NIST Cybersecurity White Paper
NIST CSWP 46

Analyzing Collusion Threats in the Semiconductor Supply Chain

Sanjay (Jay) Rekhi
Kostas Amberiadis
Computer Security
Information Technology Laboratory

Abir Ahsan Akib
Ankur Srivastava
Electrical and Computer Engineering
University of Maryland, College Park

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.46

June 30, 2025

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

Publication History
Approved by the NIST Editorial Review Board on 2025-01-30

How to Cite this NIST Technical Series Publication:
Rekhi S, Amberiadis K, Akib AA, Srivastava A (2025) Analyzing Collusion Threats in the Semiconductor Supply Chain. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 46. https://doi.org/10.6028/NIST.CSWP.46

Author ORCID iDs
Sanjay (Jay) Rekhi: 0009-0008-8711-4030
Kostas Amberiadis: 0009-0000-7771-5002
Abir Ahsan Akib: 0000-0002-1455-6662
Ankur Srivastava: 0000-0002-5445-904X

Contact Information
hwsec@nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/publications/cswp, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

This work proposes a framework for analyzing threats related to the semiconductor supply chain. The framework introduces a metric that quantifies the severity of different threats subjected to a collusion of adversaries from different stages of the supply chain. Two different case studies are provided to describe the real-life application of the framework. The metrics and analysis aim to guide security efforts and optimize the trade-offs of hardware security and costs.

Keywords

collusion; security metrics; supply chain life cycle; supply chain security.

Table of Contents

List of Figures

1. Introduction

There are numerous security challenges in the semiconductor supply chain. As most chip design companies have become fabless, they rely on offshore foundries for fabrication. This is especially true for the most advanced technology nodes, and the semiconductor supply shock in 2021 has manifested these supply chain security issues. In addition to availability uncertainty, there are many more nuanced security risks in the current semiconductor supply chain, such as IP theft, counterfeiting, Trojan insertion, and reverse engineering.

In order to counteract these security risks, many types of solutions have been proposed, ranging from design to test phases of the supply chain. Numerous government-funded research programs have been established to develop countermeasures, such as the Defense Advanced Research Projects Agency (DARPA) Automated Implementation of Secure Silicon (AISS) program [1], the DARPA Structured Array Hardware for Automatically Realized Applications (SAHARA) program [2], the Naval Surface Warfare Center (NSWC) Crane State-of-the-Art Heterogeneous Integration Prototype (SHIP) program [3], the Air Force Research Laboratory (AFRL) Locked Electronics for Assured Design (LEAD) program [4], and the AFRL Aether Spy program [5], just to name a few, as addressing these security issues is crucial to national security. Dealing with such serious challenges necessitates directing security countermeasure initiatives in stages where the severity of the threat can be best diminished.

Supply chain threat analysis is an essential component of security research. The goals of such analysis are to 1) identify the different threats and related vulnerabilities associated with integrated circuits, 2) analyze how severe the threats become at different stages of the supply chain, and 3) quantify the severity of threats due to collusion among adversaries. The first thing to acknowledge before beginning any such analysis is that, while there are many threats and related vulnerabilities, not all of them can be exploited at every stage in the semiconductor supply chain. Threats vary in severity depending on the stage of supply chain.

For example, the risk of side-channel analysis is more common in chip use scenarios, whereas the risk of a hardware Trojan is more common in the early stages of design and manufacturing, as shown in Fig. 1.

