge of where exploitations occur and the ways they can be handled.

Modern hardware designs are a culmination of millions of lines of HDL code, toolkits, scripts to facilitate design software, and modules that are outsourced across multiple vendors. Because of the complexity of a chip's design and its long development cycle, hardware is susceptible to a multitude of attacks. One major facet of hardware's vulnerability is its inability to receive low-level repairs once it is in the hands of the consumer. Software on the other hand can be modified to withstand attacks in the form of patches rolled out by development teams [10].

Without the ability to effectively "patch hardware" the only solution to hardware that has made it to maket with malicious circuitry comes in the form of recalls. Companies forced to recall products suffer damages that can range upwards of hundreds of millions of dollars. To cover potential financial losses the integrated circuit design industry has seen a major shift between all entities involved.

With this thesis I aim to briefly highlight the dangers and risks involved in integrated circuit design. After learning how hardware can be modified we can then evaluate case studies and the ways this industry has transformed to mitigate financial losses and called for higher levels of trust.

1.2 An Overview of Attacks During a Chip's Life Cycle

From a piece of hardware's inception threats are present in the form of outsourced third-party IP that designers utilize in their schematics. In a design house third-party modules are commonly referred to as "black boxes" because design teams don't have the means to easily inspect foreign intellectual property. Therein lies a huge leap of faith in which designers must have trust that their vendors don't sell them compromised designs. However, this is only the earliest critical stage.

While not as common a problem due to internal trust within a company, malicious workers have direct access to the entire design flow of a chip. This allows for the planting of malicious code, and transistors that can alter the functionality or intended use of a piece of hardware. Because of the massive scale of the code involved in designing an integrated circuit and the number of transistors present in modern processors these changes are at risk of going unnoticed. This results in a chip that has been approved for fabrication and once physically created will have undetected exploits ready for attackers to take advantage of.

If a design is approved for physical manufacturing and is free of nefarious modifications, one of the most vulnerable times in a chip's life cycle is in fabrication. Due to the cost of building and running a foundry design teams have found themselves

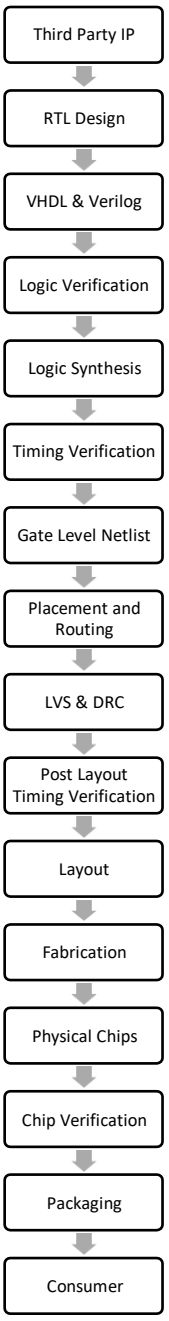

Figure 1

outsourcing to offshore foundries to reduce costs [21]. During this stage, changes to the physical elements of the chip can be made.

While attacks to hardware post-development are different in nature, there is still a high level of risk involved. Consumers with the same intent as malicious workers in foundries now have “finalized” chips that can be repurposed. The electronics counterfeit market is immensely large, and victims are present across all levels of society.

2. Trojans

Before we can further evaluate the different stages of development we must first understand what a Trojan is. In the world of computing we define the word as, camouflaged software that appears to be working as intended, but contains malicious processes. Popular definitions however fail to recognize the existence of hardware Trojans. Much like their software counterparts they infiltrate computer systems and do not cause immediate noticeable damage.

