Basel Halak *Editor*

Hardware Supply Chain Security

Threat Modelling, Emerging Attacks and Countermeasures

Springer

Hardware Supply Chain Security

Basel Halak
Editor

Hardware Supply Chain Security

Threat Modelling, Emerging Attacks and Countermeasures

Springer

Editor
Basel Halak
Electronics and Computer Science School
University of Southampton
Southampton, UK

ISBN 978-3-030-62706-5 ISBN 978-3-030-62707-2 (eBook)
https://doi.org/10.1007/978-3-030-62707-2

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To
Suzanne, Hanin and Sophia
with Love

Preface

The trend towards globalisation and the need to cut costs to gain competitive advantages have resulted in a remarkable growth of outsourcing levels; this is particularly true for the hardware supply chain. The latter has become a multinational distributed business. This evolution of the supply chain structure has brought about a number of serious challenges, including a rising level of IP piracy, counterfeiting and the emergence of new forms of attacks such as Hardware Trojans. Such attacks can lead severe consequences. Financially, counterfeiting is costing the global economy billions of US dollars every year. Furthermore, compromised hardware products pose a serious security threat if used in critical infrastructure and military applications. The threat on the security of hardware devices is exasperated by the proliferation of the internet of things (IoT) technology, wherein the majority of devices have limited computation and memory resources, making it harder to implement typical security defence mechanisms. In fact, in 2019, a staggering 2.9 billion cyberattacks on internet of things devices have been recorded. What is more, a significant portion of such embedded systems are deployed in unprotected and physically accessible locations, therefore they can be vulnerable to both invasive and side channel attacks, allowing attackers to extract sensitive data that might be stored on IoT nodes, such as encryption keys, digital identifiers and recorded measurements. To mitigate against such risks, engineers need to treat security as an integral part of the design process, not as an after-thought.

Overlooking security in the electronic products development will put a great many systems at risk, leading, in many cases, to financial losses, damage of reputation and in extreme cases to physical harm.

Building effective defence mechanisms requires a comprehensive understanding of the attack classes, goals of the adversary and their capabilities. However, what makes devising appropriate countermeasures particularly challenging is that fact that an electronic system does not always recognise it is under attack, so it may fail to activate its defences at the right time. This is because, in many cases, the attack is new, so its symptoms are unknown or the system attributes the attack to a reliability problem. Therefore, the detection of anomalous behaviours in electronic systems is an important defence technique.

The prime objective of this book is to provide a timely and a comprehensive account of emerging security attacks on the hardware supply chain, which covers all stages of an electronic system's life cycle, from initial design specifications, through its operation in the field, until it is discarded in an IC recycling centre.

To facilitate the understanding of the material, each chapter includes background information explaining related terminologies and principles, in addition to a comprehensive list of relevant references. The book is divided into three parts to enhance its readability, namely threat modelling of Hardware supply chain, Emerging attacks and countermeasures and anomaly detection in embedded systems.

The Contents at Glance

This book presents a new threat modelling approach that specifically targets hardware supply chain, covering security risks throughout the lifecycle of an electronic system. Afterword's the book presents a case study on a new security attack, which combines two forms of attack's mechanisms, from two different stages of the IC supply chain, more specifically the attack targets the newly developed light cypher (Ascon) and demonstrates how it can be broken easily, when its implementation is compromised with a hardware Trojan.

The book also discusses emerging countermeasures, including anti-counterfeit design techniques for resources-constrained devices and anomaly detection methods for embedded systems. More details on each chapter are provided below.

Part I: Threat Modelling of Hardware Supply Chain

Chapter 1 systemises the current knowledge on hardware security including emerging attacks and state-of-the-art defences, and presents a number of case study to demonstrate how to perform security validation of countermeasures in the context of specific application scenario, which allows balancing security requirements of a particular product with the cost associated with implementing defence mechanisms.

Part II: Emerging Hardware-Based Security Attacks and Countermeasures

Chapter 2 provides a case study on an emerging security threat that combines multiple attack's vectors. It demonstrates the feasibility of using hardware Trojan to undermine the resilience of Ascon cyphers to the cube attacks. The combined attack was successfully waged on a FPGA implementation of the Ascon cypher.

Chapter 3 focuses on the security of resources-constrained systems, in particular RFID. It presents a new defence mechanism to mitigate against counterfeiting attacks, such as tag cloning. This chapter proposes a new security mechanism, which consists of a lightweight three-flight mutual authentication protocol and an anti-counterfeit tag design. The solution is based on combining the Rabin public key encryption scheme with physically unclonable functions (PUF) technology.