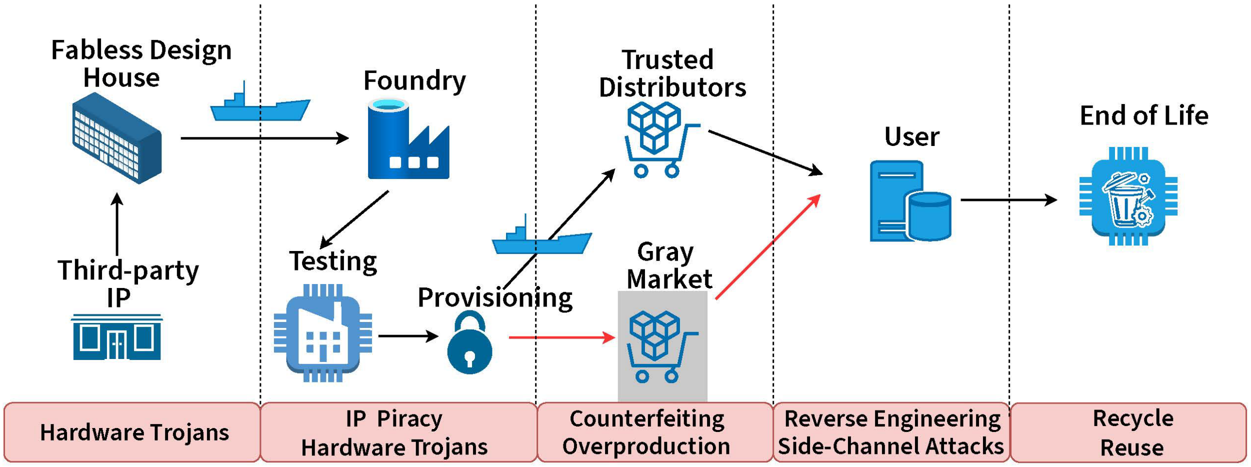

Fig. 1. Security challenges in the semiconductor supply chain

This implies that threat analysis must consider both the type of threat and the various phases of the supply chain in which the threat is most effective. Moreover, one or more adversaries from different stages of supply chain can collaborate to compromise a hardware, which increases the severity of threats. Such insider threats are called collusion threats [6].

This document focuses on potential collusion risks in the hardware supply chain and is organized as follows:

- Section 2 outlines the different phases of a semiconductor supply chain.
- Section 3 describes a framework for analyzing supply chain threats.
- Section 4 presents two real-life examples of hardware security threats to provide a comprehensive explanation of the proposed framework.
- Section 5 concludes the discussion and provides directions for future work.

2. Stages of Semiconductor Supply Chain Stages

The first step in analyzing security concerns in the semiconductor supply chain is to outline the various stages of the supply chain and identify potential threats associated with each. There is no standard set of stages. However, for our analysis we will use seven stages as defined by Areno [7]. The user stage has been merged with the deployment stage since they have similar attack surfaces. An end-of-life stage has also been added to the seven stages originally defined by Areno [7]. A brief explanation of the stages is described below

1. **Concept:** Concept stage is the birthplace of an Integrated Circuit (IC). At this stage, the goals and purpose of an integrated circuit (IC) are formulated, and the scope and target of a hardware component are discussed. Customers, the design, planning, finance teams, and other key stakeholders are involved at this stage.

2. **Design:** Design stage gives a form to the ideas generated in the concept stage. This is the stage where prototypes of the concept are created with the help of different Computer Aided Design (CAD) tools and analysis of whether the goals identified during the concept stage are met. This stage also includes the use of third-party software and hardware prototyping.

3. **Integration:** Integration is the stage where different design components from designers and third parties are integrated together. This phase is crucial since many design elements already have tested solutions, so not everything needs to be created from the ground up. It is more feasible to purchase these solutions from third parties and integrate them into the design.

4. **Manufacturing:** After the IC's design is finished, the manufacturing phase begins. This stage includes several processes, including fabrication and packaging. Due to the high cost of building and maintaining manufacturing facilities, many design houses are fabless and outsource their designs to manufacturers located elsewhere.

5. **Testing:** Testing is the stage at which manufactured Integrated Circuits (ICs) are tested to ensure that they perform properly. Following the completion of fabrication, each IC undergoes testing. An IC's functionalities are tested here to make sure they adhere to design specifications.

6. **Provisioning:** Provisioning is the stage where standard and sensitive data are loaded into the manufactured IC. Standard data are generic and mostly available open source, but the sensitive data are anything whose disclosure would compromise IP or security. For example, keys of crypto modules or logic locking keys are sensitive data.

7. **Deployment and Use:** This stage includes delivering the IC to customers and using the IC. Many hardware vulnerabilities are exploited at this stage.

8. **End of Life:** End-of-life for an IC is the stage where the manufacturer no longer sells or manufactures IC [8]. This is often because of technological advancements when new ICs exhibiting better performance have been launched. When a chip reaches its end-of-life, the deployed chips are gradually replaced and discarded. These discarded chips are

often reused or recycled into new hardware compromising their quality and performance.