2.1 Taxonomy of a Trojan

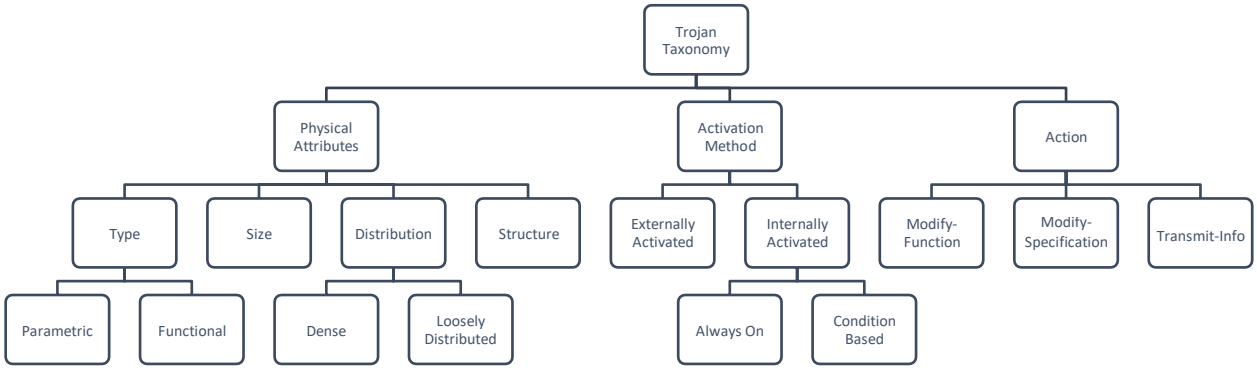

Figure 2

Any hardware trojan can be broken down into 3 principal characteristics: physical attributes, activation method, and action [19] as show in Figure 2.

***Physical Attributes**:* Defining physical features of a Trojan include type, size, distribution, and structure. Type can be categorized into two distinct Trojans, functional and parametric. Functional Trojans are implemented by either inserting or removing transistors and gates. Parametric Trojans are Trojans that are created through the altering of existing physical features on the chip. The size of a Trojan is measured not by its physical makeup on the chip but by the number of modifications that have been made to implement the Trojan. These modifications count HDL level additions or deletions of gates, and physical altercations of chips. The distribution of a Trojan is measured by the density of a Trojan on a chip. Modifications can be in close proximity on a layout or dispersed throughout the chip. This all depends on the available empty space in a design. Structure refers to the detectable physical footprint of a Trojan. Because parametric Trojans alter preexisting design elements they are harder to detect. However functional Trojans that are larger and more densely distributed can be detected by localized power spikes on a chip. Loosely distributed Trojans require longer wire lengths to interlink components and have a higher chance of altering expected timing delay results on a chip. Because of these two detection methods, attackers have had to create new techniques to forego detection.

Activation Method: The next characteristic of a Trojan is how it is activated. Activation can be divided into two categories, external or internal activation. In external activation, attackers can activate a Trojan at the time of their choosing. This is done by sending external signals to a chip that are input through onboard receivers and commence the Trojan's internal attack. Wang furthermore breaks down internal activation into two subcategories, always-on and condition-based. Always-on Trojans are usually of the type parametric. This is because to remain activated physical changes to nodes or wires must be made. Condition-based activation if undetected can

be compared to a ticking time bomb. Without knowledge of the existence of the Trojan a near limitless amount of conditions could activate it. Wang provides examples such as chip voltage sensors, external temperature and humidity sensors, or internal logic states. Surprisingly, always on Trojans are harder to detect. Because of their parametric type, only subtle physical changes to the chip are made. Condition-based Trojans, however, require the addition of logic components to be activated thus they are always consuming power, or the increased loads on wires change the expected timing delay results.

Action: Lastly Trojans can be characterized by their actions and in this characteristic there are three subcategories, modify-function, modify-specification, and transmit-info. Modify-function Trojans change the expected logical behavior of a design. Modify-function capabilities by their nature are very broad in range and can result in numerous types of attacks. Modify-specification Trojans once again represent parametric Trojans because they change physical features on a chip. The capabilities are generally limited to the eventual failure of a chip. Transmit-info Trojans steal information at a hardware level such as encryption keys or passwords and then send them back to the attacker.

2.2 Example Trojan

Because of the increased complexity present in modern hardware functional type Trojans can now be inserted into an ocean of transistors. One of the earliest research examples was the Illinois Malicious Processor [12] or IMP for short. The IMP was a variant of the Aeroflex Gaisler Leon 3 and was able to function as a Leon 3 until its Trojan was externally activated. By adding 1,341 gates into the design researchers were able to carry out attacks such as encryption key stealing, password stealing, and privilege escalation. The Trojan present in the IMP was

externally activated through a corrupt network packet and subsequently received commands from the network which were then executed on the processor.