Part III: Anomaly Detection in Embedded Systems

Chapter 4 outlines the underlying causes of anomalous behaviours in embedded systems, distinguishing between those caused by reliability problems and others resulting from security attacks.

Chapter 5 provides an overview of hardware performance counters, an important tool used for anomaly detection in electronic systems.

Chapter 6 provides a comprehensive summary of anomaly detection techniques and presents a detailed case study on the use of machine learning algorithms in this context.

Book Audience

The book is intended to provide a comprehensive coverage of the latest research advances in the key research areas of hardware supply chain security; this makes it a valuable resource for graduate student researchers and engineers working in these areas. I hope this book will complement ongoing research and teaching activities in this field.

Southampton, UK
September 2020

Basel Halak

Acknowledgments

I would like to thank all of those who contributed to the emergence, creation and correction of this book. Firstly, I gratefully acknowledge the valuable contributions from my students at the University of Southampton, for the many hours they have spent working in their labs to generate the experimental results. Of course, the book would not be successful without the contributions of many researchers and experts in the field of security and embedded systems.

Finally, I would like to thank the great team at Springer for their help and support throughout the publication process.

Contents

About the Editor

Basel Halak is the director of the embedded systems and IoT programme at the University of Southampton, a visiting scholar at the Technical University of Kaiserslautern, a visiting professor at the Kazakh-British Technical University, an industrial fellow of the royal academy of engineering and a senior fellow of the higher education academy. He has written over 70-refereed conference and journal papers, and authored four books, including the first textbook on Physically Unclonable Functions. His research expertise includes evaluation of security of hardware devices, development of appropriate countermeasures, the development of mathematical formalisms of reliability issues in CMOS circuits (e.g. crosstalk, radiation, ageing), and the use of fault tolerance techniques to improve the robustness of electronics systems against such issues. Dr. Halak lectures on digital design, Secure Hardware and Cryptography, supervises a number of MSc and PhD students, and is the ECS Exchange Coordinators. He is also leading the European Masters in Embedded Computing Systems (EMECS), a 2-year course run in collaboration with Kaiserslautern University in Germany and the Norwegian University of Science and Technology in Trondheim (electronics and communication). Dr. Halak serves on several technical programme committees such as HOST, IEEE DATE, IVSW, ICCCA, ICCCS, MTV and EWME. He is an associate editor of IEEE access and an editor of the IET circuit devices and system journal. He is also a member of the hardware security-working group of the World Wide Web Consortium (W3C).

Part I
Threat Modelling of Hardware Supply Chain

Chapter 1
CIST: A Threat Modelling Approach for Hardware Supply Chain Security

Basel Halak

1.1 Introduction

1.1.1 Motivation

The remarkable growth of outsourcing in the hardware supply chain has brought about serious challenges in the form of new security attacks, particularly IC counterfeit and Hardware Trojan insertion. Such attacks can have severe consequences. Financially, counterfeiting is costing the UK economy around £30 billion and is putting 14,800 jobs at risk [1]. The consequences of an insecure IC supply chain are not only limited to major financial losses, but they also pose a national security threat. A recent report by Bloomberg alleged that Chinese spies reached almost 30 US companies, including Amazon and Apple, by compromising America's technology supply chain by inserting a hardware Trojan.[1] Although the above-mentioned companies have denied these claims, an analysis by a prominent hardware security expert indicated the above attack was entirely feasible.[2] Another study has indicated that counterfeit ICs can cause the malfunctioning of military weapons and vehicles [2]. Another trend that has further increased the hardware attack surface is the proliferation of the internet of things (IoT) technology. The

[1] https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

[2] https://www.google.co.uk/amp/s/gigazine.net/amp/en/20181010-supermicro-motherboard-attack.

B. Halak (✉)
Electronics and Computer Science School, University of Southampton, Southampton, UK
e-mail: basel.halak@soton.ac.uk

B. Halak (ed.), *Hardware Supply Chain Security*,
https://doi.org/10.1007/978-3-030-62707-2_1

latter has led to a rapid increase in computing devices (around 50 billion in 2025). In fact, in 2019, a staggering 2.9 billion cyberattacks on IoT devices have been recorded [3].