3. Framework for Supply Chain Threat Analysis

This work proposes a framework for analyzing different threats and how collusion among adversaries can affect the severity of threats. This analysis is divided into five distinct stages that discuss adversaries' intent, access, and resources, and how their collusion affects the severity of different threats. The framework is shown in Fig. 2. The framework incorporates threats across all stages of supply chain including insider threats.

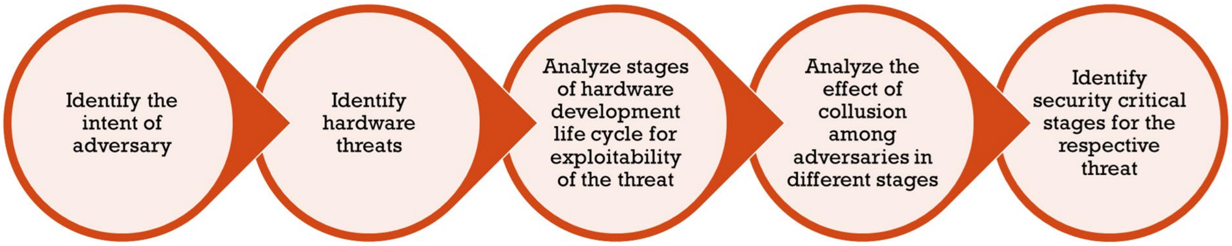
Identify the intent of adversary
Identify hardware threats
Analyze stages of hardware development life cycle for exploitability of the threat
Analyze the effect of collusion among adversaries in different stages
Identify security critical stages for the respective threat

Fig. 2. Methodology for supply chain threat analysis

3.1. Identify the Intent of the Adversary

Supply chain security analysis begins with identifying the adversary's objectives. For example, an adversary may wish to disrupt a hardware's functionality or steal a designer's intellectual property (IP). This analysis describes the potential attacker, the resources that must be protected, and the semiconductor supply chain stage at which mitigation is best applied.

3.2. Identify Hardware Threats

The second step is identifying the threats associated with the adversary's intent. For example, if the intent is IP theft, then the IP to be protected must be identified. In this context, an attack on logic obfuscation can be characterized as a threat. Similarly, if the adversary intends to infiltrate hardware, then hardware Trojan insertion may need to be examined.

3.3. Analyze Stages of Hardware Development Life Cycle for Exploitability of the Threat

At this point, one or more significant hardware threats have been identified. The following stage involves determining which stage of the semiconductor supply chain the threat can be exploited. Questions such as how much threat an adversary in the manufacturing stage poses to logic obfuscation, or whether an adversary in the provisioning stage offers threats to hardware Trojan insertion, are raised. In light of a threat, this step determines the semiconductor supply chain's security-critical phases. In addition, this step determines if a threat is unexploitable at a specific point in the supply chain.

3.4. Analyze the Effect of Collusion Among Adversaries in Different Stages

Since every stage of the semiconductor supply chain is distinct, adversaries have varying degrees of access to and knowledge of the system at different stages of the semiconductor supply chain. The effectiveness of an attack depends largely on the adversary's knowledge of the system and their level of access. Different adversaries possess varying degrees of both. For example, a manufacturer may have detailed design knowledge, while an end user typically has limited access and little insight into a system's internal functions. As a result, their capabilities differ significantly.

Thus, collusion between adversaries from different stages of the life cycle can make threats considerably more severe, which is why this stage is crucial in the context of security analysis.

At this point in the analysis, we apply a linear scale to determine the severity of threats when adversaries from different stages of the supply chain collude. This scale ranges from 0 to 10 and represents the relative threat level of a group of colluding adversaries. Fig. 3 is an example of the scale developed in the context of the threat of hardware trojan insertion. The scale begins at 10, representing the highest threat severity level. This scenario assumes that all relevant adversaries are collaborating. From this point, we progressively remove one adversary at a time from the collusion and assess the resulting threat severity for each possible combination of remaining adversaries. As adversaries are removed, the threat severity decreases, depending on the number of adversaries and their specific roles. For instance, as shown in Fig. 3, if the manufacturer is removed from the collusion, the threat severity level drops to 8. However, if the designer is removed, the threat severity level decreases to 6. This suggests that a malicious designer poses a higher risk of hardware Trojan insertion compared to a malicious manufacturer.