Surely 1,341 additional gates would not go unnoticed. Designs are comprised of hundreds if not thousands of files, millions of lines of code, and gate counts already in the scale of millions that are projected to increase. Because of the sheer magnitude of a design, a relatively small Trojan sophisticated in design can carry out a lot with only a little.

3. Analysis of Attacks

3.1 Third-Party IP

Because of the time and cost involved with designing an SoC design, designers often utilize third-party intellectual property. This practice is used to avoid the unnecessary design of modules that are meant to be reused several times within a design. Design houses save money and internal design efforts, and instead utilize a module that is proven to work. A high level of trust must be placed on the third-party vendor to supply modules that work effectively and safely, but in some cases third-party IP arrives compromised. Before designers are even considering final tape-outs and physical fabrication they are at risk of integrating malicious hardware into their designs. These Trojans are generally classified as functional Trojans. They are capable of causing serious damage by being present in a mere 0.1% - 0.5% of the overall design layout [15].

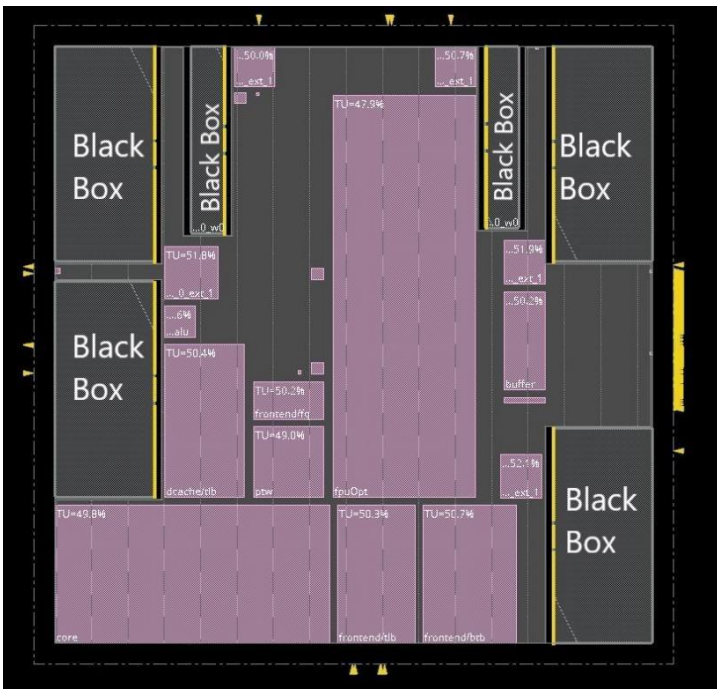

Figure 3

When organizations utilize third-party intellectual property, modules present in the design are quite literally a “black box”. To visualize what a physical implementation engineer is creating on design tools Figure 3 is the floorplan of a Rocket Core that I designed. Pink modules are spaces reserved for modules designed in-house, and modules labeled "Black Box" are third-party SRAM and DRAM modules. Because these black boxes cannot be inspected easily with EDA tools, designers are unable to see if extra transistors are present before sending their designs to foundries. Detection then comes in the form of rigorous simulation tests to ensure no anomalies are present. These anomalies could present themselves in the form of irregular power usage or timing irregularities due to additional added cable routes between malicious transistors [15].

Because of these risks, designers are left with the task of testing and verifying third-party IP if they want to ensure the security of their system. While time-consuming, in the grand scheme of development, testing saves designers more time and resources than having to design these modules in-house.

3.2 In House Attacks

In-house attacks can be incredibly rare but that does not mean they’re impossible. These attacks are once again carried out during the design phase of a chip but are much harder to

implement and hide effectively. Security in design houses can be achieved through several avenues, the first being selective hiring. Because of the high levels of suspicion in the industry of physical chip design hiring is and should be taken very seriously. Failed background checks or failure to obtain security clearance can deter malicious users. Previous employment with competing organizations is also taken into consideration. However, if someone with malicious intent were to be employed as part of a design team he/she would be one of many working on a design. With multiple personnel on a team to hold each other accountable attacks can be detected during the many steps of the design phase. During the design of a chip, every change and simulation is logged. Design repositories flag alterations to code for peers to review, and during the many design generations and tape-out reviews, nearly every aspect of a layout is observed closely. Even though attacks are not impossible internally within organizations, the most critical attack point before fabrications is present in third-party intellectual property.

