The Big Hack Explained: Detection and Prevention of PCB Supply Chain Implants

DHWANI MEHTA, HANGWEI LU, OLIVIA P. PARADIS, MUKHIL AZHAGAN M. S., and M. TANJIDUR RAHMAN, Florida Institute for Cybersecurity (FICS) Research, University of Florida
YOUSEF ISKANDER, CISCO Systems
PRAVEEN CHAWLA, Edaptive Computing Inc.
DAMON L. WOODARD, MARK TEHRANIPOOR, and NAVID ASADIZANJANI, Florida Institute for Cybersecurity (FICS) Research, University of Florida

Over the past two decades, globalized outsourcing in the semiconductor supply chain has lowered manufacturing costs and shortened the time-to-market for original equipment manufacturers (OEMs). However, such outsourcing has rendered the printed circuit boards (PCBs) vulnerable to malicious activities and alterations on a global scale. In this article, we take an in-depth look into one such attack, called the "Big Hack," that was recently reported by Bloomberg Buisnessweek. The article provides background on the Big Hack from three perspectives: an attacker, a security investigator, and the societal impacts. This study provides details on vulnerabilities in the modern PCB supply chain, the possible attacks, and the existing and emerging countermeasures. The necessity for novel visual inspection techniques for PCB assurance is emphasized throughout the article. Further, a review of various imaging modalities, image analysis algorithms, and open research challenges are provided for automated visual inspection.

CCS Concepts: • **Printed Circuit Boards → Supply chain vulnerabilities**; *Electrical testing*; Automated visual inspection; Hardware Trojans;

Additional Key Words and Phrases: Emerging attacks, PCB testing, imaging modalities, machine learning, bill of materials

ACM Reference format:
Dhwani Mehta, Hangwei Lu, Olivia P. Paradis, Mukhil Azhagan M. S., M. Tanjidur Rahman, Yousef Iskander, Praveen Chawla, Damon L. Woodard, Mark Tehranipoor, and Navid Asadizanjani. 2020. The Big Hack Explained: Detection and Prevention of PCB Supply Chain Implants. *J. Emerg. Technol. Comput. Syst.* 16, 4, Article 42 (August 2020), 25 pages.
https://doi.org/10.1145/3401980

Authors' addresses: D. Mehta, H. Lu, O. P. Paradis, M. Azhagan M. S, M. T. Rahman, D. L. Woodard, M. Tehranipoor, and N. Asadizanjani, Florida Institute for Cybersecurity (FICS) Research, University of Florida, 601 Gale Lemerand Drive, Gainesville, Florida, 32603; emails: {dhwanimehta, qslvhw, paradiso, mukhil.mallaiyan, mir.rahman}@ufl.edu, {dwoodard, tehranipoor, nasadi}@ece.ufl.edu; Y. Iskander, CISCO Systems; email: yiskande@cisco.com; P. Chawla, Edaptive Computing Inc; email: p.chawla@edaptive.com.

1550-4832/2020/08-ART42 $15.00
https://doi.org/10.1145/3401980

1 INTRODUCTION

1.1 The Big Hack

Though the world has grown accustomed to software-based attacks, hardware has historically been *perceived* as secure. This notion has changed in the past two decades due to the shift in the semiconductor industry toward outsourcing different manufacturing steps for printed circuit boards (PCBs) around the world. Outsourcing has reduced manufacturing costs and allowed industries to meet aggressive time-to-markets. However, such globalization grants third-party players access to advanced technologies that are manufactured for critical infrastructures [Guin et al. 2014; Karri et al. 2010; Tehranipoor and Koushanfar 2010; Tehranipoor and Wang 2011]. Therefore, outsourcing introduces vulnerabilities in the PCB supply chain for adversaries to exploit.

Hardware attacks can be much graver than software attacks. Patching software is relatively easy and seamless, even when the product is deployed in the field. However, patching hardware is much more difficult and prone to error, especially when the product is in the field. Though hardware attacks are more difficult to carry out, because they require more time and resources, they can be more disastrous, because they provide long-term covert access. "The Big Hack" incident, published on October 2018 by Bloomberg Businessweek, is a prominent and recent example of one such hardware attack as shown in Figures 1(a) and 1(b). Figure 1(a) depicts the microchip that infiltrated almost 30 U.S. companies and Figure 1(b) divides the attack into three phases for ease of understanding. An account of the Big Hack is detailed below [The Bloomberg Businessweek 2018]:

According to the Big Hack article published by Bloomberg, the security of the motherboards of Super Micro Computer Inc. (Supermicro) was compromised. Supermicro's motherboards, which functioned as the neurons of several data centers, were found to possess a small malicious chip that infected the motherboards with malware every time the server booted up (Figure 1(a)). Though the investigation of the malicious chips began in 2015, it is believed that the attack on Supermicro's motherboards was initiated in 2014 (see the detailed timeline in Figure 2). It is suspected that the malicious chips were embedded onto Supermicro's motherboards by China's Liberation Army [The Bloomberg Businessweek 2018].