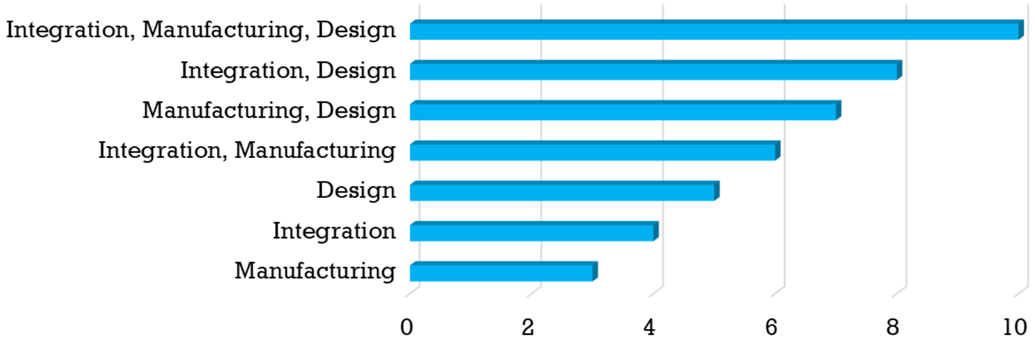

Fig. 3. Threat severity levels for colluding adversaries in the context of hardware Trojan insertion

This scale is relative, meaning it provides a context on the severity of the threat posed by different adversaries in a collusion but does not quantify the exact difference in severity. For example, Fig. 3 illustrates that a collusion between an integrator and a designer presents a more severe threat than one involving a manufacturer and a designer, but the scale does not specify how much more severe the threat is. This relative approach is intentional, as different stakeholders may prioritize different metrics for evaluating threat severity. One analyst might prioritize attack completion time, while another may focus on the likelihood of attack success. This flexibility allows analysts to develop their own customized, non-linear scales based on the metrics they deem most important. These scales can provide a more detailed understanding, such as quantitatively comparing the severity of a designer's threat versus that of a manufacturer.

3.5. Identify Security-Critical Stages for the Respective Threat

The final step involves determining the type and severity of each threat in relation to where it is located on the semiconductor supply chain. The choice of which stage in the semiconductor supply chain may and should be secured must be made at this step, taking into account all threat matrices. This inevitably comes down to weighing the cost-security trade-off.

4. Case Study

This framework for supply chain threat analysis is meant to adapt to different threat types. The following example scenarios consider IP theft and hardware infiltration.

4.1. Hardware Infiltration

- Step 1: A security analysis identifies an adversary's intent to infiltrate a chip. To that end, the adversary might take steps that make the hardware unusable, transmit sensitive information from the chip [9], or receive signals that can make the chip operate abnormally.
- Step 2: One method of infiltrating hardware is through the insertion of hardware Trojans. Hardware Trojans might be inserted in silicon inside the chip, in printed circuit boards, in firmware, etc. For this example, the threat considered is hardware Trojan circuits being inserted into the chip.
- Step 3: The only places in the IC life cycle where Trojans can be inserted are the pre-packaging stages, and, thus, design, integration, and manufacturing become the stages of interest. Hardware Trojans have been inserted in the netlist during the design and integration stages by Yu et al, and Cruz et al. [10], [11]. Hardware Trojans have also been inserted in the finalized layout by Perez et al., which can be implemented by an adversary in manufacturing [12]. Hardware Trojans cannot be inserted during provisioning, deployment, or end-of-life, and, thus, they can be left out of analysis. A critical stage in this context is testing. This is the stage where chips are tested for functionality and Trojans. If this stage is compromised, untested IC will be circulated in the market with increased risk of non-conformity to functionality and standards, and Trojan infestation. Thus, testing is a security-critical stage and must be secured.
- Step 4: A key to inserting Trojan in hardware is to make it difficult to detect. With that intent, adversaries design Trojans which get activated only with very rare input combinations and with minimal changes made to the hardware. This makes designers the strongest adversaries as their knowledge about the internals of the design enable them to choose a rare input vector for Trojan activation. On the other hand, manufacturers have to insert extra hardware in the layout which makes the Trojans more easily detectable. The threat with integrator is between these two adversaries. Fig. 3 shows the severity level of Trojan insertion for colluding adversaries. In this case, increasing collusion among adversaries leads to increase in the number of inserted Trojans. This increases the possibility of one or more Trojans to remain undetected.
- Step 5: At this step, there is an option of securing one or more of the three stages (integration, manufacturing, or design). Since securing supply chain stages have costs associated with it, cost vs. security analysis needs to be performed to select the stages that should be secured.