3.3 Fabrication Attacks

Before packaging and consumer selling this is the final step of production in which hardware is at risk of being maliciously modified. During this phase, designs have been finalized and sent for fabrication. With many modern design houses being "fabless" and the cost of running a foundry being so high, the most common method of turning digital designs into tangible designs has been to send final tape-outs to foundries. Under the assumption that a Trojan was not inserted through third-party intellectual property or in-house, this is now the most critical stage of a chip's production. Because many foundries are overseas or do not allow direct oversight of production the design is now completely in the hands of yet another organization. With that comes an extreme level of trust, and attempts at preventing modifications.

By creating a densely packed tape-out designers leave little room for the addition of gates. If there are areas on the design where gates can be modified the additional gates must be connected to specific modules which means extra wiring through multiple metal layers. Additionally, attackers must be able to keep the chip fully operational after production until their Trojan needs to be activated [18]. With so much complexity one might wonder, “Why is this such a dangerous phase of production”. After having explored functional type trojans that add gates at an HDL or RTL level, we must further explore parametric type Trojans. While they may not be as sophisticated as functional trojans that can steal memory information or leave backdoors, their damage can be just as catastrophic. Take for example a missile detection system that has worked flawlessly for some time and then suddenly malfunctions due to modifications made in fabrication.

A parametric Trojan is created by modifying physical aspects on the chip. During the development phase wire sizes, lengths, and connections are all meticulously planned out. By altering these physical aspects of the chip attackers can craft dopant level Trojans. By altering the dopant concentration on an input pin of a logic gate attackers can change the logical input from a 0 to a 1 or vice versa [21]. For example, a CMOS transistor's strength is determined by its width. By reducing the area that is doped on a transistor it is possible to change the width and therefore its strength. While more complex doping mechanisms have been explored the simplest method is altering the dopant concentration of the active area of a transistor to a smaller area. In the following diagram, we see an altered mask that has changed the dopant concentration of the P-well to reduce its overall size. In Figure 4 below [9] we can see how forcing the dopant concentration causes the area of the P-Well to shrink.

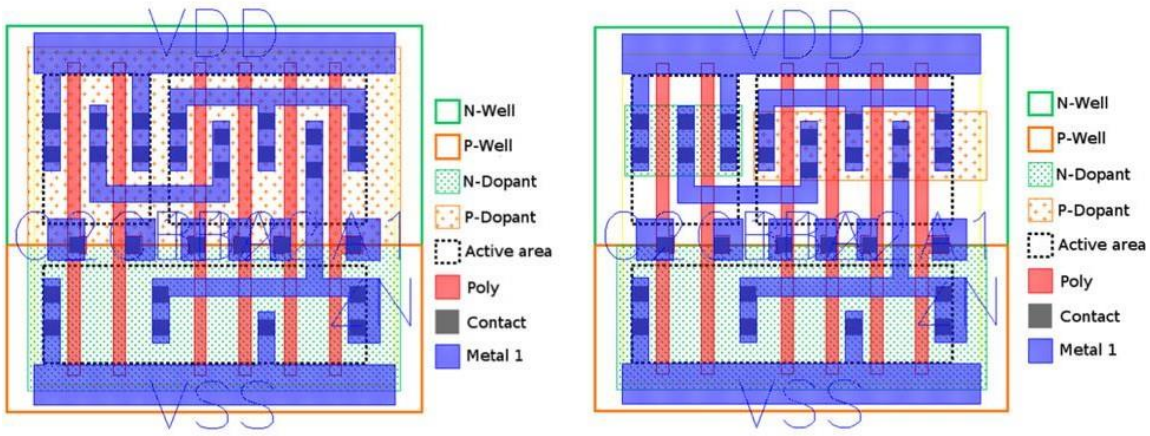

Figure 4

Because these are existing circuits and gates, dopant level Trojans are extremely hard to detect and leave a very small footprint in the finished design.

