TAKSHASHILA INSTITUTION

A Survey of Chip-Based Hardware Backdoors

Satya S. Sahu

Takshashila Discussion Document 2024-06
Version 1.0, May 2024

This discussion document conducts a broad survey of chip-based hardware backdoors. The study attempts to examine different kinds of chip-based hardware backdoors, differentiates them based on where they can be inserted in the semiconductor global value chain, and assesses their real-world prevalence.

Recommended Citation:
Satya S. Sahu, "A Survey of Chip-Based Hardware Backdoors," Takshashila Discussion Document No. 2024-06, May 2024, The Takshashila Institution.

Executive Summary

This discussion document provides a broad survey of chip-based hardware backdoors — clandestine entry points built into semiconductor chips that allow unauthorised access and control over the systems where they are deployed.

The study examines different types of chip-based hardware backdoors, differentiates them based on where they can be inserted in the semiconductor global value chain (GVC), and assesses their real-world prevalence.

Chip-based hardware backdoors pose severe risks due to the ubiquity and meta-criticality of semiconductor chips across virtually every domain, from critical infrastructure to consumer electronics. These backdoors can enable espionage, data theft, and sabotage on an unprecedented scale while evading traditional security measures. The complex, globalised nature of the semiconductor GVC presents multiple opportunities for the insertion of backdoors by malicious actors.

The document identifies three main stages in the GVC where backdoors can feasibly be introduced: a) design, b) fabrication, and c) assembly, testing, marking, and packaging (ATMP). Each stage presents distinct challenges and attack vectors. The design stage is particularly vulnerable due to the use of third-party IP cores and electronic design automation

This document has been formatted to be read conveniently on screens with landscape aspect ratios. Please print only if absolutely necessary.

Author
Satya S. Sahu is a Research Analyst with the High-Tech Geopolitics Programme at the Takshashila Institution, Bengaluru, India.

He can be reached at
satya@takshashila.org.in

Acknowledgments
The Author would like to thank his colleague Pranay Kotasthane for his feedback and comments for this paper.

He also thanks G.S.Madhusudan for his valuable inputs.

(EDA) tools. In the fabrication stage, malicious modifications can be made to the photomasks, doping processes, or metal interconnects. The ATMP stage also offers opportunities for backdoor insertion through chip packaging and printed circuit board alterations.

Despite the grave risks posed by chip-based hardware backdoors, there is a striking lack of publicly confirmed real-world instances. This scarcity can be attributed to the extreme difficulty in detecting well-designed backdoors, the unfavourable risk-to-payoff ratio for attackers, the possibility of disguising backdoors as accidental vulnerabilities, and the reluctance of the hardware community to disclose such flaws.

Proactive policy efforts will be needed to build a more resilient and trustworthy semiconductor ecosystem that can withstand the evolving landscape of hardware security threats. This research aims to inform such efforts by providing a foundational understanding of the nature, feasibility, and prevalence of chip-based backdoors.

Table of Contents

I. Introduction

In 2018, Bloomberg published an explosive report alleging that Chinese spies had infiltrated the supply chain of Super Micro Computer Inc., an American company headed by a Taiwanese American, and one of the world's biggest suppliers of server motherboards, and planted tiny malicious microchips that provided a backdoor into the servers.[1] According to the report, these compromised servers made their way into data centres operated by dozens of companies, including Apple and Amazon, and allowed the attackers to create a stealth doorway into any network that included the altered machines. While the companies strongly denied the allegations and no definitive evidence has emerged, the story underscored the severe risks posed by the prospect of chip-based hardware backdoors in critical infrastructure.

The implications of these revelations are profound. In today's technological landscape, semiconductor chips play a fundamental and ubiquitous role across virtually every domain of human experience. They are not mere components but the bedrock upon which innumerable technologies and infrastructure rely, from power grids and water treatment facilities to transportation networks, military systems, and consumer electronics.[2]

Advancements in critical technologies are contingent upon access to a secure semiconductor supply chain, cementing chips as foundational to technological progression.[3] The hyper-globalised nature of the semiconductor supply chain necessitates international cooperation to ensure resilience, mirroring the intricate global manufacturing and distribution network involved in chip production.[4] Finally, the strategic employment of semiconductor supply-chain bottlenecks for geopolitical ends in recent years showcases the profound importance of chips in international relations and national security.[5]

This makes chips a "meta-critical" technology; indeed, their integrity and security are paramount to the functioning of modern society:[6]

Risks Posed by Hardware Backdoors

The existence of chip-based hardware backdoors in this context is a matter of grave concern. These backdoors — clandestine entry points deliberately built into the silicon itself, can provide covert access and control over the systems in which they are deployed, enabling espionage, data theft, and sabotage on an unprecedented scale. They operate at the lowest levels of the system and can evade traditional software-based security measures, making them extremely difficult to detect and mitigate.[7]

The security implications are massive, with hardware backdoors in critical infrastructure and consumer electronics enabling espionage, data theft, and sabotage.[8] These threats are exacerbated by the difficulty in detecting such covert mechanisms. Regarding privacy, hardware backdoors in consumer devices raise significant concerns, as they can be used by malicious actors to clandestinely gather sensitive personal information, infringing upon individual rights and civil liberties.

Their strategic use by state and non-state actors for espionage or cyber warfare can have substantial international ramifications, affecting international relations and national security, especially given the globalised nature of the semiconductor supply chain.[9]

Further, even the plausible presence of chip-based hardware backdoors can impede technological advancement, eroding trust in innumerable supply chains and hindering global trade. The complex and fragmented semiconductor supply chain presents many opportunities for inserting hardware backdoors, underscoring the imperative for governments and industry to understand, detect and mitigate the associated risks.

While previous studies have investigated theoretical hardware backdoors and their detection methods,[10] there is a lack of comprehensive research which could help inform policy to tackle threats posed by chip-based backdoors in the context of the semiconductor global value chain (GVC).[11]

The objectives of this research are threefold: **first**, to provide a broad overview of chip-based hardware backdoors; **second**, to identify the stages in the semiconductor global value chain where these backdoors are most likely to be inserted; and **third**, to assess their real-world prevalence.

This discussion document is, therefore, structured accordingly; it starts with an overview of chip-based hardware backdoors, their defining characteristics, and differentiates them from vulnerabilities. Then, it highlights the potential ways in which backdoors can be feasibly introduced at specific points in the GVC, and, finally, assesses their real-world prevalence by examining reported cases.

II. Understanding Hardware Backdoors

As a blanket term, hardware backdoors denote covert methods of bypassing normal authentication or security controls in a computer system (or devices like routers, etc.), which physically interact with or are embedded deep within the system's hardware itself.[12] An associated software component may or may not be required for these to be effective. Hardware backdoors can be intentionally designed into the hardware by the manufacturer or inserted by malicious attackers.[13]

Definitional Conundrums

It is also important to differentiate between backdoors, vulnerabilities, and design flaws. Making this distinction is crucial for accurately assessing security risks and formulating appropriate responses to them. There are four key distinguishing features:

1) **Intent**: Backdoors are intentionally created and embedded into the hardware for unauthorised access or control. This can be done either by the hardware manufacturer or by an attacker who has inserted it during one or more of the supply chain's design, fabrication, and assembly stages. In contrast, vulnerabilities or design flaws like Spectre

Unlike intentional hardware backdoors, Spectre and Meltdown are critical flaws inadvertently introduced in modern processors. These vulnerabilities stem from performance optimisations like speculative execution and out-of-order execution.
While intended to speed up processors, security implications were overlooked, allowing unprivileged processes to access restricted memory. Spectre and Meltdown affect Intel, AMD, and ARM chips, impacting billions of devices.
Mitigating them requires redesigning processors and patching operating systems, often at the cost of reduced performance.

or Meltdown are unintentional weaknesses or errors in the chip design or fabrication process. They are not created deliberately but arise from oversights, errors, or lack of foresight in the design and production stages.[14]

2) **Origin**: Backdoor creation is deliberate, either by someone with malicious intent or as a "hidden feature" by the manufacturer for reasons such as diagnostics, maintenance, or state surveillance.[15] In the case of the former, the origin is an attacker who has surreptitiously compromised a particular stage of the supply chain. In the latter case, the vendor that designs the chip makes the decision to implement a backdoor voluntarily or upon compulsion by the government.[16] In this respect, kill switches in John Deere's tractors,[17] or Intel's Management Engine,[18] can be considered backdoors even though both seem to be accepted as industry practice.

   John Deere tractors have incorporated a "kill switch" feature that allows the company to disable and render any tractor reported stolen remotely inoperable. This functionality is built into the hardware and firmware of the tractor as an anti-theft measure.[19] While intended as a security feature, it has sparked a debate on manufacturers' power to remotely access and control devices without the end user's knowledge or consent.