This steady drumbeat of news stories on successful security attacks makes it abundantly clear that current defence mechanisms are insufficient to protect from the developing risks of cyber and physical attacks. One reason behind the failure of current practices is that the threat models on which the security of systems rely fail to account for the big picture [4].

Threat modelling is a process by which potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified, enumerated and mitigations can be prioritized. Such a process makes it feasible to perform systematic analysis of the probable attacker's profile; the most likely attack vectors, the assets most desired by an attacker, and more importantly the most effective defence mechanisms.

Although, there are plenty of work in the literature on the different types of attacks on hardware supply chain and computing devices, there are very few attempts to develop a comprehensive threat modelling approach that considers the life cycle of hardware systems from the initial design specifications to the recycling phase of discarded ICs.

One of the earliest work in this area is [5], in which the need for systematic approach to analysing the security threat of the IC supply chain is highlighted. A more comprehensive security analysis appeared few years later in [6], in which the authors provided a summary of exiting attacks and possible countermeasures. Both of these papers indicated that existing threat modelling approach such as those based on the Microsoft's STRIDE model [7, 8] is not suitable for analysing the security of IC supply chain; this is because the type of threats in the latter case is of an inherently different nature compared to those included in the STRIDE model. To the best of our knowledge, there is currently no comprehensive threat modelling approach that is tailored to the needs of IC supply chain. Furthermore, new IC fabrication techniques are continuously being developed to keep pace with Moore's law [9]; these new approaches may have fundamentally different security assumptions, which need to be systematically evaluated and analysed in order to understand whether or not these new models carry any unforeseen security risks. Having a clear understanding of the types of threats of future IC supply chain will allow for defence mechanisms to be put in place at an early stage of the development process, i.e. building a secure-by-design IC supply chain.

The contributions of this work are as follows:

1. It systematizes the current knowledge on security attacks on hardware supply chain, providing a comprehensive review of security attacks and the state-of-the-art countermeasures.
2. It presents a new threat modelling approach specifically developed for hardware supply chain, which takes into consideration the nature of the system, the most probable attacker's profile and the root of vulnerability. This allows the development of appropriate countermeasures that balances security needs with available resources and other operation requirements.

3. It presents a number of exemplar case studies that demonstrate how the proposed threat modelling approach can be used to evaluate the appropriateness and the level of protection provided existing defence mechanisms in the context of a specific application.

1.1.2 Chapter Summary

The remainder of this paper is organized as follows. Section 1.2 reviews related work and preliminary background. Sections 1.3 and 1.4 present a summary of the proposed threat modelling approach called *CIST*. Section 1.5 explains the (PROV-N) technique adopted in this work for modelling the IC supply chain security. Sections 1.6 and 1.7 provide a comprehensive review of the attacks on the hardware supply chain and corresponding countermeasures, respectively. Section 1.7 demonstrates using a number of case studies how the CIST approach can be used for security validation of existing countermeasures. Conclusions are drawn in Sect. 1.9.

1.2 Background

1.2.1 Related work

Modelling of security threats and attacks has been extensively studied in the literature. Attack trees proposed in [10] provide a systematic way of describing the security of a system, each tree consists of one root, leaves and children. The root is the ultimate goal of the attack (e.g. insert a Trojan). The child nodes are conditions that must be satisfied to make the direct parent node true. In other words, the attack described in the root may require one or more of many attacks described in child nodes to be satisfied. Attack pattern [10] is a similar approach that relies on the use of AND/OR composition of operations (Pattern) that may generate an attack. Both methods are originally developed to analyse software and networking system security, therefore, their use to model hardware security threat has not been investigated.

The work in [11] proposed a unified conceptual framework for security auditing from a risk management perspective through the generation of threat models. This approach, called "Trike", relies on a "requirements model." The latter is used to ensure the level of risk assigned to each asset is appropriate to relevant stakeholders. This can be challenging to implement in large complex application scenarios, as it needs the designer to have an overview of the entire system to be able to conduct the attack surface analysis. Another widely used approach is STRIDE [7], which is used to categorize the identified threats into six categories *Spoofing, Tampering, Repudiation, Information disclosure, Denial of service* and *Elevation*

of privilege. The goal of this approach is to ensure that applications meet the security properties of *Confidentiality, Integrity and Availability (CIA), along with Authorization, Authentication and Non-Repudiation*. All of the above methods are very useful in performing threat and risk analysis. However, these have not been specifically developed for Hardware attacks. Some categories are not applicable to hardware threats, e.g. Spoofing, Repudiation and Elevation of privilege; some can be applied but may have different meanings, e.g. confidentiality and tampering, while some hardware-related risks are not even covered such as IC counterfeit and supply chain sabotage, hence the need for a more tailored threat modelling approach that consider all hardware-related attacks throughout the cycle of the IC.