3.4 Counterfeiting

Once a product has left the foundry and has been extensively tested by the design team it is now susceptible to aftermarket modifications and counterfeiting. Out of the hands of the design team, attackers can make any modifications they wish and pass off their products as either "new" or alter the markings on the printed circuit board to sell the product as something else entirely. Through various techniques such as sandblasting and acid washes [6] counterfeiters are able to salvage potentially decades-old components and resell them. With the limited lifespan of computer hardware, it's easy to see how dangerous it is to integrate these counterfeited parts into a computer system.

In a 2011 Senate Hearing [17] it was reported that approximately 15% of all electronic parts purchased by The Pentagon as either spare or replacement parts were counterfeit. With a 3 in 20 chance of having a component present in systems meant to protect civilians the risk is very high, and that's solely the statistic for the government sector. When we take into consideration

the possibility of counterfeits in medical technology or transportation we begin to question the products that we as average consumers own or are impacted by in our lives.

To further highlight the gravity of the situation I present to you the 2014 arrest of Marc Heera. In 2014 the FBI arrested Heera for selling cloned Hondata s300's. Hondata, a popular aftermarket Honda automobile modification, manufactures hardware that can bypass security measures in a Honda vehicle. The chip is capable of changing the limits put in place by Honda in the Honda engine computer. Enthusiasts can unlock more horsepower and fine-tune their vehicles to get the most out of them. Having a piece of hardware that already has so much power over your vehicle be modified is a recipe for disaster. Heera was able to carry this out by paying Chinese companies to manufacture these chips and once received he passed them off as genuine by labeling them and packaging them just as Hondata does. In Figure 5 to the right the genuine Hondata part is pictured below and the counterfeit above [16].

Figure 5

While these "attacks" differ from the Trojan-based attacks we have explored so far, it is important to recognize them to understand how vulnerable our modern computer hardware is. With so much focus placed on dated legacy software, we need to consider how dated or genuine our equipment is. With more scrutiny on the parts used across multiple different spaces, government and personal alike, we can mitigate the risk to consumers.

4. Effects on Industry

4.1 Financial Evaluation and the Need for Trust

Assessment of damages suffered by component designers is a hard metric to measure accurately because of the very nature of Trojans. A well-placed and designed functional or parametric Trojan can go undetected for a long time, only to reveal itself until its activation method. Because of this, we can instead explore the changes that have been made to the integrated circuit industry and the different countermeasures that have been established to circumnavigate the issues of trust. Before doing so we must first identify the three third-party entities that an SoC design house establishes contracts with for development: foundries, IP vendors, and EDA tool vendors.

Foundries: Foundries are fabrication facilities that manufacture components once they have received tape-outs from SoC designers. Foundries have multibillion-dollar facilities and for this reason many SoC design organizations outsource. Currently 5 companies make up 54% of all global wafer capacity. Taiwan Semiconductor Manufacturing Company or TSMC for short is the second largest semiconductor manufacturing company with a 13.1% share of global wafer production [8]. In 2019 TSMC was responsible for the production of 10,761 products and serviced 499 different customers [7] across 17 different foundries predominantly located in Taiwan and China. In May of 2020 TSMC proposed to build a fab in Arizona with the total expenditure of the project estimated to cost 12 billion dollars with plans for expansion or modification to wafer production [11]. Without considering US taxes it is estimated that wafer production in the Arizona fab will be approximately 7% more expensive than wafer production in Fab 18 located in Taiwan [11]. These plans came about to ease issues of trust within the US

government. With these expenditure estimates and production cost increase figures one can assess the lengths that organizations go to and resources foundries expend to establish trust with their customers.

IP Vendors: Third-party intellectual property vendors are one of the two primary concerns in IC design and production. Because of the high possibility of functional Trojan insertion from external entities into an SoC design trust between vendors and customers is crucial. Major IP vendors include companies such as ARM, Synopsys, and Cadence with a reported combined 64.9% market share in 2019 [14]. Analyzing costs of IP usage can be very complex due to the large variety of costs and vendor business models. Factors include proposed usage by SoC designers, licensing fees, royalties, time of usage, and technologies purchased. An upfront cost with ARM to utilize their Cortex-A5 CPU begins at $75,000, on top of that cost there is an additional $50,000 licensing fee. Their higher-end package which includes more resources and is an annual package has an upfront cost of $200,000 with licensing fees assessed per use case [20]. These numbers however are only upfront costs and licensing fees, because ARM's licensing terms are secret a further breakdown of costs is harder to achieve. In Q4 of 2020 alone ARM acquired 579 million dollars in net sales [3]. With a 40% share of the market and their reported quarterly profits, we can evaluate the amount of trust placed on reputable IP vendors to deliver products that will come free of security risks.