Intel's Management Engine (ME) is an example of a hardware backdoor built into Intel chipsets by the manufacturer. The ME is an autonomous subsystem that has full access to memory, the network stack, and cryptography engine. While intended for remote administration, critics argue the ME could enable surveillance by Intel or third-parties. The ME's code is proprietary and cannot be audited. Researchers have uncovered vulnerabilities in the ME that could be exploited by attackers. Although Intel maintains the ME is not a backdoor, its privileged access, opacity, and history of flaws make it a concerning example of manufacturer-included hardware backdoors and their risks

Intel's Management Engine (ME) is an autonomous subsystem incorporated into virtually all Intel processor chipsets since 2008.[20] It comprises a microcontroller onboard Intel CPUs and proprietary firmware running on a separate microprocessor in vendor motherboards, with extensive system hardware access, including networking and storage.[21] The ME runs continuously, even when the system is powered off, and has been criticised by security experts as a potential backdoor due to its privileged level of hardware access and the fact that it could not, for a long time, be disabled or audited.[22]

3) **Impact**: Backdoors provide a covert means of bypassing security controls, allowing unauthorised access or control over the system to carry out any range of attack vectors. Attackers can also exploit vulnerabilities or design flaws to compromise systems. However, unlike backdoors, they are not designed for a bespoke purpose and may or may not be discovered and leveraged to perform similarly impactful actions. Assessment of the seriousness of the risks posed by either backdoors or vulnerabilities is essential to any policy response. This distinction can be cloudy, and backdoors are generally accepted as a subset of hardware vulnerabilities.[23]
4) **Detection and Mitigation**: Detecting backdoors can be extremely challenging, especially chip-based backdoors, as they are intentionally obfuscated and can operate at the most fundamental level in a system.[24] Examination or reportage of discovered real-world examples of chip-based hardware backdoors is minimal.[25] This means that there is no

Despite the severe risks posed by hardware backdoors, concrete examples are rarely reported publicly. Researchers have demonstrated proofs-of-concept, like the stealthy "A2" backdoor requiring just one malicious component among billions. However, companies and governments are reticent to disclose discovered incidents, likely fearing reputational and security implications.
Notable exceptions include counterfeit Cisco routers with backdoors around 2008, and an alleged 2018 supply chain attack on Apple and Amazon servers, which the companies disputed. Overall, public understanding of real-world chip backdoors remains limited.

> single systematic methodology for investigating their presence outside of theoretical simulations, and this hurdle will become progressively difficult to surmount as chip complexity grows.[26]
>
> As chips become larger and more complicated with billions of transistors, there are more opportunities to hide malicious circuits. Backdoors could remain dormant and be triggered by obscure combinations of events that are impractical to test exhaustively.[27] [28] While vulnerabilities can also be difficult to detect, especially in complex systems, they are generally more straightforward to identify, as they are not intentionally concealed from the scrutiny of security researchers. These can often be mitigated through design revisions, patches, or recalls.

For the purposes of this research document, the definition of hardware backdoors excludes vulnerabilities or design flaws in its scope. However, including hardware backdoors at the Printed Circuit Board (PCB) level is pertinent here. Even though they exist at different levels as hardware, board-level backdoors can be inserted at the assembly and packaging stage of the semiconductor supply chain.

Chips only gain their functionality upon being mounted on PCBs. Therefore, board-level backdoors may have similar low-level system access that is also beyond the reach of most software-based security measures. For example,

small electronic devices can tap into PCB traces and chip pins to alter functions and implant malware.[29] They are also similar to chip-based backdoors in terms of their persistence characteristics, the detection and mitigation challenges posed,[30] and the ability to be tailored for a wide range of attack functions like intercepting data, injecting malicious code, or creating hidden communication channels.[31]

Finally, board-level backdoors raise similar supply chain security concerns as chip-based backdoors. The manufacturing process of PCBs, which often involves multiple suppliers and complex production lines, can be susceptible to tampering or the insertion of unauthorised components.[32]

We can assess a more comprehensive spectrum of hardware-level security threats by considering board-level backdoors within the broader definition of chip-based hardware backdoors. Therefore, a more relevant term incorporating this definition would be "**chip and board-based backdoors**", wherever applicable.

It should be noted that within the scope of this paper, different types of chips (memory vis a-vis logic chips) are grouped together for simplicity's sake. Also, while outside the scope of this paper, firmware-based detection and mitigation strategies for hardware backdoors merit further study. Firmware can be considered an intrinsic part of the hardware itself, as they are tightly coupled together. We will touch upon it briefly in this paper, but since the

supply chain for firmware is very different and not always intertwined with the supply chain for chips and PCBs, we have excluded it from the paper's purview.

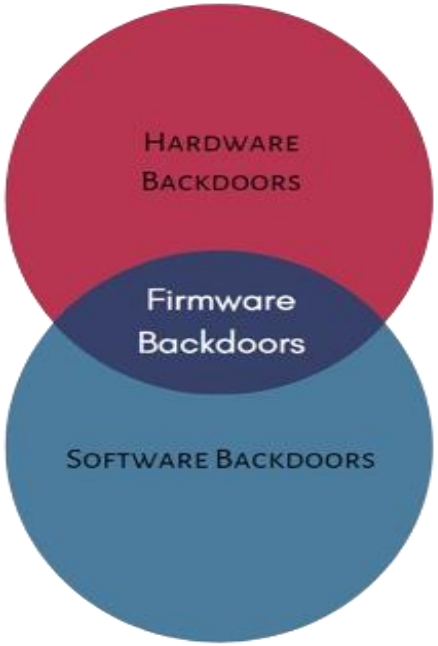

Figure 1: Author's Visualisation

Types of Hardware Backdoors

Hardware backdoors and Trojans refer to the same concept: malicious modifications to chip circuitry that compromise system security. Like the misleading Trojan Horse of Greek mythology, hardware Trojans are disguised as normal components but contain hidden malicious functionality. Once triggered, they can leak secrets, degrade performance, or cause failures. The terms "backdoor" and "Trojan" are used interchangeably for such attacks at the hardware level.

While discussing chip and board-based hardware backdoors specifically, it is useful to understand the taxonomy of hardware backdoors in general. Tehranipoor et al. provide a useful framework for classifying different types of "hardware trojans", categorising them according to their physical, activation, and action characteristics:

1. **Physical characteristics** cover how the backdoor changes the Integrated Circuit's (IC) function or performance (for instance, does it add or delete gates or modify wiring and logic), its size (number of components affected), distribution (its location in the circuit/chip), and structure (changes in the chip's physical layout).
2. **Activation characteristics** cover how the backdoor is triggered. Backdoors can either be triggered externally (by something outside the chip, like a sensor that interacts with its environment or other hardware) or internally (where the backdoor is always active and is activated by a specific condition, such as a sensor output, certain input patterns, or internal logic state). For example, a backdoor might only activate when a specific key combination is entered or when a certain date is reached. This makes such backdoors harder to detect during normal operation, as they do not observably affect the system's functionality until the trigger condition is met.

3. **Action characteristics** describe backdoors in terms of how they modify the chip's functions (in other words, the attack pattern of the backdoor); a backdoor could engage in Denial of Service, change a function, leak or transmit information, or degrade the chip's performance.

Characteristics of Chip and Board-Based Hardware Backdoors

Chip and Board-based backdoors differ from other hardware backdoors in four key aspects:

1) **Integration Level**: These backdoors are embedded directly into the silicon of the processor or microchip (or the PCB), whereas other hardware backdoors might exist in peripheral devices or firmware.[33]
2) **Access and Control**: Due to their location in the core computational hardware, chip and board-based backdoors can potentially control or access all operations performed by the device, including data processing, encryption/decryption, and communication, whilst other kinds of backdoors usually only interact with one of these functions.[34]
3) **Detection Difficulty**: Detecting such backdoors is extremely challenging because they operate at the silicon die level and can evade most software-based security checks. Specialised equipment and

expertise are often required to analyse the hardware for potential backdoors.[35]

4) **Mitigation or Persistence**: These backdoors are typically unaffected by software updates, factory resets, or operating system changes, making them more persistent and difficult to mitigate than software-based backdoors. Mitigation strategies also usually involve compromising the chip's capabilities. Other kinds of hardware backdoors can either be physically removed or rendered inert.[36]