1.2.2 Description of IC Production Process

Semiconductor technologies have infiltrated all areas of modern life driven by a multitude of emerging applications. The unprecedented demand for cheaper and more complex silicon chip has led to a rise in the outsourcing level in IC production process. The latter has become a multinational distributed business that involves hundreds of suppliers and complex logistics. Figure 1.1 provides a summary of the IC production chain. The first stage consists of sourcing (IP) designs from third party providers. The second stage is the system-on-chip (SoC) integration, which takes place at the design house and produces the layout files. The latter are sent for fabrication and testing. The next stage is packaging and integration into the final product. The latter will be in use for a period of time, depending on its nature (e.g. mobile phone are used for 2–3 years, TV are used for 5–10 years . . .). Once the product is discarded, some silicon chips are illegally recycled to be used in other products.

1.2.3 Preliminaries

1.2.3.1 How to Develop a Secure System in a Nutshell

The notion of "security" is relative. If an adversary has unlimited amount of time and resources, they can break any system. "Secure" simply means that the amount of efforts and costs for breaking a system exceeds potential benefits.

Fig. 1.1 A simplified illustration of the IC production chain

Therefore, establishing whether or not a product is secure requires understanding the underlying motivation of the most likely adversary. For example, if an attacker was seeking an economic gain, then an effective countermeasure should make breaking the system more expensive than any potential financial benefits. On the other hand, if the adversary's goal were to use the attack as weapon to undermine enemies' capabilities and infrastructure, then they would likely have access to a great deal of recourses, which makes implementing a countermeasure much more difficult, and in some cases futile. The best approach in this case is to prevent the attack by isolating and physically protecting the system or ideally by removing the root of vulnerability that made the attack technically feasible.

The notion of security is "temporary". In other words, the attack surface is constantly changing with new attacks emerging every day. Therefore, a product that was deemed secure at the design time can still be compromised if new attacks mechanisms are developed. Therefore, security defence mechanisms should be continually reviewed and updated if necessarily. However, enhancing defence measures to protect against a newly discovered hardware vulnerability may not be feasible unless this can be done at the software level.

1.2.3.2 Attack Difficulty

Attack difficulty refers to the amount of resources and the level of expertise required to carry an attack successfully. This metric can be particularly useful when assessing the level of protection afforded by various security defence mechanisms (i.e. how much more difficult the attack has become after implementing the countermeasure).

The attack difficulty in this work will be based on the classification proposed in [12] as shown in Table 1.1.

1.2.3.3 Adversary Classification

Adversary can be classified according to their knowledge, resources and motivation into four categories based on [13] as shown in Table 1.2. Knowing the class of the most likely adversary is vital for developing effective countermeasures.

1.3 CIST: A Hardware-Specific Threat Modelling Approach

The proposed approach covers hardware-related risks throughout the life cycle of the IC from design to recycle.

The proposed modelling process is comprised of five high-level steps similar to that in as shown in Fig. 1.2.

The aim of the first step is to define the desired hardware security properties, which can be summarized as *authenticity, confidentiality, integrity* and *availability*.

Table 1.1 Classification of attack difficulty

Level	Name	Description
1	Common tools	Commonly available tools and skills may be used (e.g. those tools available from retail department or computer stores, such as a soldering iron or security driver bit set).
2	Unusual tools	Uncommon tools and skills may be used, but they must be available to a substantial population (e.g. multi-meter, oscilloscope, logic analyser, hardware debugging skills, electronic design and construction skills). Typical engineers will have access to these tools and skills.
3	Special tools	Highly specialized tools and expertise may be used, as might be found in the Laboratories of universities, private companies or governmental facilities. The attack requires a significant expenditure of time and effort.
4	In laboratory	A successful attack would require a major expenditure of time and effort on the part of a number of highly qualified experts, and the resources available only in a few facilities in the world.
5	Not feasible	The attack is no longer feasible

Table 1.2 Classes of the adversaries

Resources	Class 1 (a small group of curious hackers)	Class 2 (an academic research group)	Class 3 (an organized criminal gang)	Class 4 (a state-funded organization)
Time	Limited	Moderate	Large	Large
Budget	<$10,000	<$500,000	>$500,000	Unknown but Large
Goal	Challenge/prestige	Publicity	Money	Varies
Organized?	No	Yes	Yes	Yes
Will they release the attack's information?	Yes	Yes	No	No
Attacks they can wage	1–2	1–3	1–3	1–4

The "model" step will develop a graphical representation of the life cycle of an integrated circuit, which describes its main processes, their interactions and related security risks.