EDA Tool Vendors: Electronic design automation tools or EDA tools for short are tools utilized by SoC designers to facilitate IC design. The major vendors in this category are Synopsys, Cadence, Xilinx, and Altera. In SoC design designers often use multiple toolsets across different EDA vendors with factors in pricing being time used, tools utilized, and licenses granted to the organization. For example, an organization may purchase 5 licenses for synthesis tools, and

another 3 for floor planning tools because of this it is again difficult to answer the question, "How much does an SoC design house spend on these tools?" Mistrust of an EDA tool vendor stems from software gathering more information than required of a design.

In this IC market model diagram created by He Li and Jiliang Zhang [13], we can see how all of these parties are directly tied to the SoC designer and have an impact on the product that the end-user receives. At the center of it all is the SoC designer, who is at the mercy of these external threats. Due to the recent call for hardware security, we can discern why designers must be on high alert and conduct rigorous testing throughout the entire development phase to ensure a safe and secure product for their end-users.

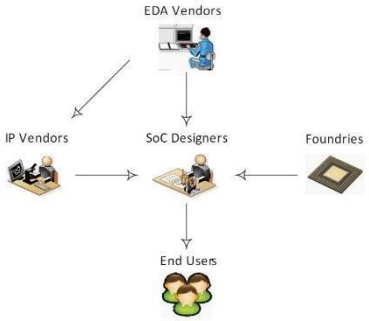

Figure 6

4.2 A Bombing in Syria and the Emergence of Trust

One of the very first calls to arms in the space of hardware security was the 2007 bombing executed by Israel on Syria. The reason this bombing was under so much spotlight in the IC design industry was because of the failure of a Syrian radar that was supposed to alarm the Syrian military of the incoming bombing. Because this was before hardware was suspected of being at risk for attack nobody knew exactly what led to this failure. However, the consensus was that a functional Trojan inserted into the radar detection system contained a backdoor that allowed attackers to shut it off or alter its functionality long enough to carry out the bombing [2]. Because of a famous article published by Sally Adee, The Hunt for the Kill Switch, SoC designers were made more aware of the need for trusted electronics.

Three months shortly after the bombing, DARPA, a research and development wing of The Pentagon, created the Trust in Integrated Circuits program. Initially when this program was created three separate government contractors were tested to meet the standards put forth by the program. Now because of the Trust in Integrated Circuits program facilities and contractors across the entire development process can receive accreditation from The Pentagon [1]. To receive accreditation organizations must meet the metrics put forth by The Pentagon and ensure that measures are being taken to provide secure computer components to the US Military. This program has led to a much higher level of accountability placed across all entities who wish to fulfill contracts with the military.

5. Solutions

When we begin to look at methods and techniques to reduce the risk of hardware Trojans, we ask “How can we prevent this?” However complete elimination of the threat is very hard to achieve. For a design team to remove the risks of external entities and have a completely trusted chip they would need to design the entire chip from scratch and fabricate it themselves. As discussed in the financial evaluation this is not a feasible solution. We can instead make efforts to prevent malicious modifications at fabrication and detect them if they are present before harm is done.

5.1 Prevention

The best way to prevent the insertion of Trojans is close monitoring of a design from start to finish. Because complete design and fabrication are not feasible, the emergence of trusted design houses has reduced the level of danger posed to the military sector. With small teams and a high level of accountability placed within them, consumers have increased faith that their

product does not have a hidden agenda. However, fabrication attacks at offshore foundries are still a present risk. For this reason, designers have constructed methods to deter and detect modifications.