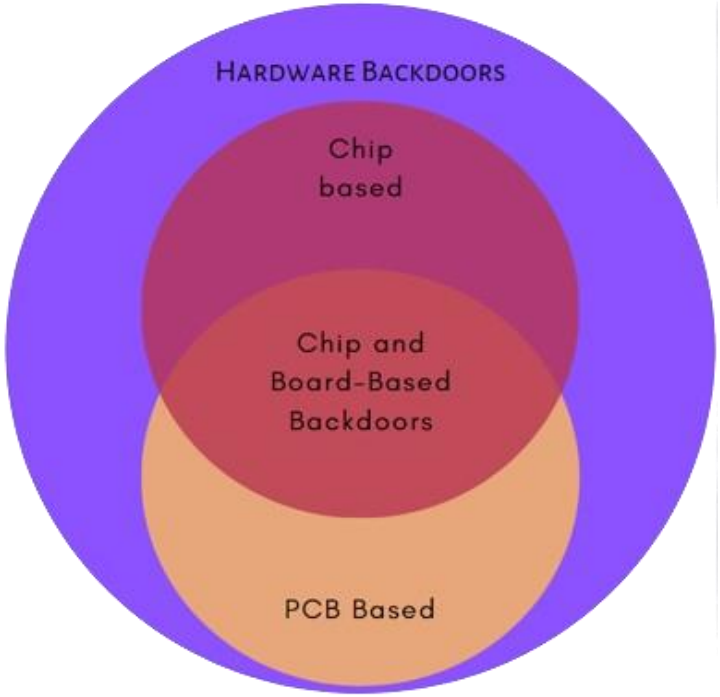

Figure 2: Author's Visualisation

However, in order to craft broadly actionable policy strategies for the prevention, detection, and mitigation of the risks posed, it would be more useful to differentiate chip and board-based hardware backdoors based on where they can be feasibly inserted in the semiconductor GVC.

III. Where Can Backdoors be Inserted?

The semiconductor GVC is a complex, globalised network involving multiple stages and actors, from design to final integration. Each stage presents unique opportunities and challenges for the insertion of hardware backdoors.

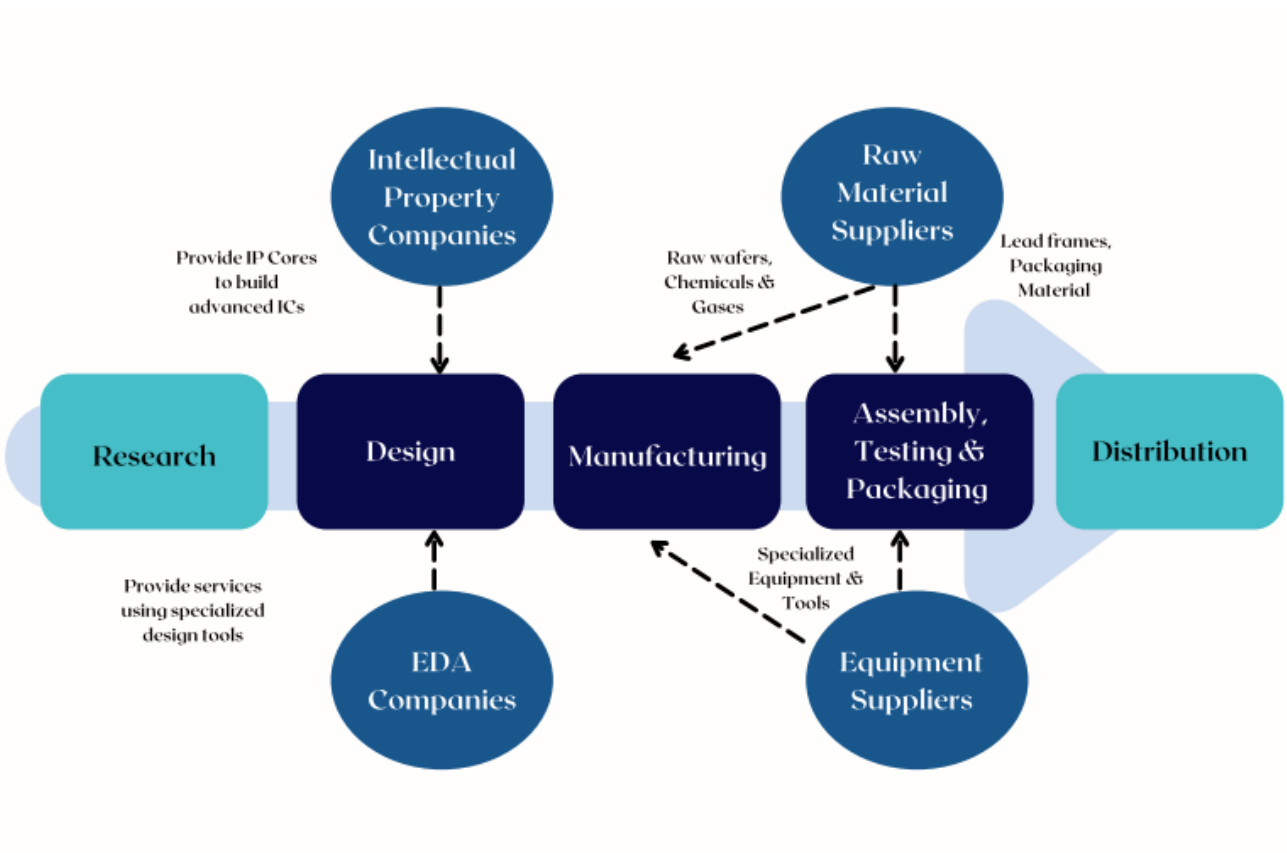

Figure 3: Simplified View of the Semiconductor Value Chain (Takshashila Discussion SlideDoc, India's Semiconductor Ecosystem: A SWOT Analysis)[37]

There are three broad segments: **design**, **fabrication**, and **ATMP** (assembly, testing, marking, and packaging). All three segments offer potential points for the insertion of hardware backdoors. Above is a simplified depiction of the semiconductor GVC.

1) **Design Stage**: The design stage of the semiconductor supply chain is a critical point where chip-based hardware backdoors can be introduced, as it involves the development of the chip's architecture, logic, and physical layout.[38] This stage is typically carried out using Electronic Design Automation (EDA) tools,[39] and involves multiple levels of abstraction, from high-level behavioural descriptions to low-level transistor layouts.

   Backdoors inserted at the design stage can be particularly challenging to detect, as they can be deeply embedded into the chip's logic and may not be visible in the final manufactured product,[40] especially when they do not affect its observable performance and functionality.

   These backdoors can be introduced by rogue designers through the use of untrusted third-party Intellectual Property (IP) cores or by compromised EDA tools.[41]

   a) **Rogue Designers**: A malicious designer could deliberately insert a hardware backdoor into the chip's design by adding or modifying logic gates or other components. For example, a designer could add a hidden circuit that bypasses security checks or leaks sensitive information when triggered by a specific input sequence. Such backdoors can be carefully crafted to minimise

The semiconductor GVC has become increasingly fragmented and geographically concentrated to optimize for efficiency and cost. For example, 75% of manufacturing is in China and East Asia, while the US leads in design and equipment. This pursuit of specialization over resilience has made the semiconductor GVC susceptible to geopolitical tensions, natural disasters, and infrastructure failures.

their impact on the chip's overall functionality and to evade detection during standard verification and testing procedures.[42]

b) **Untrusted Third-Party IP Cores**: Modern chip designs often incorporate pre-verified third-party IP cores (pre-designed circuit blocks that implement a specific function and can be integrated into the overall chip design) to reduce development time and cost.[43] Using third-party IP allows chip companies to focus on their unique value-add and differentiated designs rather than re-implementing standard functions. Common types of third-party IP include processors, memory controllers, I/O interfaces, analogue blocks, etc.[44] However, these IP cores could contain hidden backdoors if sourced from untrusted vendors.[45] An attacker could modify an IP core's design to include malicious logic or create an entirely new IP core with a built-in backdoor. When integrated into the larger chip design, these compromised IP cores can introduce vulnerabilities that can be exploited later.[46]

c) **Compromised EDA Tools**: The complex design process relies heavily on EDA tools for tasks such as synthesis, place-and-route, and verification. If an attacker compromises these tools, they could feasibly insert backdoors into the chip design without the designer's knowledge.[47] For instance, a malicious synthesis tool could add extra logic gates or modify the netlist[48] to create a backdoor circuit. Compromised place-and-route tools could

The EDA industry is dominated by an oligopoly of three companies - Synopsys, Cadence, and Siemens EDA - which control about 70% of the global market. Their tools are essential for chip design across the semiconductor supply chain. This concentration makes the EDA industry a potential chokepoint; compromising widely-used EDA tools could enable backdoors across many chip designs. The oligopoly's stability is reinforced by high switching costs and the need for tool interoperability and standardisation.

create covert channels by manipulating the chip's physical layout.[49] [50] [51]

Design-for-Testability (DFT) and formal verification are two important approaches for ensuring the security of semiconductor chips. DFT involves adding special circuitry to chips to enable thorough testing for manufacturing defects that could be exploited by attackers. Formal verification mathematically proves that the chip's design matches its intended secure functionality, identifying any discrepancies or potential vulnerabilities.