4.2. IP Theft

- Step 1: For this example, we assume the intent of the adversary is IP theft. IP can be of different forms, like designs or programs running inside the IC, etc. IP theft has serious financial implications, e.g., sometimes rival companies might get their hands on the IP and gain an unfair edge [13]. Again, counterfeit ICs can be produced, which might have inferior quality and cause immeasurable damage to business, life, and property [14]. In this case, we assume that the IP worth protecting is the design secrets.

- Step 2: One method of protecting design secrets is logic obfuscation, which enhances combinational logic cones and/or finite-state machines in the design by introducing key inputs and key gates [15]. Such techniques are powerful countermeasures against attacks by untrusted manufacturers. In order to evaluate the security of locking mechanisms, researchers have proposed numerous deobfuscation methods to emulate an adversary who attempts to unlock the design. Thus, the threat associated with the intent is the threat of logic obfuscation.

- Step 3: Once the threat is identified, we analyze the stages of the supply chain to identify where the threat exists. Each deobfuscation method requires a specific threat model (i.e., the level of access to and knowledge of the locked design). Most deobfuscation methods assume access to a working chip at some level, including Input/Output (I/O) access, scan chain access, or access to side-channel measurements. Shamsi et al. and Massad, et al. have explored deobfuscation techniques when only inputs and outputs are accessible by the adversary [16][17]. If internal register values can also be accessed through the scan chain, a Boolean satisfiability (SAT) attack and its derivatives can be employed to deobfuscate the locked design [18]. These types of access are available after the provisioning stage is completed. Thus, these techniques can be used to deobfuscate the design during the deployment and use stage and the end-of-life stage. In the real world, adversaries are likely experienced engineers and/or institutions who not only have tools and resources needed to extract secrets from a chip but also have years of experience dealing with different designs. These adversaries exist in the early stages of the life cycle in the form of integrator, manufacturer, and tester, where there is no working system, but there exists a lot of experience and knowledge about the design. Deobfuscation techniques under this scenario focus on mapping the locked netlist with designs which have been previously encountered by the adversary. One approach in this direction is finding the structural similarity among the locked netlist and previously encountered netlist [19]. Another way of exploiting the structural similarities is using graph similarity algorithm presented by Fyrbiak et al. [20]. Such techniques can be employed by adversaries in the integration, manufacturing, and testing stages to extract design secrets.

  The design stage contains unobfuscated design, and the provisioning stage contains the keys needed to deobfuscate the design. These two stages do not need to launch any attack to extract design secrets. Thus, in the context of logic locking, threats exist in every stage of the supply chain from design to end-of-life. The IP in this context belongs to the designer, and there is no security if the designer is compromised. Again, provisioning is the stage where keys of logic locking gets uploaded in the IC. Once the keys are known, the entire design secret is revealed, and, thus, provisioning stage is also very security critical.

- Step 4: From the analysis so far, the stages with limited information about design secrets are integration, manufacturing, testing, deployment and use, and end-of-life. To analyze the threat associated with their collusion, an analysis of what information or knowledge an adversary of each stage can bring to the threat needs to be made. The integrator might have a hierarchical view of the obfuscated design. On the other hand, a manufacturer has experience of working with a wide range of different types of designs. For example, an offshore foundry has access to designs from different fab-less design houses all around the world. Testers have some input-output vectors, and the user has a working system. Thus, adversary in each stage has their own set of knowledge and access. This indicates that as more adversaries collude, more information is available, and, thus, the threat gets more severe. Fig. 4 shows the threat levels for different combination of colluding adversaries. Here, the manufacturer has a high level of knowledge, and thus, they alone can make a strong adversary. However, access to working system increases the likelihood of IP theft. This makes adversaries at end-of-life stage and the chip-user stage stronger. In this context, adversaries at end-of-life and deployment and use stages have similar levels of access to a working system and a similar amount of information available to them. End-of-life stage is thus grouped with the deployment stage in Fig. 4.