To counteract malicious modification at the fabrication stage designers have begun to create their designs with virtually no empty spaces. While most attacks at fabrication come in the form of parametric Trojans, zero empty space mitigates the threat of functional type Trojans at fabrication. By adding functional filler cells that come at a negligible performance cost, designers can detect changes made to the integrated circuit at fabrication. Prefabrication tests give designers expected results to test for once they have their physical chip. Experiments conducted by Ba show that once the same inputs used pre-fabrication are used after modifications have been made, their expected signatures do not match [4].

The end product of functional filler cells results in post-fabrication testing, which would be better classified as a detection method. Because there are so many steps where designs could be tampered with, preventing a compromised chip from being sold comes ultimately in the form of detection.

5.2 Detection

The least used detection method is destructive reverse engineering. By deconstructing a chip post-fabrication using chemical mechanical polishing we now have access to individual components within the chip [5]. We can then put these components under an electron microscope to analyze the chip and detect malicious modification methods, assuring that our chip is safe for consumer use. This process that inspects even the smallest of components however is very expensive requiring many techniques for analysis over a period of weeks or months. At the end

of validation, you will have destroyed a single chip from an entire batch of manufactured chips. During fabrication only some samples may have been tampered with which calls for the deconstruction of all chips to verify their safety. For these reasons, reverse engineering is not an attractive detection method. Instead, we can conduct logic tests and side-channel analysis.

Logic Tests: Using automatic test pattern generation or ATPG we can apply inputs to a chip and compare their outputs to expected results. This method originally designed to detect faulty chips can be applied to detect parametric Trojans. ATPG is run by EDA tools that have knowledge of existing routes and modules in the chip therefore finding hidden functional trojans through predetermined tests is not feasible[19]. Instead, we can test for rare combinational inputs using MERO. MERO is short for "multiple excitation of rare occurrence". By detecting low probability conditions and applying rare inputs we can trigger functional type Trojans [5]. Applying rare inputs to low probability nodes a sufficient number of times and activating conditional-based triggers is our best method of logical detection for functional trojans.

Side-Channel Analysis: By observing the physical characteristics of an IC under nondestructive tests we can detect functional type Trojans. Observable side-channels include power anomalies, EMF variations, temperature variations, or execution times. As previously stated functional Trojans are constantly consuming power at some level to monitor for their activation methods. If we were to activate the power grid and observe the power spikes throughout, we could detect the power consumed by inserted malicious gates searching for their activation trigger [19]. We also can detect timing anomalies that present themselves when extra wiring is added. Because of the added gates and their need to be connected to existing components to affect the chip, longer routing is required for Trojans to work. We can isolate Trojans by applying rare inputs and flagging unexpected timing delays.

Side-channel analysis however fails in one regard and that is the need for a “golden chip”. Golden chips can be defined as chips that are known to be free of any malicious tampering. By having a chip to compare to we have evidence that an anomaly is in fact an anomaly. The best method to obtaining a golden chip comes from destructive reverse engineering. By having fully analyzed a chip under a microscope and confirming the chip is unmodified, design houses have a baseline chip with which to perform their side-channel analysis. The other method for obtaining a golden chip would be through extensive logic testing however experimenting with every possible input combination would take many months on large-scale SoC designs. The solution to the golden chip method is temporal self-referencing [5].

By comparing transient current signatures across multiple different time windows one can reveal the existence of Trojans without a golden chip. When multiple state transitions are undergone, transient current signatures change across a span of time windows in modified circuits. Trojan free designs on the other hand have a constant signature when following sequential logic. Using tools that log all signatures we can compare current signatures to past signatures and make the existence of Trojans known.

6. Conclusion

The existence of malicious hardware should be taken into more consideration when evaluating risk in cybersecurity. With software and firmware being the focal point, we have largely omitted the need to evaluate the circuitry responsible for executing these processes. By dissecting a hardware Trojan into multiple parts and highlighting critical development phases we can take measures to prevent and detect malicious modifications. When these modifications go undetected the IC design industry suffers.

From expensive products and contracts to high levels of mistrust we have experienced a shift in hardware design. Even more worrying is the existence of malicious hardware in current electronics. From counterfeit computer chips in the government and transportation vectors to Trojan infected missile detection systems the danger is present. With efforts placed on domestic manufacturing and trusted design houses, we have made strides in mitigating the risk. Sophisticated detection methods utilized by trusted design houses have restored faith in government contractors. Because of articles like “The Hunt for the Kill Switch” and news stories of multibillion-dollar domestic fabrication facilities awareness has grown but there is still a need for more.