The feasibility and ease of inserting backdoors at the design stage depend on several factors, including the attacker's skill level, their access to the design process, and the complexity of the chip design.[52] If we assume that a skilled attacker has infiltrated a design vendor and has direct access to the design files and tools, inserting a backdoor can be relatively straightforward, especially if they are familiar with the chip's architecture and functionality. They can carefully craft the backdoor logic to minimise its impact on the chip's performance and power consumption, making it harder to detect.

If the attacker doesn't have direct access to the design files, they may still be able to introduce backdoors by compromising the Electronic Design Automation (EDA) tools or the IP cores used in the design. This can be more challenging, as it requires keeping other design team members in the dark, as well as finding and exploiting vulnerabilities in these tools or cores (which are typically proprietary and resistant to unscrutinised modifications), but it can also be more effective, as it can potentially affect multiple chip designs that use the same compromised components.[53]

The complexity of the chip design itself can influence the feasibility of backdoor insertion. In larger, more complex designs with millions of gates

and multiple IP cores, it may be easier for an attacker to hide a backdoor among the legitimate circuitry. On the other hand, smaller, simpler designs may be more amenable to thorough verification and testing, making it harder for backdoors to go unnoticed.[54]

2) **Fabrication stage**: This stage involves the physical production of chips based on the design files provided by the design house. It is often outsourced to third-party foundries, typically located overseas, to reduce costs. The globalised and opaque nature of IC manufacturing means that complete oversight of the process from the design firm may be more difficult to achieve.[55]

   Again, our theoretical assumptions are that the attacker has infiltrated a third-party foundry, and has privileged enough access to compromise formal verification procedures. Having assumed that, there are several points during fabrication where a hardware backdoor can be inserted:

   a) **Mask Modification**: The photolithography process uses a series of photomasks to transfer the chip design onto the silicon wafer. An attacker with access to the mask generation process could modify the masks or GDSII layout to add, remove, or alter specific features like logic gates, effectively creating a hardware backdoor.[56] [57] These modifications can be as minor as making changes to the dopant polarity of a few transistors. For example,

Chip fabrication involves multiple stages, each presenting opportunities for backdoor insertion if proper oversight is lacking. Photolithography, which transfers the chip design onto the silicon wafer, could be subverted to modify circuits or add malicious logic. During etching, extra connections or gates could be discreetly added. Doping, which introduces impurities to alter electrical properties, might be exploited to create hard-to-detect triggers. Subtle changes in deposition of conductive/insulating layers could create hidden pathways. Testing could be compromised to mask backdoor presence. While such attacks require deep technical sophistication, the globalised supply chain and reliance on third-party fabs make it challenging to maintain full oversight, necessitating rigorous assurance measures.

an attacker could modify the metal layer mask to create a covert communication channel between different parts of the chip, enabling it to leak sensitive information or bypass security measures.[58] However, the general consensus seems to be that the photomask and wafer manufacturing stage is less feasible for backdoor insertion due to the number of processes attackers must get access to.[59]

b) **Doping Alteration during fabrication**: The electrical properties of the transistors on the chip are controlled by the precise doping of the silicon substrate with impurities. An attacker could alter the doping process to create regions with different electrical characteristics, which could be exploited as a trigger or payload for a hardware backdoor. For instance, an attacker could create a "doping bridge" between two unconnected parts of the chip, allowing them to short-circuit the device under specific conditions.[60]

c) **Interconnect Modification**: The metal interconnects that carry signals between different parts of the chip are created using a combination of deposition, etching, and planarisation processes. An attacker could modify these processes to alter the routing or timing of specific signals, creating a hardware backdoor that is activated by a specific sequence of events.[61] For example, an attacker could modify a circuit carrying a signal, causing a delay

that could be exploited to bypass authentication or enable a malicious function.[62]

d) **Compromising post-fabrication verification**: After fabrication, chips undergo testing to check for defects and correct functionality. During this stage, a malicious foundry could substitute backdoor-infected chips for genuine ones and, therefore, disguise infected chips within batches of genuine ones as they move on to the ATMP stage of the GVC.

The feasibility and ease of inserting a fabrication-stage hardware backdoor depends on various factors, including the complexity of the chip design, the security measures in place at the foundry, and the resources and expertise of the attacker. In general, fabrication-stage backdoors are considered to be more difficult to insert than design-stage backdoors, as they require physical access to the manufacturing process and a deep understanding of the chip's layout and materials.[63]

However, the difficulty of detecting and mitigating fabrication-stage backdoors also makes this a highly attractive attack vector with the potential for a large payoff. An adversary with access to a foundry has a high degree of control over the fabrication process and can customise backdoors to be extremely stealthy. The fragmented nature of the semiconductor GVC makes it challenging to ensure the security and integrity of components, equipment, and processes. The industry's economic imperative focuses on

GDSII (Graphic Design System II) is a binary file format used to represent integrated circuit layouts for fabrication. Developed by Calma in the 1970s, it has been the de facto industry standard for decades. GDSII files contain planar geometric shapes, text labels, and hierarchical information that define the physical layout of a chip. Each shape is assigned attributes like layer number, datatype, etc. During fabrication, photolithography transfers the GDSII layout onto silicon wafers layer by layer. The wafer is coated with photoresist, a mask containing the GDSII pattern for one layer is aligned, and the resist is exposed and developed. By repeating this process with masks for each layer, the complete chip is manufactured based on the GDSII specification.

reducing costs,[64] and consequently, includes numerous actors spread across multiple regions. Therefore, the threat surface at this stage can also be fairly expansive.

Attackers may be able to exploit weaknesses in the supply chain, such as unsecured communication channels or untrusted third-party vendors, to introduce backdoors or compromised materials. Moreover, as mentioned earlier, the increasing complexity and transistor density of modern chips can make it easier for attackers to hide backdoors among the billions of transistors and interconnects.[65] The use of advanced packaging techniques, such as 3D integration or multi-chip modules, can also create new opportunities for attackers to introduce backdoors at the interface between different components.

Advanced packaging techniques that combine multiple chips, like 3D stacking or multi-chip modules (MCMs), rely on complex interconnects between components. These interfaces, such as microbumps, through-silicon vias (TSVs), and interposers, present new attack surfaces. Malicious modifications to interconnect layouts could create subtle backdoors that are difficult to detect. For example, a compromised interposer could enable unauthorised communication between chiplets or leak sensitive data. The disaggregation of designs across multiple dies also introduces security risks, as each die may come from different sources with varying levels of trust. Comprehensive security analysis of the entire heterogeneous system therefore becomes critical.

3) **ATMP stage**: The assembly, testing, marking, and packaging (ATMP) stage is the final phase of the semiconductor manufacturing process before chips are shipped to customers. It involves dicing the fabricated wafers into individual dies, packaging the dies into protective enclosures, integrating them onto PCBs, and thoroughly testing the packaged chips to ensure they meet specifications.[66] This stage often takes place in separate facilities than ones involved in the fabrication

stage and may involve multiple suppliers and subcontractors spread out across different regions.

There are multiple points during the ATMP flow where a malicious actor could potentially implant a chip and board-based hardware backdoor; by modifying the chip packages, altering the testing procedures, or tampering with the PCB assembly process. For example, a compromised assembly facility could add a malicious component to the PCB that interacts with the chip to enable a backdoor.[67]

a) **Packaging Modification**: Post fabrication, bare dies are assembled to be packaged into finished chips. A sophisticated attacker could replace legitimate dies with malicious ones containing backdoors during this packaging process.[68]
b) **PCB Alteration**: Apart from swapping out legitimate chips with malicious ones on the PCB, attackers could modify the PCB itself to introduce backdoors via disguised and compromised components.[69] As mentioned earlier, PCB-level backdoors can be as powerful as chip-level ones.[70]
c) **Testing**: Packaged chips and assembled PCBs undergo extensive testing to verify functionality, performance, and security. Attackers could compromise the test environment to falsely pass malicious chips off as legitimate ones. Backdoors could also be

inserted during provisioning when firmware, security keys, and configurations are programmed into chips.[71]

d) **Re-marking and counterfeiting**: Chips that fail testing may be discarded but then fraudulently remarked as legitimate and resold on grey markets. Attackers could acquire defective or lower-grade chips and remark them as high-assurance versions, potentially with backdoors added during the remarking process.[72]

The feasibility and ease of inserting backdoors at the ATMP stage depends on factors like the complexity of the chip package and PCB design, the security controls and oversight in place, and the resources and capabilities of the attacker. However, here too, the heterogeneous nature of the ATMP stage makes it an attractive target for backdoor insertion. The process involves numerous different suppliers, equipment, and materials — from chip packaging facilities to substrate vendors to PCB assembly and test facilities. This globalised supply chain is opaque to end customers and, therefore, provides ample opportunities for malicious actors to infiltrate.