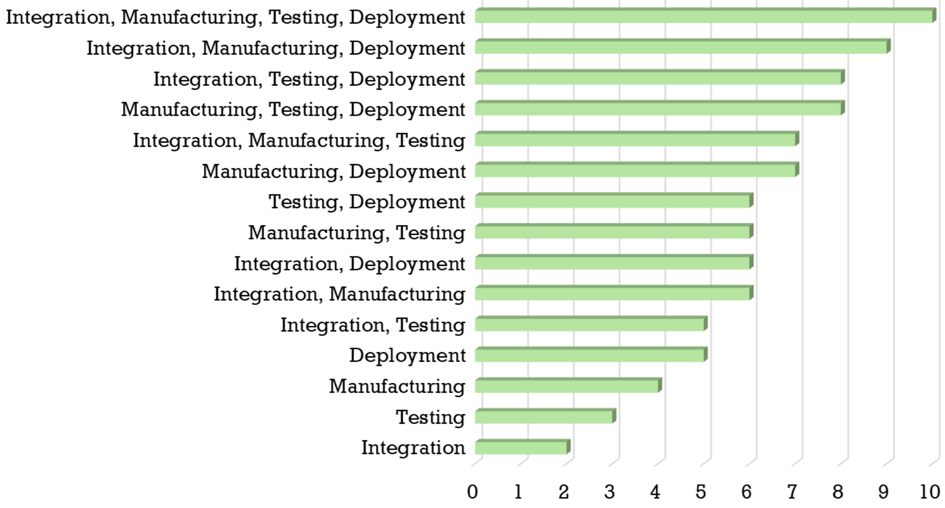

Fig. 4. Threat severity levels for colluding adversaries in context of logic obfuscation

If these adversaries collude with the manufacturer, the access to working system gets combined with the wealth of knowledge making the threat more severe. If the integrator colludes with them, the attack surface can easily be divided into smaller parts, and, thus, attacks can converge quicker which increases the severity of threat on logic obfuscation. The scenario where integration, manufacturing, testing, and deployment stages collaborate represents the highest severity level of threat. At this point in the supply chain, the collusion results in a convergence of extensive system knowledge and broad access, leading to what we classify as a severity level of 10. By systematically removing adversaries from this collusion scenario, we can observe how the levels of knowledge and access change, and consequently, how the threat severity is affected.

- Step 5: A cost versus security analysis is performed to prioritize the stages to be secured (i.e., integration, manufacturing, testing, deployment and use, or end-of-life).

5. Conclusions and Future Work

The investigation of semiconductor supply chain security reveals a complex interplay of weaknesses and opportunities that must be addressed in order to provide a resilient and secure infrastructure. The consequences of supply chain interruptions are becoming more serious as the demand for semiconductors continues to rise globally. In this paper, we analyze security concerns and effects of collusion across the semiconductor life cycle, and the motivation for the attacks. Other motivations can be analyzed through this methodology as well. The methodology provides a relative risk-based score to help plan mitigation. In the future, NIST plans to extend this work to analyze the supply chain threats related to 3D heterogeneous integration and integrate different hardware vulnerabilities into the framework, which will help the stakeholders to improve their threat mitigation techniques and implement more secure and robust designs. Addressing these hardware and supply chain security issues is essential to safeguard national interests and promote economic stability.

References

[1] DARPA (2020) DARPA Selects Teams to Increase Security of Semiconductor Supply Chain. Available at https://www.darpa.mil/news/2020/semiconductor-supply-chain-security

[2] DARPA (2021) Expanding Domestic Manufacturing of Secure, Custom Chips for Defense Needs. Available at https://www.darpa.mil/news-events/2021-03-18

[3] NSWC Crane Corporate Communications (2019) NSWC Crane leverages OTA to ensure that the U.S. Government has access to secure state-of-the-art design, assembly, packaging and test for state-of-the-art microelectronics. Available at https://www.navsea.navy.mil/Media/News/Article/2005099/nswc-crane-leverages-ota-to-ensure-that-the-us-government-has-access-to-secure/