The consequences for Supermicro were devastating: its stock went down catastrophically by 41% [Vanian 2018]. The after-effects of the Big Hack were not limited to Supermicro. According to Bloomberg Businessweek, the malicious chips allowed Chinese spies to infiltrate at least 30 U.S. companies downstream the supply chain from Supermicro. Affected companies include Amazon, Apple, a major bank, and several government contractors [The Bloomberg Businessweek 2018]. Thus, the malicious chips threatened the whole U.S. intelligence community. Though so many groups were affected by the Big Hack, the consumers and many companies remained unaware until at least three years later, when the Bloomberg report was released. To better understand the Big Hack, a brief background of the major companies whose products were attacked is provided in the following. Then, the Big Hack is analyzed from three major angles as shown in Figure 1(b): (1.3) Attacker—where we emphasize on the targets for the attack—infiltrating U.S. companies, understanding the design, and the attack execution phase. (1.4) Investigator—where we emphasize on the private sector, intelligence officers, and U.S. officials involved in the investigations, and (1.5) Societal Impact—where we emphasize on the impact on the government and public companies.

1.2 Impacted Companies

1.2.1 Elemental Technologies. Elemental Technologies (Elemental) specialized in developing software to compress large video files meant for television screens, formatting them for display

(a) (b)

Fig. 1. (a) The microchip that infiltrated almost 30 U.S. companies [The Bloomberg Businessweek 2018]; (b) The Big Hack divided into these three phases.

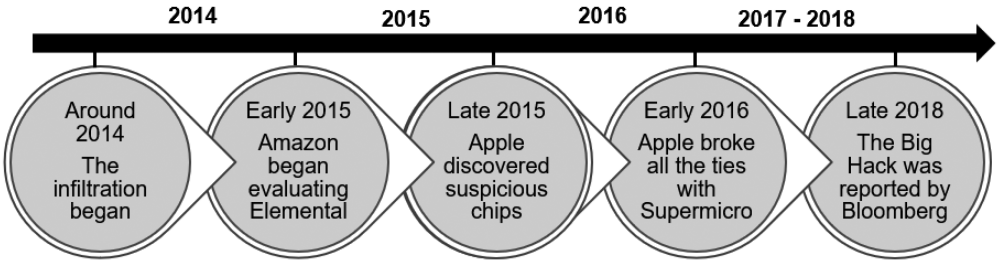

Fig. 2. The Big Hack timeline.

on smaller platforms such as smart-phones and tablets [AWS Elemental 2006]. Elemental soon developed a partnership with the CIA's investment arm. Through this deal, Elemental played a key role in several security missions, which include communicating with the International Space Station for NASA and funnelling drone footage for the Department of Defense. Thus, a collaboration with Elemental was considered by Amazon, which was planning a major expansion in its streaming video services (now known as Amazon Prime Video) and its highly secure cloud for the CIA (Amazon Web Services, AWS). Due to its role in multiple critical projects with the U.S. government, Elemental was a highly desirable target for foreign adversaries.

1.2.2 Supermicro Computer Inc. Supermicro specializes in servers, storage, networking devices, and server management software for data centers and cloud computing [Supermicro 1993]. In 2016, Supermicro was ranked the 18th fastest growing company on Fortune Magazine's top 100 list of the world's largest U.S. publicly traded companies [Fortune 2016]. Supermicro servers were used by hundreds of companies, including Elemental, for various purposes such as weapon systems, MRI machines, and web hosting devices. Though Supermicro had assembly facilities in California, Taiwan, and the Netherlands, its motherboards were manufactured by contractors in China. Due to its outsourced supply chain, Supermicro was an ideal target for foreign adversaries.