Firmware as a Potential Vector

Firmware is a type of low-level software that is permanently embedded into a hardware device's non-volatile memory (which means it persists even if the device is switched off), and is a combination of persistent memory, program code, and data stored in the memory chip.[73] It provides the necessary instructions for how the device should operate and communicate with other hardware components (processors-memory-peripherals). Firmware is crucial for controlling the core functions of a device at a fundamental level and acts as an interface between the hardware and higher-level software such as operating systems and applications. It is usually not meant to be frequently updated, and is device-specific. Examples of firmware can include a PC's UEFI/BIOS or even a simple program handling the functioning of a basic kitchen appliance like a toaster.[74]

Firmware, UEFI, and BIOS are stored in non-volatile memory like flash memory or ROM on a device's motherboard. This allows the low-level software to retain critical settings and code even when the power is turned off. For example, BIOS contains boot instructions, hardware initialization routines, and configuration data in its non-volatile memory. UEFI firmware also resides in non-volatile memory, storing boot manager code and system settings. Firmware in other devices like hard drives, SSDs, GPUs, and peripherals is also held in their own integrated non-volatile memory. This persistent storage enables the firmware to provide consistent low-level hardware control across power cycles.

Firmware is critical for initialising hardware during the boot process, managing power and memory, and enabling communication between different parts of the system.[75] Its essential role, deep integration, and privileged access, therefore, also make it a powerful vector for inserting chip-based hardware backdoors, as the functionality of the backdoor needs to be triggered, monitored, and exploited by the firmware. Malicious modifications to firmware can enable unauthorised access and control over a

device in ways that are extremely difficult to detect and mitigate.[76] It shares similar characteristics with physical chip-based hardware backdoors:

1) **Stealth**: Firmware backdoors can operate below the level of the operating system and applications, making them invisible to most security software. They can hide from debuggers and evade detection during verification and testing. Backdoors could be triggered by external input like specially crafted network packets or by internal conditions like timers.
2) **Persistence**: Firmware backdoors can survive OS reinstalls and hard drive wipes. Some firmware is never updated during a device's lifetime, allowing backdoors to persist indefinitely.[77]
3) **Privilege and Control**: Firmware could have unfettered access to hardware and memory. Backdoors can abuse this to escalate privileges, circumvent security boundaries, and access protected data, thereby altering the hardware functionality, compromising computations, transmitting sensitive data, or causing denial-of-service.

In theory, detecting backdoors in firmware could be easier than finding them in hardware, since firmware is essentially software and can potentially be read out and analysed. However, they are still challenging to detect due to two factors:

1) **Opaque designs**: Much firmware is proprietary and publicly undocumented. Chip vendors tightly control access to firmware source code and design documentation, making third-party audits difficult.[78]

Some vendors encrypt firmware binaries, which protects against modification but also hinders security audits. Vulnerabilities and backdoors could hide in encrypted firmware indefinitely. [79]

2) **Complexity**: As chips grow more sophisticated, firmware complexity is increasing exponentially. Manual analysis of firmware is very time-consuming and impractical, and therefore, does not cater to the economic imperative of the semiconductor industry (in which time-to-market is critical).[80]

However, further study is needed to map the supply chain for firmware, in order to reliably pinpoint specific points where backdoor could feasibly be inserted, and how these could be detected and mitigated.

IV. Prevalence and Real-World Cases of Chip and Board-Based Backdoors

The potential existence and proliferation of chip and board-based hardware backdoors have become a growing concern in recent years as the complexity of the semiconductor GVC has increased, and reliance on outsourced design

and manufacturing has become more prevalent.[81] While numerous research papers and theoretical studies have explored how hardware backdoors could be inserted into ICs and the potential countermeasures that could be employed to detect and mitigate these threats, there remains a striking lack of concrete evidence and confirmed real-world instances of such backdoors.[82]

Prima facie, the scarcity of verified real-world cases raises important questions about the true prevalence and impact of these perceived threats based on which nation-states worldwide have begun efforts to enact countermeasures. It also calls into question the effectiveness of current detection and prevention methods.

The absence of verifiable cases of hardware backdoors is likely due to the following factors:

1) **Difficulties in Detection**: The lack of public evidence does not necessarily mean backdoors aren't present in some chips. Detecting a well-designed hardware backdoor is extremely challenging. Backdoors would be designed to be stealthy and difficult to detect using traditional testing and verification methods. They may be triggered only under specific, rare conditions and may not observably affect the chip's normal functionality, making them challenging to identify through standard functional testing or performance analysis. They could potentially stay dormant for years until activated by an external

signal. Furthermore, certain detection strategies are extremely expensive to conduct at scale.[83]

The globalised and fragmented nature of the semiconductor GVC makes it difficult to trace the provenance and integrity of all components and design elements used in a chip.[84] Fabless semiconductor companies, outsourcing their chip fabrication to third-party foundries, may not have full visibility into the manufacturing process and cannot always verify that their designs have not been tampered with.

Many chip designs and Third-Party IP cores are proprietary and closely guarded by their owners, making it difficult for third parties to inspect and validate the hardware for potential backdoors. This lack of transparency and independent auditing creates opportunities for malicious actors to introduce backdoors without detection.

Finally, the semiconductor industry is driven by intense competition, cost pressures, and time-to-market demands,[85] which can disincentivise companies from investing in comprehensive hardware security measures and rigorous testing procedures. The high costs and technical challenges associated with detecting hardware backdoors may deter companies from prioritising this issue, especially if the perceived risk or impact is considered low.

2) **Practicality and Risk**: While hardware backdoors are technically possible, actually implanting them in real-world products may be too expensive and risky for most attackers. Modifying chip designs requires deep knowledge of the target device and specialised skills that are difficult to acquire covertly. Rogue elements inserted during design, fabrication, or ATMP stages must avoid detection by the firm's vetting, testing and quality control processes. Backdoors are more likely to be deployed selectively against high-value targets rather than risking exposure through widespread proliferation via the supply chain. Attackers may calculate that the potential blowback from discovery exceeds the benefits of mass-deploying backdoors.

3) **Intentional Disguise as Vulnerabilities**: Instead of explicitly implanting backdoors, attackers could introduce subtle flaws or vulnerabilities into chip designs that appear accidental but enable exploitation later. Such "bugdoors" would be difficult to conclusively distinguish from the numerous unintended defects that could inevitably slip through the design process. This approach would sacrifice some of the stealth and versatility of a purpose-built backdoor but provide plausible deniability for a rogue actor within the supply chain if discovered. Bugdoors could also arise from careless design practices or underinvestment in security that is discovered by a rogue actor who can then exploit it. Remote control or kill switches built into chips,

boards, or firmware, that are inserted as management or diagnostic features into electronic products, are also protected from scrutiny due to intellectual property protections (as patents or trade secrets etc.) and therefore, may prevent an accurate assessment.

Despite these challenges, two publicly reported examples (however not sufficiently substantiated in some cases) provide some insights into their real-world implications:

1) **Actel/Microsemi ProASIC3 FPGA Backdoor**: Researchers from Cambridge University discovered a backdoor in the Actel/Microsemi ProASIC3 chip, which is used in military and industrial applications. Using a technique called Pipeline Emission Analysis (PEA), they were able to extract the key to activate the backdoor and access unencrypted configuration data, reprogram other crypto and access keys, modify low-level silicon features, or permanently damage the device. This backdoor was not present in the chip's firmware but in the actual silicon hardware. It's unclear whether the backdoor was intentionally inserted by the manufacturer or a malicious actor in the supply chain.[86]

   While there has been limited information about the real-world prevalence or exploitation of this backdoor beyond the initial research paper published by the researchers, it nevertheless demonstrates the difficulty in detection and the potential impact on critical military systems.

Pipeline Emission Analysis (PEA) is an advanced technique used to detect security vulnerabilities in semiconductor chips. It analyses the chip's electromagnetic emissions during operation to extract sensitive data like encryption keys. PEA provides much higher signal sensitivity than traditional power analysis methods by focusing on the chip's specific areas of interest. This allows PEA to break the security of chips previously considered "unbreakable" in a matter of seconds, posing a serious threat to the semiconductor industry if misused

2) **Supermicro Server Backdoor Allegations**: In 2018, Bloomberg reported that tiny malicious chips had been found on Supermicro server motherboards that allegedly created backdoors for Chinese spies. According to the article, these chips were inserted during the manufacturing process in China and could allow attackers to remotely access and compromise the servers.[87] [88] However, this report was met with strong denials from the companies involved (Apple, Amazon, Supermicro), and no concrete evidence of the alleged backdoor chips was presented. Subsequent investigations by security researchers and government agencies did not substantiate Bloomberg's claims.[89] Despite the lack of credible evidence, this case is indicative of the challenges inherent in verifying and attributing such attacks.