[4] Institute for Systems Research (2020) AFRL-Northrop Grumman: Locked Electronics for Assured Design (LEAD): Delay Locking ASIC IP Blocks to Protect Functionality. Available at https://isr.umd.edu/research-funding/afrl-northrop-grumman-locked-electronics-assured-design-lead-delay-locking-asic-ip

[5] Wolfe F (2020) Aether Spy Next-Generation Multi-Function Radar to Advance, Northrop Grumman Says. *Defense Daily*. Available at https://www.defensedaily.com/aether-spy-next-generation-multi-function-radar-advance-northrop-grumman-says/air-force/

[6] CISA (2020) Defining Insider Threats. Available at https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

[7] Areno M (2020) Supply chain threats against integrated circuits. *Intel Whitepaper*. Available at https://www.intel.com/content/dam/www/central-libraries/us/en/documents/2022-08/supply-chain-threats-against-integrated-circuits-whitepaper-july2020.pdf

[8] Evernex (2024) EOL Meaning: What Does End of Life Mean for Your Hardware? Available at https://evernex.com/industry-guide/eol-meaning/

[9] Vincent J (2018) Chinese spies reportedly inserted microchips into servers used by Apple, Amazon, and others. Available at https://www.theverge.com/2018/10/4/17935868/-chinese-spies-microchip-hack-servers-apple-amazon-supermicro

[10] Yu S, Liu W, O'Neill M (2019) An improved automatic hardware Trojan generation platform. *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)* (IEEE, Miami, Florida), pp 302–307. https://doi.org/10.1109/ISVLSI.2019.00062

[11] Cruz J, Huang Y, Mishra P, Bhunia S (2018) An automated configurable Trojan insertion framework for dynamic trust benchmarks. *Design, Automation & Test in Europe Conference & Exhibition* (IEEE, Dresden, Germany) pp 1598–1603. https://doi.org/10.23919/DATE.2018.8342270

[12] Perez TD, Pagliarini S (2023) Hardware Trojan insertion in finalized layouts: From methodology to a silicon demonstration. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (IEEE) 42(7): 2094–2107. https://doi.org/10.1109/TCAD.2022.3223846

[13] Astute Electronics (2024) SK Hynix Engineer Jailed for Semiconductor IP Theft Amidst Global Tech Rivalry. Available at https://www.astutegroup.com/news/general/sk-hynix-engineer-jailed-for-semiconductor-ip-theft-amidst-global-tech-rivalry/

[14] Takahashi D (2011) Feds close huge chip counterfeiting case (exclusive). Available at https://venturebeat.com/business/feds-close-the-books-on-a-huge-chip-counterfeiting-scheme/

[15] Chakraborty A, Jayasankaran N G, Liu Y, Rajendran J, Sinanoglu O, Srivastava A, Xie Y, Yasin M, Zuzak M (2019) Keynote: A disquisition on logic locking. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (IEEE) 39(10):1952–1972. https://doi.org/10.1109/TCAD.2019.2944586

[16] Shamsi K, Li M, Pan D Z, Jin Y (2019) KC2: Key-Condition Crunching for Fast Sequential Circuit Deobfuscation. *Design, Automation & Test in Europe Conference & Exhibition* (IEEE, Florence, Italy) pp 534–539. https://doi.org/10.23919/DATE.2019.8715053

[17] Massad M E, Garg S, Tripunitara M (2017) Reverse engineering camouflaged sequential circuits without scan access. *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)* (IEEE, Irvine, CA) pp 33–40. https://doi.org/10.1109/ICCAD.2017.8203757

[18] Subramanyan P, Ray S, Malik S (2015) Evaluating the security of logic encryption algorithms. *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)* (IEEE, Washington, DC) pp 137–143. https://doi.org/10.1109/HST.2015.7140252

[19] Cheng Y, Wang Y, Li H, Li X (2015) A similarity-based circuit partitioning and trimming method to defend against hardware trojans. *IEEE Computer Society Annual Symposium on VLSI* (IEEE, Montpellier, France) pp 368–373. https://doi.org/10.1109/ISVLSI.2015.93

[20] Fyrbiak M, Wallat S, Reinhard S, Bissantz N, Paar C (2020) Graph similarity and its applications to hardware security. *IEEE Transactions on Computers* (IEEE) 69(4):505–519. https://doi.org/10.1109/TC.2019.2953752