7. References

[1] Activity, D. M. (n.d.). *DMEA Trusted IC Program*. Retrieved from DMEA: https://www.dmea.osd.mil/TrustedIC.aspx

[2] Adee, S. (2008). The Hunt for the Kill Switch. *IEEE Spectrum*.

[3] Alsop, T. (2020, July 10). *Arm's quarterly net sales worldwide 2017-2020*. Retrieved from Statista: https://www.statista.com/statistics/132064/arm-quarterly-net-sales-worldwide/

[4] Ba, P.-S., Palanichamy, M., Dupuis, S., Flottes, M.-L., Di Natale, G., & Rouzeyre, B. (2015). *Hardware Trojan Prevention using Layout-Level Design Approach.* ECCTD.

[5] Bhunia, S., Hsiao, M. S., Banga, M., & Narasimhan, S. (2014). *Hardware Trojan Attacks: Threat Analysis and Countermeasures.* IEEE.

[6] Daniel, B. (2020, July 27). *Counterfeit Electronic Parts: A Multibillion-Dollar Black Market*. Retrieved from Trenton Systems: https://www.trentonsystems.com/blog/counterfeit-electronic-parts

[7] *Dedicated Foundry*. (n.d.). Retrieved from TSMC: https://www.tsmc.com/english/dedicatedFoundry

[8] Desk, N. (2021, February 10). *5 Fabs Own 54% of Global Semiconductor Capacity*. Retrieved from EPS News: https://epsnews.com/2021/02/10/5-fabs-own-54-of-global-semiconductor-capacity/

[9] *Hardware trojan attacks and countermeasures*. (n.d.). Retrieved from Tech Design Forums: https://www.techdesignforums.com/practice/guides/hardware-trojan-security-countermeasures/

[10] Hicks, M., Finnicum, M., King, S. T., Martin, M. M., & Smith, J. M. (2010). *Overcoming an Untrusted Computing Base: Detecting and Removing Malicious Hardware Automatically.* IEEE.

[11] Jones, S. (2020, May 9). *Cost Analysis of the Proposed TSMC US Fab*. Retrieved from SemiWiki: https://semiwiki.com/semiconductor-manufacturers/tsmc/285846-cost-analysis-of-the-proposed-tsmc-us-fab/

[12] King, S. T., Cozzie, A., Grier, C., Jiang, W., & Zhou, Y. (2008). *Designing and implementing malicious hardware.* LEET.

[13] Li, H., Liu, Q., Zhang, J., & Lyu, Y. (2015). *A Survey of Hardware Trojan Detection, Diagnosis and Prevention.*

[14] Manners, D. (2020, May 20). *Top Ten Semiconductor IP Suppliers*. Retrieved from Electronics Weekly: https://www.electronicsweekly.com/blogs/mannerisms/ten-best/top-ten-ip-suppliers-2020-05/

[15] Robinson, W. H., Reece, T., & Mahatme, N. N. (2013). *Addressing the Challenges of Hardware Assurance in Reconfigurable Systems.*

[16] Tehranipoor, M. M., Guin, U., & Bhunia, S. (2017, April 24). *Invasion of the Hardware Snatchers: Cloned Electronics Pollute the Market*. Retrieved from IEEE Spectrum: https://spectrum.ieee.org/computing/hardware/invasion-of-the-hardware-snatchers-cloned-electronics-pollute-the-market

[17] The Committee's Investigation Into Counterfeit Electronic Parts in the Department of Defense Supply Chain. (2011, November 8).

[18] Tsoutsos, N. G., & Maniatakos, M. (2013). *Fabrication Attacks: Zero-Overhead Malicious Modifications Enabling Modern Microprocessor Privilige Escalation.* IEEE.

[19] Wang, X., Tehranipoor, M., & Plusquillic, J. (2008). *Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions.* IEEE.

[20] *Why Arm How Arm Licensing Works*. (n.d.). Retrieved from ARM.

[21] Yang, K., Hicks, M., Dong, Q., Austin, T., & Sylvester, D. (2016). *A2: Analog Malicious Hardware.* IEEE.