There are also examples of vulnerabilities (not backdoors) such as those discovered in Xilinx FPGAs,[90] or in Intel, and AMD processors (Spectre and Meltdown),[91] with similarly catastrophic potential for exploitation. Beyond this, there are a multitude of research papers and presentations that demonstrate the feasibility of various types of hardware backdoors, such as analog malicious hardware,[92] [93] dopant-level Trojans,[94] and supply chain security in system-on-chip (SoC) designs.[95] However, these are proofs-of-concept or theoretical attacks rather than confirmed cases of backdoors in commercially available products.

On one hand, the absence of definitive proof of widespread hardware backdoors could be seen as a reassuring sign, suggesting that the existing security measures and testing procedures in the semiconductor supply chain are effective in detecting and preventing the insertion of malicious modifications. It may also indicate that the incentives and risks associated with introducing hardware backdoors are not as compelling for attackers.

Finally, voluntary disclosure of a backdoor by a chip firm can be more damaging than one made by a software firm, since the latter is much better-understood and the former can be very powerful and potentially unpatchable. The norms in the hardware community around backdoors is therefore, characterised by a reluctance to discuss their real-world prevalence.[96]

That said, the lack of publicly verified real-world instances does not necessarily mean chip-based hardware backdoors don't exist, but it does highlight the difficulties in detecting and attributing such attacks. A combination of technical complexity, supply chain diversification and opacity, economic disincentives, and the absence of an imperative to share information, may contribute to the gap between theoretical risks and publicly confirmed real-world incidents.

V. Conclusion

The examination of the semiconductor GVC reveals that hardware backdoors can be introduced at multiple stages: design, fabrication, and ATMP. Each stage presents distinct opportunities and challenges for the insertion of backdoors, with varying levels of feasibility and complexity.

Significant difficulties remain in detecting and confirming the presence of chip-based hardware backdoors in real-world systems. Both, the inherent complexity and opacity of modern chip designs, as well as the especially covert nature of these backdoors, contribute to the challenge of identification, detection, and mitigation. Further research into policy and technical solutions for the detection and mitigation of such backdoors tailored to each of these stages is needed.

Beyond these stage-specific efforts, there is an overarching need for comprehensive approaches to ensuring the security and integrity of the semiconductor GVC. This may involve the development of new standards and best practices for secure chip design, manufacturing, and testing, as well as the establishment of trusted supply chain partnerships and improved information sharing among industry stakeholders.

VI. References

[1] Robertson, Jordan, and Michael Riley. "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies." *Bloomberg*, October 4, 2018. https://archive.is/n3Xov.

[2] Shivakumar, Sujai, and Charles Wessner. "Semiconductors and National Defense: What Are the Stakes?" Center for Strategic and International Studies, June 8, 2022. https://www.csis.org/analysis/semiconductors-and-national-defense-what-are-stakes.

[3] Sawbridge, Oliver. "Supply Chain Resilience: Semiconductor Autonomy." *Economist Impact - Perspectives* (blog), October 13, 2022. https://impact.economist.com/perspectives/economic-development/supply-chain-resilience-semiconductor-autonomy.

[4] Reinsch, William A., Emily Benson, and Aidan Arasasingham. "An Affirmative Agenda for International Cooperation." Center for Strategic and International Studies (CSIS), 2022. http://www.jstor.org/stable/resrep42770. ;
Benson, Emily, Japhet Quitzon, and William Alan Reinsch. "Securing Semiconductor Supply Chains in the Indo-Pacific Economic Framework for Prosperity." CSIS, May 30, 2023. https://www.csis.org/analysis/securing-semiconductor-supply-chains-indo-pacific-economic-framework-prosperity.

[5] Shivakumar, Sujai, Charles Wessner, and Thomas Howell. "Balancing the Ledger: Export Controls on U.S. Chip Technology to China." CSIS, February 21, 2024. https://www.csis.org/analysis/balancing-ledger-export-controls-us-chip-technology-china. ;

Park, Seohee. "Semiconductors at the Intersection of Geoeconomics, Technonationalism, and Global Value Chains." *Social Sciences* 12, no. 8 (August 21, 2023). https://doi.org/10.3390/socsci12080466.

[6] Kotasthane, Pranay, and Abhiram Manchi. *When the Chips Are Down*. Bloomsbury Publishing, 2023.

[7] Simonite, Tom. "NSA's Own Hardware Backdoors May Still Be a 'Problem from Hell.'" *MIT Technology Review*, October 8, 2013. https://www.technologyreview.com/2013/10/08/176195/nsas-own-hardware-backdoors-may-still-be-a-problem-from-hell/. ;
Mutschler, Ann. "The Threat Of Supply Chain Insecurity." *Semiconductor Engineering*, September 7, 2023. https://semiengineering.com/the-threat-of-supply-chain-insecurity/.

[8] Sumathi, G., L. Srivani, D. Thirugnana Murthy, N. Murali, S.A.V. Satya Murty, and T. Jayakumar. "DSDPC: Delay Signatures at Different Process Corners Based Hardware Trojan Detection Technique for FPGAs." In *2015 International Conference on Robotics, Automation, Control and Embedded Systems (RACE)*. IEEE, 2015. http://dx.doi.org/10.1109/race.2015.7097284.

[9] "Eradicate Faults and Backdoors in Information Technology and Facilitate Innovation." Quattro S Initiative, 2019. https://www.itas.kit.edu/downloads/projekt/projekt_webe17_quattros_info.pdf. ;
Goldman, Jeff. "Chip Backdoors: Assessing the Threat." *Semiconductor Engineering*, August 4, 2022. https://semiengineering.com/chip-backdoors-assessing-the-threat/.

[10] Worthman, Ernest. "Back Doors Are Everywhere." *Semiconductor Engineering*, March 3, 2016. https://semiengineering.com/back-doors-everywhere/.

[11] Department for Science, Innovation & Technology. National Semiconductor Strategy (2023). https://www.gov.uk/government/publications/national-semiconductor-strategy/national-semiconductor-strategy. ;
"National Cyber Strategy 2022." HM Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf.

[12] Dong, Chen, Yi Xu, Ximeng Liu, Fan Zhang, Guorong He, and Yuzhong Chen. "Hardware Trojans in Chips: A Survey for Detection and Prevention." *Sensors (Basel, Switzerland)* 20, no. 18 (September 10, 2020): 5165. https://doi.org/10.3390/s20185165.

[13] Infosec. "Hardware Attacks, Backdoors and Electronic Component Qualification." Accessed April 26, 2024. https://www.infosecinstitute.com/resources/hacking/hardware-attacks-backdoors-and-electronic-component-qualification/.

[14] Barta, Brian. "Advice on Improving Detection & Classification of HW Backdoors vs SW Vulnerabilities in the IoT Space," August 3, 2023. https://www.linkedin.com/pulse/advice-improving-detection-classification-hw-backdoors-barta/. ;
Xiao, Forte et al., "Hardware Trojans."

[15] Barta, "Advice on Improving Detection & Classification of HW Backdoors vs SW Vulnerabilities."

[16] Simonite, "NSA's Own Hardware Backdoors May Still Be a 'Problem from Hell.'" ;

Schoen, Seth. "The Government Wants A Backdoor Into Your Online Communications." *Electronic Frontier Foundation*, May 22, 2013. https://www.eff.org/deeplinks/2013/05/caleatwo.

[17] Brumfield, Cynthia. "Remote Bricking of Ukrainian Tractors Raises Agriculture Security Concerns." *CSO Online*, May 26, 2022. https://www.csoonline.com/article/572811/remote-bricking-of-ukrainian-tractors-raises-agriculture-security-concerns.html.

[18] Smith, Ms. "Now You, Too, Can Disable Intel ME 'backdoor' Thanks to the NSA." *CSO Online*, August 29, 2017. https://www.csoonline.com/article/562761/researchers-say-now-you-too-can-disable-intel-me-backdoor-thanks-to-the-nsa.html.

[19] Fylyppov, Olexsandr, and Tim Lister. "Russians Plunder $5M Farm Vehicles from Ukraine – to Find They've Been Remotely Disabled." *CNN*, May 1, 2022. https://edition.cnn.com/2022/05/01/europe/russia-farm-vehicles-ukraine-disabled-melitopol-intl/index.html.

[20] Portnoy, Erica, and Peter Eckersley. "Intel's Management Engine Is a Security Hazard, and Users Need a Way to Disable It." *Electronic Frontier Foundation*, May 8, 2017. https://www.eff.org/deeplinks/2017/05/intels-management-engine-security-hazard-and-users-need-way-disable-it.

[21] Benchoff, Brian. "What You Need To Know About The Intel Management Engine." *Hackaday* (blog), December 11, 2017. https://hackaday.com/2017/12/11/what-you-need-to-know-about-the-intel-management-engine/.