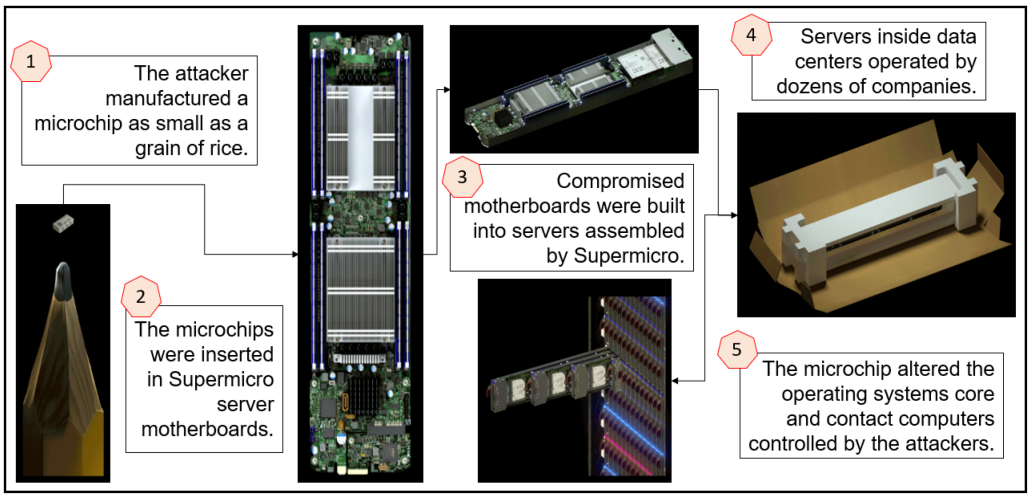

Fig. 3. The Big Hack: Execution steps of the infiltration.

1.3 Analyzing the Big Hack from Attacker's Perspective

1.3.1 Target for the Attack. As mentioned above, both Elemental and Supermicro served as ideal targets for attackers to invade critical infrastructures for long-term access. Such backdoor access could be used to cripple a company or a government. To carry out such a large-scale attack, it was first necessary to develop a deep understanding of the product design, manipulate the design during manufacturing, and ensure the manipulated products reached the desired locations.

1.3.2 Gaining the Design Understanding. In contrast to *interdiction*, which involves manipulating devices as they are in transit from manufacturer to customer, *seeding attacks* involve manipulating devices more upstream the supply chain. Seeding attacks occur during the manufacturing stages and require detailed knowledge of how the targeted company operates [The Bloomberg Businessweek 2018]. In the case of the Big Hack, X-ray images prepared by Amazon's security team indicated that the malicious chips looked similar to signal conditioning couplers, which are common components on motherboards. Variations between different chips indicated that a variety of malicious chips were delivered to various factories by the attacker. The malicious chips were capable of manipulating the core operating instructions, rerouting data across the motherboards, editing the information queue, injecting malicious code, and further altering the order of the CPU instructions. Attacks that are more upstream in the supply chain can grant attackers more widespread control in an inconspicuous manner.

1.3.3 Execution of the Infiltration. U.S. intelligence agencies heavily depend on advanced technologies provided by companies such as Supermicro. Supermicro had three headquarters: two in Taiwan and one in Shanghai. When there was a backlog of orders, Supermicro hired different subcontractors to help. A workflow of the infiltration is depicted in Figure 3. This unlatched a perfect channel for seeding attacks. Adversaries claiming to be representatives of Supermicro or the government requested, bribed, or, in some cases, threatened plant managers into manipulating the original board designs to include the malicious chips (Figure 3). The code in the malicious chips was small due to size constraints, but it was able to carry out two major tasks: (1) command the motherboard to communicate with external, anonymous computers and (2) prepare the device's operating system to accept new code from those external computers. This was possible because

the chips were connected to the baseboard management controller, which granted administrative access to remotely log-in. This could give attackers control of the most sensitive code in critical infrastructures during conflict and war. Details of the investigations into the malicious chips are highlighted in the next section.

1.4 Analyzing the Big Hack from Investigator's Perspective

As claimed by the Bloomberg story, the U.S. authorities went to the White House in 2014 with this information: China's Military was preparing to infiltrate U.S. companies by inserting malicious chips into Supermicro's motherboards, but it was not clear why and how. At the time, the government could not publicly issue a warning, because there was no conclusive evidence. The government had to be cautious, since Supermicro was the largest U.S. motherboard supplier and, thus, a publicly issued warning would affect many other companies. Hence, the FBI's investigation was limited at the time.

Meanwhile Amazon, which was interested in a potential acquisition for its own AWS cloud, began investigating Elemental's video compression technology through a third-party company. After the first security check revealed troubling issues, an investigation on Elemental's servers was conducted. Evaluators found a tiny microchip nested on the server's motherboards that was not part of the board's original design. Thus, Amazon filed a report and gave access to the sabotaged Elemental servers to the U.S. authorities.

In 2015, Amazon acquired Elemental Technologies with the intention of moving their software to the AWS cloud, whose chips, motherboards, and servers were typically designed in-house and manufactured by Amazon's contractors. However, an exception was AWS's data centers inside China, which mostly consisted of Supermicro servers. Tampered motherboards were discovered by Amazon's security team even inside AWS's Beijing facilities. Very thin malicious chips were found embedded in the fiberglass layers upon which other components were attached.