The "Identify Threats" step aims to provide an answer to the question "What do Attackers want". Understanding the goal of the attackers is critical to developing appropriate countermeasures. To achieve this, the following clarification of the goals of the IC supply chain attacker is proposed and adopted in this work, these are tied closely with security properties discussed previously, namely *counterfeiting, information Leakage, sabotage and tampering* (CIST). This step will also identify the attacks mechanisms related to each threat category. This includes identifying the following information for each attack:

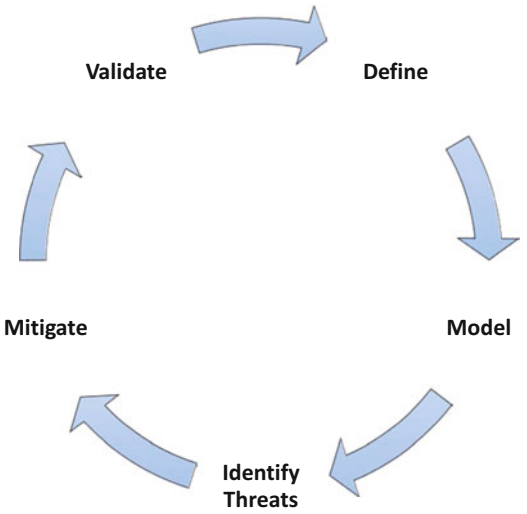

Fig. 1.2 The Threat Modelling Process of IC Supply Chain

1. The most likely adversary to wage the attack.
2. The attack difficulty.
3. The preconditions required to perform it. This include the assumed capabilities of the adversary and the root of security vulnerability. The latter include the factors that makes the attack feasible, technically or otherwise.
4. The stage(s) at which it is likely to take place during the IC life cycle.
5. Its impact or the damage it can cause (e.g. financial losses and reputation damage political gains).

The "mitigate" step identifies the defence techniques that could be used to mitigate the risk of ach attack.

The "validate" step considers the effectiveness of each of the countermeasures identified in step 4, taking into consideration the profile of the most likely attacker, the difficulty of the attack after implementing the countermeasure and the application scenario.

The CIST approach as identified above allows for systematic analysis of security threats and the identification of most appropriate countermeasures, given a particular application scenario.

1.4 Define: Definition of Security Properties

There are four fundamental goals for hardware security, which are based on the IC's applications and life cycle, namely:

- Authenticity is the assurance that an integrated circuit, an embedded device or any other piece or hardware is from the source it claims to be from. Authenticity

Table 1.3 CIST: a threat modelling approach for the IC supply chain

Threat	Security property	Definition	Examples of attack mechanisms
Counterfeiting	Authenticity	Fraudulently imitating an original IC	IC recycling IC overproduction
Information leakage	Confidentiality	Exposing sensitive design information or secret data stored on chip	Side-channel analysis IP piracy
Sabotage	Availability	Deliberately damage or destroy an IC or obstruct its production	Cyber-physical attacks Attacks on transport links to delay IC production
Tampering	Integrity	Maliciously change the data associated with the IC, during its development process or after its deployment	Trojan insertion Fault injections

requires a proof of identity, which should be provided by the device being checked.

- Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities or processes. In the context of hardware security, this information includes any sensitive data or code stored in the device or design secrets related to the intellectual property (IP) of the underlying circuitry.
- Integrity: means maintaining and assuring the accuracy, correct functionality and trustworthiness of the hardware device over its entire lifecycle, in other words the device is doing what it is expected to do nothing less and nothing more.
- Availability means the integrated circuit and its different abstraction levels are available when it is needed at every stage of its life cycle, from the initial specification to the final deployed hardware device. An example of an attack that undermine the availability include sabotaging the manufacturing cite to delay production or tampering with a deployed system to take it out of service. All types of Hardware security attacks aim to undermine one or more of the above four properties.

Table 1.3 provide a summary of the threats and corresponding security properties and exemplar attacks.