[22] Portnoy and Eckersley, "Intel's Management Engine Is a Security Hazard."

[23] NIST, U.S. Department of Commerce. "National Vulnerability Database." Information Technology Laboratory, August 3, 2023. https://nvd.nist.gov/vuln.

[24] Yang, Kaiyuan, Matthew Hicks, Qing Dong, Todd Austin, and Dennis Sylvester. "A2: Analog Malicious Hardware." In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2016. http://dx.doi.org/10.1109/sp.2016.10.

[25] Infosec. "Hardware Attacks, Backdoors and Electronic Component Qualification."

[26] Goldman, "Chip Backdoors: Assessing the Threat."

[27] Tehranipoor, Mohammad, and Farinaz Koushanfar. "A Survey of Hardware Trojan Taxonomy and Detection." *IEEE Design & Test of Computers* 27, no. 1 (January 2010): 10–25. https://doi.org/10.1109/mdt.2010.7.

[28] Greenberg, Andy. "This 'Demonically Clever' Backdoor Hides In a Tiny Slice of a Computer Chip." *WIRED*, June 1, 2016. https://www.wired.com/2016/06/demonically-clever-backdoor-hides-inside-computer-chip/.

[29] Lofy, Cheri, and Mark Vriesenga. "Demystifying Platform Cyber Resilience," 2019. http://gvsets.ndia-mich.org/documents/VEA/2019/Demystifying_Platform_Cyber_Resilience_Lofy_Vriesenga_20190701a.pdf.

[30] Kulkarni, Ameya, and Chengying Xu. "A Deep Learning Approach in Optical Inspection to Detect Hidden Hardware Trojans and Secure Cybersecurity in Electronics Manufacturing Supply Chains." *Frontiers in Mechanical Engineering* 7 (July 27, 2021). https://doi.org/10.3389/fmech.2021.709924.

[31] Robertson, Jordan, and Michael Riley. "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies." *Bloomberg*, October 4, 2018. https://archive.is/n3Xov.

[32] Altium. "Protect Your PCB Design: How to Avoid Counterfeit Electronic Components," April 11, 2017. https://resources.altium.com/p/how-to-protect-your-pcb-designs-from-counterfeit-electronic-components. ; Kulkarni and Xu, "A Deep Learning Approach in Optical Inspection."

[33] Xiao, K., D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor. "Hardware Trojans." *ACM Transactions on Design Automation of Electronic Systems* 22, no. 1 (May 27, 2016): 1–23. https://doi.org/10.1145/2906147.

[34] Skorobogatov, Sergei, and Christopher Woods. "Breakthrough Silicon Scanning Discovers Backdoor in Military Chip." International Association for Cryptologic Research, 2012. https://www.cl.cam.ac.uk/~sps32/ches2012-backdoor.pdf.

[35] Dong et al., "Hardware Trojans in Chips: A Survey for Detection and Prevention," 5165.

[36] Dong et al., "Hardware Trojans in Chips: A Survey for Detection and Prevention," 5165. ;
Goldman, "Chip Backdoors: Assessing the Threat." ;
"Real-World Impact Measurement of Spectre and Meltdown Patches." Spirent, 2018. https://assets.ctfassets.net/wcxs9ap8i19s/6gHpgAh6Lu6HGVABnSGMq0/ac9ef1a75a177ca300f17efobe41adba/Real-World-Impact-Measurement.pdf. ;
"Meltdown and Spectre." Accessed April 26, 2024. https://meltdownattack.com/.

[37] Tripathy et al, "India's Semiconductor Ecosystem: A SWOT Analysis", Takshashila Discussion SlideDoc 2021-02, August 2021

[38] Kotasthane and Manchi, *When the Chips Are Down*.

[39] Cadence Design Systems. "What Is Electronic Design Automation (EDA)?" Accessed April 26, 2024. https://cadence.com/en_US/home/explore/what-is-electronic-design-automation.html.

[40] Xiao et al., "Hardware Trojans."

[41] Xiao et al., "Hardware Trojans."

[42] King, Samuel T., Joseph Tucek, Anthony Cozzie, Chris Grier, Weihang Jiang, and Yuanyuan Zhou. "Designing and Implementing Malicious Hardware," 2008. https://www.usenix.org/legacy/event/leet08/tech/full_papers/king/king_html/.

[43] Al-Anwar, Amr, Yousra Alkabani, M. Watheq El-Kharashi, and Hassan Bedour. "Hardware Trojan Protection for Third Party IPs." In *2013 Euromicro Conference on Digital System Design*. IEEE, 2013. http://dx.doi.org/10.1109/dsd.2013.133.

[44] Gupta, Mohit. "Using 3rd Party IP in ASIC/SoC Design." *EE Times*, February 25, 2013. https://www.eetimes.com/using-3rd-party-ip-in-asic-soc-design/.

[45] Xiao et al., "Hardware Trojans."

[46] Bhunia, Swarup, Michael S. Hsiao, Mainak Banga, and Seetharam Narasimhan. "Hardware Trojan Attacks: Threat Analysis and Countermeasures." *Proceedings of the IEEE* 102, no. 8 (August 2014): 1229–47. https://doi.org/10.1109/jproc.2014.2334493.

[47] Basu, Kanad, Samah Mohamed Saeed, Christian Pilato, Mohammed Ashraf, Mohammed Thari Nabeel, Krishnendu Chakrabarty, and Ramesh Karri. "CAD-Base: An Attack Vector into the ElectronicsSupply Chain." *ACM Transactions on Design Automation of Electronic Systems* 24, no. 4 (April 18, 2019). https://doi.org/10.1145/3315574.

[48] Barrozo, Jharwin. "What Is a Netlist? Understanding the Basics of Electronic Design Automation." *Flux.Ai* (blog), August 30, 2023. https://www.flux.ai/p/blog/what-is-a-netlist-understanding-the-basics-of-electronic-design-automation.

[49] Xiao et al., "Hardware Trojans."

[50] Basu et al., "CAD-Base: An Attack Vector into the ElectronicsSupply Chain."

[51] Proulx, Alexandre, Jean-Yves Chouinard, Paul Fortier, and Amine Miled. "A Survey on FPGA Cybersecurity Design Strategies." *ACM Transactions on Reconfigurable Technology and Systems* 16, no. 2 (March 11, 2023): 1–33. https://doi.org/10.1145/3561515.

[52] Xiao et al., "Hardware Trojans." ;
Bhunia et al., "Hardware Trojan Attacks"

[53] Basu et al., "CAD-Base: An Attack Vector into the ElectronicsSupply Chain."

[54] Bhunia et al., "Hardware Trojan Attacks"

[55] Cassano, Luca, Mattia Iamundo, Tomas Antonio Lopez, Alessandro Nazzari, and Giorgio Di Natale. "DETON: DEfeating Hardware Trojan Horses in Microprocessors

through Software ObfuscatioN." *Journal of Systems Architecture* 129 (August 2022): 102592. https://doi.org/10.1016/j.sysarc.2022.102592. ;
Dong et al., "Hardware Trojans in Chips: A Survey for Detection and Prevention," 5165. ;
Upadhyay, Akshat. "Role of Semiconductors in India's National Security." *MP-IDSA Occasional Paper No. 61*. Manohar Parrikar Institute for Defence Studies and Analyses, February 2023. https://www.idsa.in/system/files/opaper/Occasional-Paper-61.pdf.

[56] Zantout, Salam R. "Hardware Trojan Detection in FPGA through Side-Channel Power Analysis and Machine Learning ." University of California, Irvine, 2018. ;
Zhou, Boyou, Aydan Aksoylar, Kyle Vigil, Ronen Adato, Jian Tan, Bennett Goldberg, M. Selim Unlu, and Ajay Joshi. "Hardware Trojan Detection Using Backside Optical Imaging." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 40, no. 1 (January 2021): 24–37. https://doi.org/10.1109/tcad.2020.2991680.

[57] Greenberg, "'Demonically Clever' Backdoor Hides In a Tiny Slice of a Computer Chip."

[58] Li, He, Qiang Liu, and Jiliang Zhang. "A Survey of Hardware Trojan Threat and Defense." *Integration* 55 (September 2016): 426–37. https://doi.org/10.1016/j.vlsi.2016.01.004.

[59] Dong et al., "Hardware Trojans in Chips: A Survey for Detection and Prevention," 5165.

[60] Dong et al., "Hardware Trojans in Chips: A Survey for Detection and Prevention," 5165.

[61] Raj, E. Yaswanth , Y. Malathi, Ch SVSS Upendra, and R. Saroja Sneha. "Hardware Trojan Insertion and Detection Using Side Channel Analysis and Implementation of BPUF." ANITS, Visakhapatnam, 2021. https://ece.anits.edu.in/Project%20Reports%202020-21%20NAAC/Sec-A/A-11.pdf.