1.5 Model: Modelling the IC Supply Chain Security

There are a number of approaches that can be adopted here, data flow diagram [7] and PROV-N [14]. PROV-N is the notation of W3C provenance PROV family, which brings information about activities and people involved in producing a piece of

data. This information can be used to assess quality, reliability and trustworthiness [15]. PROVDM is the conceptual data model and distinguishes core structures, forming the essence of provenance information, from extended structures catering for more specific uses of provenance. PROV-DM is organized into six components, respectively, dealing with: (1) entities and activities, and the time at which they were created, used, or ended; (2) derivations of entities from entities; (3) agents bearing responsibility for entities that were generated and activities that happened; (4) a notion of bundle, a mechanism to support provenance of provenance; and (5) properties to link entities that refer to the same thing; (6) collections forming a logical structure for its members. This semantic modelling approach lends itself well to the description of the IC supply chain in the context of threat modelling, as it makes it feasible to construct a detailed articulation of the stages of the IC production, the agents responsible on each stages and associated security threats. Furthermore, it makes it feasible to investigate the vulnerabilities that are not yet exploited and expose potential attack combinations, with the lack of empirical data on some of the hardware attacks, the hypothetical attack scenarios provided by semantic modelling can assist in developing appropriate security policies for the IC supply chain. Therefore, the semantic modelling used in this research is based on the PROV-N modelling [16]. This was adapted to first model the IC manufacturing production line. The workflow was analysed from general description of IC manufacturing and was mapped using the following rules.

Rule 1 a process uses an entity to generate another entity.
Rule 2 an entity is either an input or an output.
Rule 3 a stakeholder is a person(s) that is directly responsible for a process.

Additional rules for the threat analysis are generated by blending the cyber-physical taxonomy [17] with semantic modelling using Prov-N as follows:

Rule 4 an attack targets only an entity that was generated by a process.
Rule 5 an attack that invalidates a generated entity automatically invalidates the adjacent process that used the same entity.
Rule 6 an attack needs a precondition for the attack to be successful.
Rule 7 an attack is carried by an attacker.

The graphical representation of the model will use the coloured notations listed in Table 1.4:

The above rules are used to model to each stage of the IC life cycle as shown in Fig. 1.3.

To explain, how this modelling approach can be used to systematically analyse hardware security threat, we consider a Trojan insertion attack on an IP development company as shown in Fig. 1.4. In this example, the stakeholder is the IP vendor. The latter is responsible for the IP development (i.e. a process). The input for this process is the research performed by the company and associated expenses. The output is the IP. The precondition that need to be satisfied for this attack to succeed is to have access the IP being developed. Such access can be achieved in a number of ways, typically referred to as the *Entry Points* (i.e. the entrances

Table 1.4 Notation for the CIST threat modelling analysis

Object	Notation
Process	
Stakeholder	
Entity	
Attack	
Attacker	
Preconditions	
Impact	