[62] Bao, Chongxi, Domenic Forte, and Ankur Srivastava. "On Application of One-Class SVM to Reverse Engineering-Based Hardware Trojan Detection." In *Fifteenth International Symposium on Quality Electronic Design*. IEEE, 2014. http://dx.doi.org/10.1109/isqed.2014.6783305.

[63] Dong et al., "Hardware Trojans in Chips: A Survey for Detection and Prevention," 5165.

[64] Wilson, Brent. "What Risks Are Hiding in Your Supply Chain?" *Supply Chain Navigator*, July 25, 2016. https://scnavigator.avnet.com/article/july-2016/what-risks-are-hiding-in-your-supply-chain/.

[65] Dong et al., "Hardware Trojans in Chips: A Survey for Detection and Prevention," 5165.

[66] Kotasthane and Manchi, *When the Chips Are Down.* ;
Pennisi, Salvatore. "The Integrated Circuit Industry at a Crossroads: Threats and Opportunities." *Chips* 1, no. 3 (October 6, 2022): 150–71. https://doi.org/10.3390/chips1030010.

[67] Robertson and Riley, "Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies."

[68] Miller, John F. "Supply Chain Attack Framework and Attack Patterns." Fort Belvoir, VA: Defense Technical Information Center, December 1, 2013. http://dx.doi.org/10.21236/ada610495.

[69] Robertson and Riley, "Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies."

[70] Russ, Samuel H., and Jacob Gatlin. "Three Ways to Hack a Printed Circuit Board." *IEEE Spectrum*, August 21, 2020. https://spectrum.ieee.org/three-ways-to-hack-a-printed-circuit-board.

[71] Zhu, Huifeng, Xiaolong Guo, Yier Jin, and Xuan Zhang. "PCBench: Benchmarking of Board-Level Hardware Attacks and Trojans." In *Proceedings of the 26th Asia and South Pacific Design Automation Conference*. Tokyo, Japan: ACM, 2021. http://dx.doi.org/10.1145/3394885.3431596. ;
Hu et al., "An Overview of Hardware Security and Trust," 1010–38. ;
Piliposyan, Gor. "Investigation into Detection of Hardware Trojans on Printed Circuit Boards." University of Liverpool, 2023. https://livrepository.liverpool.ac.uk/3169204/1/201368983_Mar2023.pdf.

[72] Ghosh, Pallabi, Ulbert J Botero, Fatemeh Ganji, Damon Woodard, Rajat Subhra Chakraborty, and Domenic Forte. "Automated Detection and Localization of Counterfeit Chip Defects by Texture Analysis in Infrared (IR) Domain." In *2020 IEEE Physical Assurance and Inspection of Electronics (PAINE)*. IEEE, 2020. http://dx.doi.org/10.1109/paine49178.2020.9337739.

[73] Sun, Jiming, Marc Jones, Stefan Reinauer, and Vincent Zimmer. 'Introduction'. In *Embedded Firmware Solutions: Development Best Practices for the Internet of Things*,

edited by Jiming Sun, Marc Jones, Stefan Reinauer, and Vincent Zimmer, 1–11. Berkeley, CA: Apress, 2015. https://doi.org/10.1007/978-1-4842-0070-4_1.

[74] Sun et al., 'Introduction', 1–11.

[75] Gough, Corey, Ian Steiner, and Winston Saunders. 'BIOS and Management Firmware'. In *Energy Efficient Servers: Blueprints for Data Center Optimization*, edited by Corey Gough, Ian Steiner, and Winston Saunders, 153–71. Berkeley, CA: Apress, 2015. https://doi.org/10.1007/978-1-4302-6638-9_5.

[76] Greenberg, Andy. 'Millions of PC Motherboards Were Sold With a Firmware Backdoor'. *Wired*. Accessed 26 April 2024. https://www.wired.com/story/gigabyte-motherboard-firmware-backdoor/.

[77] Greenberg, 'Millions of PC Motherboards Were Sold With a Firmware Backdoor'.

[78] Administrador. 'OWASP FSTM, Stage 3: Analyzing Firmware'. Tarlogic Security, 19 September 2022. https://www.tarlogic.com/blog/owasp-fstm-stage-3-analyzing-firmware/.

[79] Bakhshi, Taimur, Bogdan Ghita, and Ievgeniia Kuzminykh. 'A Review of IoT Firmware Vulnerabilities and Auditing Techniques'. *Sensors (Basel, Switzerland)* 24, no. 2 (22 January 2024): 708. https://doi.org/10.3390/s24020708.

[80] Costin, Andrei, Jonas Zaddach, Aurélien Francillon, and Davide Balzarotti. "A Large-Scale Analysis of the Security of Embedded Firmwares." In Proceedings of the 23rd USENIX Conference on Security Symposium, 95–110. Berkeley, CA, USA: USENIX Association, 2014. https://dl.acm.org/doi/10.5555/2671225.2671232.

[81] Dong et al., "Hardware Trojans in Chips: A Survey for Detection and Prevention," 5165.

[82] Goldman, "Chip Backdoors: Assessing the Threat."

[83] Waksman, Adam, and Simha Sethumadhavan. "Silencing Hardware Backdoors." In 2011 IEEE Symposium on Security and Privacy, 49-63. IEEE, 2011. https://www.cs.columbia.edu/~simha/preprint_oakland11.pdf.

[84] Ravi, Sarah. "Strengthening the Global Semiconductor Supply Chain in an Uncertain Era." Semiconductor Industry Association, April 1, 2021. https://www.semiconductors.org/strengthening-the-global-semiconductor-supply-chain-in-an-uncertain-era/.

[85] Kotasthane and Manchi, *When the Chips Are Down*.

[86] Skorobogatov and Woods, 'Breakthrough Silicon Scanning Discovers Backdoor in Military Chip', 23–40.

[87] Robertson and Riley, "Big Hack."

[88] Chadda, Ankur. "Chinese Spies Planted Hardware Backdoors on Servers in Supply Chain Attack." *Decipher*. Accessed April 26, 2024. https://duo.com/decipher/chinese-spies-planted-hardware-backdoors-on-servers-in-supply-chain-attack.

[89] Russ and Gatlin, "Three Ways to Hack a Printed Circuit Board."

[90] Ender, Maik, Pawel Swierczynski, Sebastian Wallat, Matthias Wilhelm, Paul Martin Knopp, and Christof Paar. "Insights into the Mind of a Trojan Designer: The Challenge

to Integrate a Trojan into the Bitstream." In 29th USENIX Security Symposium (USENIX Security 20), 1817–1830. USENIX Association, 2020. https://www.usenix.org/system/files/sec20-ender.pdf.

[91] Goldman, "Chip Backdoors"

[92] University, Carnegie Mellon. "Detecting Trojans in Analog Hardware - Electrical and Computer Engineering - College of Engineering." Carnegie Mellon University. Accessed April 26, 2024. https://www.ece.cmu.edu/news-and-events/story/2023/08/detecting-trojans-in-analog-hardware.html.

[93] Yang, Kaiyuan, Matthew Hicks, Qing Dong, Todd Austin, and Dennis Sylvester. "A2: Analog Malicious Hardware." In 2016 IEEE Symposium on Security and Privacy (SP), 18–37. San Jose, CA: IEEE, 2016.https://web.eecs.umich.edu/~taustin/papers/OAKLAND16-a2attack.pdf.

[94] Becker, Georg T., Francesco Regazzoni, Christof Paar, and Wayne P. Burleson. "Stealthy Dopant-Level Hardware Trojans." In Cryptographic Hardware and Embedded Systems – CHES 2013, edited by Guido Bertoni and Jean-Sébastien Coron, 197–214. Lecture Notes in Computer Science 8086. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. https://www.iacr.org/archive/ches2013/80860203/80860203.pdf.

[95] Ray, Sandip, Yier Jin, Ramesh Karri, Swarup Bhunia, Mark Tehranipoor, and Domenic Forte. "System-on-Chip Platform Security Assurance: Architecture and Validation." Proceedings of the IEEE 106, no. 1 (January 2018): 21–37.https://swarup.ece.ufl.edu/papers/J/J73.pdf.

[96] Goldman, "Chip Backdoors: Assessing the Threat."

The Takshashila Institution is an independent centre for research and education in public policy. It is a non-partisan, non-profit organisation that advocates the values of freedom, openness, tolerance, pluralism, and responsible citizenship. It seeks to transform India through better public policies, bridging the governance gap by developing better public servants, civil society leaders, professionals, and informed citizens.

Takshashila creates change by connecting good people, to good ideas and good networks. It produces independent policy research in a number of areas of governance, it grooms civic leaders through its online education programmes and engages in public discourse through its publications and digital media.