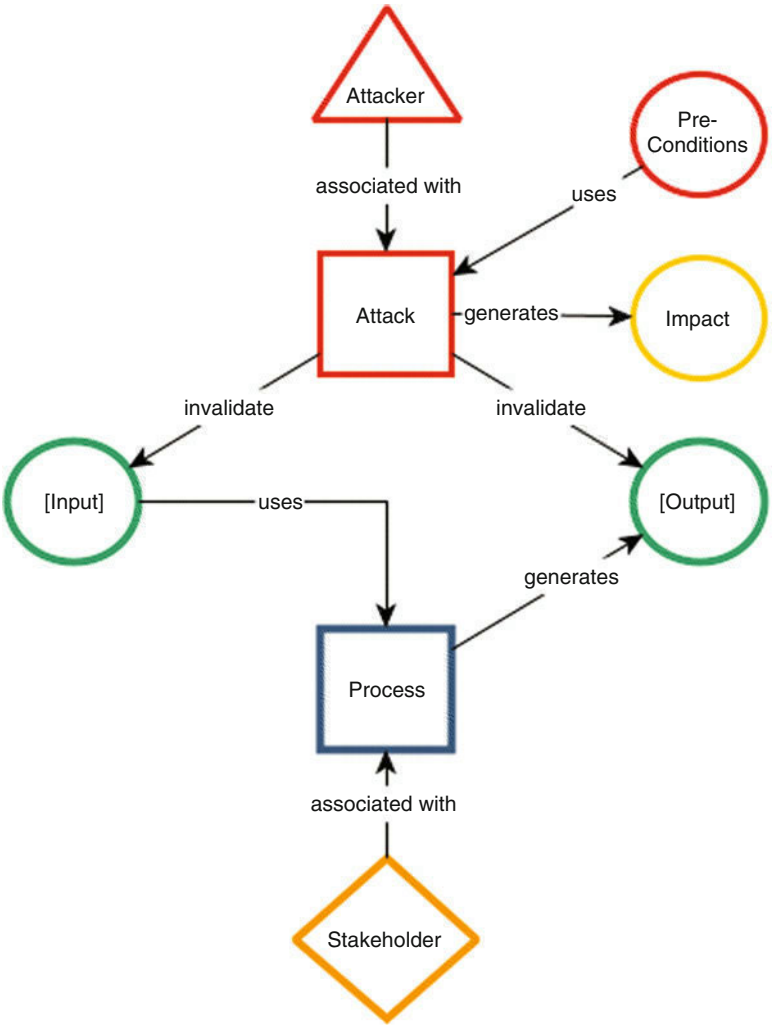

Fig. 1.3 A reference diagram for hardware supply chain threat modelling

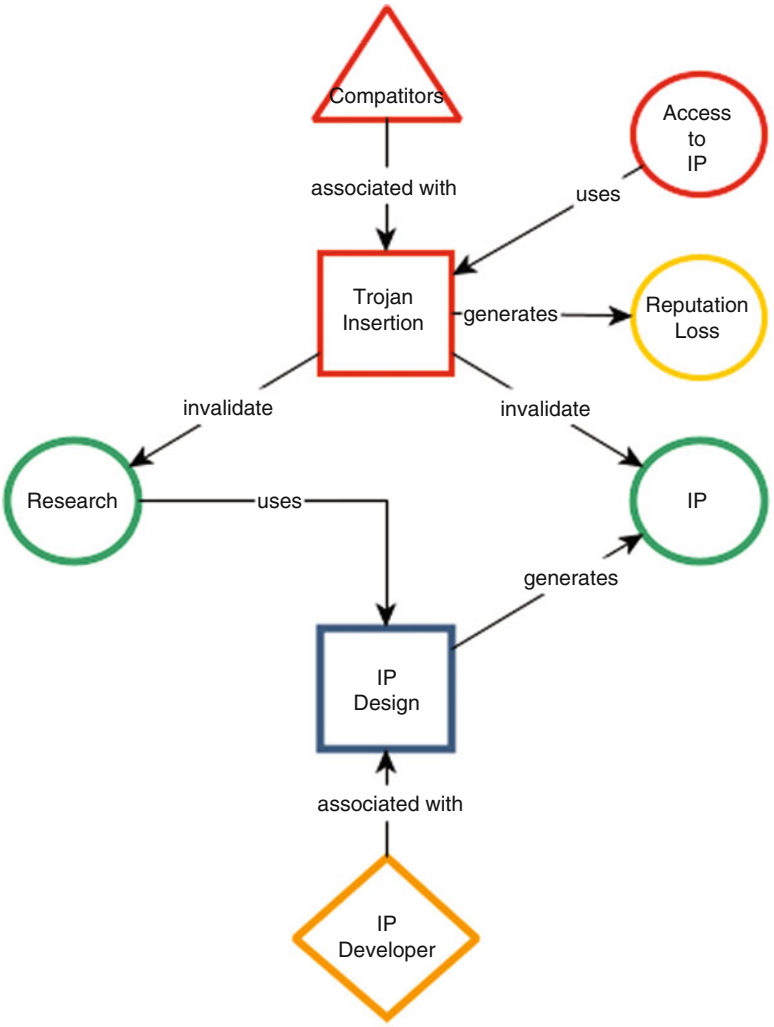

Fig. 1.4 Threat modelling of hardware Trojan attacks on IP vendors

where the attackers can interface with the target), which should be enumerated at this stage of the threat modelling process. In this example, the entry points include a malicious insider in the design house, a malware in the circuit design tools, and vulnerability in the IT infrastructure. There are a number of potential attackers, in this case, which include, a competitor or a malicious tool developer, or even a state-funded institution. However, it is important to identify the class of the most likely adversary in order to develop appropriate countermeasures.

The important aspect of this method is that it provides a systematic approach to think about each threat, its motivation, mechanisms and consequences. Furthermore,