Similar accounts of malicious chips were reported by other companies such as Apple in May 2015. However, Apple did not provide government investigators with access to its facilities or the tampered hardware. Hence, the extent of the effects of the Big Hack on Apple remained outside the government's view. Even though the effects of the malicious chips on many companies were kept confidential, there was enough evidence for the FBI's cyber and counterintelligence teams to run a full investigation.

The investigators discovered that the chips opened a covert doorway into networks that could be used to alter critical infrastructures. It was concluded that the chips were inserted by Chinese subcontractors and was suspected to be the work of a People's Liberation Army unit specializing in hardware attacks. The government, armed with conclusive evidence, then issued a warning to Supermicro customers.

1.5 Analyzing Social Impacts of the Big Hack

The Big Hack was elaborately seeded during manufacturing and thus, was difficult to detect. Such hardware attacks pose severe consequences for companies beyond replacement costs for mal-functional servers. Time, money, and resources must be spent on thorough investigations to authenticate devices from untrusted sources. Without thorough investigations, companies risk privacy breaches and ruined reputations. When Apple identified the malicious chips, they had to remove and replace 7,000 Supermicro servers. Apple denied any such change, however, Apple did cut all ties with Supermicro the coming year citing "unrelated reasons" and a "minor security incident." Three senior Apple insiders reported the discovery of compromised Supermicro motherboards.

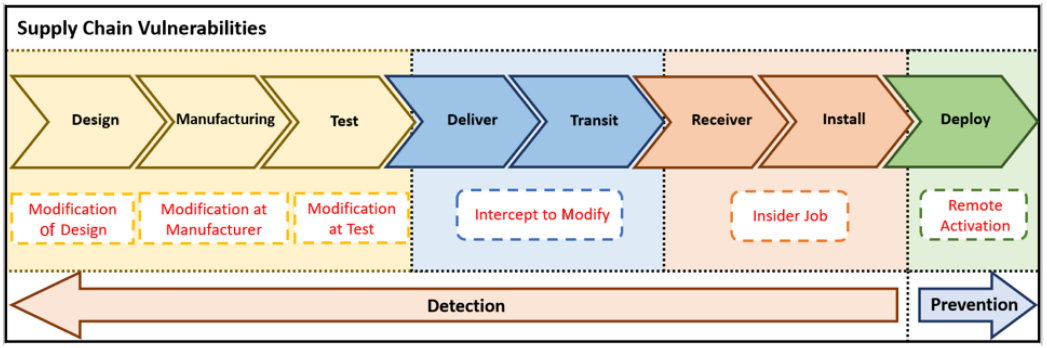

Fig. 4. PCB supply chain vulnerabilities.

Later, Amazon, Apple, and Supermicro denied all claims in Bloomberg Businessweek's report while the CIA and NSA declined to comment. The Chinese government implied the plausibility of the Big Hack by issuing a statement "Supply chain safety in cyberspace is an issue of common concern, and China is also a victim." Further, the manipulation of Supermicro's motherboards was confirmed by 17 credible sources, as claimed by the Bloomberg report. Due to sensitive and classified information, those sources were granted anonymity.

Supermicro not only denied all accounts in the Bloomberg report, it also denied any notifications of malicious chips by customers or law enforcement. Later, Supermicro failed to file reports that were required by regulators, resulting in the delisting of the company from Nasdaq on August 23, 2018. One year later, new vulnerabilities allowing remote USB access was discovered in Supermicro servers. Such vulnerabilities could be exploited by an attacker to gain control of the affected systems. On September 4, 2019, Supermicro issued security updates to patch vulnerabilities that affected the Baseboard Management Controller (BMC). These updates were for BMC components of X9, X10, and X11 platforms [CISA 2019]. As the aftermath of the Big Hack continues, it has been made clear by the White House that the supply chain needs to be less dependent on a small handful of countries.

The story of the Big Hack is told as a tangible, motivating example to question the security of the supply chain. In summary, vital PCB steps such as manufacturing, design, packaging, and distribution have been outsourced to lower the manufacturing costs and time-to-market. This outsourcing renders the supply chain vulnerable to attacks from external entities. The Big Hack is simply one such attack that shook the electronics community. Hence, the vulnerabilities of the supply chain are focused on in the next section.

2 SUPPLY CHAIN VULNERABILITIES

The modern business model of PCB design and fabrication favors extensive outsourcing and integration of untrusted components and entities in the PCB lifecycle to lower manufacturing costs and decrease time-to-market. Outsourced steps of PCBs have introduced numerous vulnerabilities and threats in the supply chain. Figure 4 [Rebello 2019] shows a detailed description of the existing stages in the PCB supply chain, as well as the vulnerabilities that are introduced in each stage. An untrusted entity can exploit these vulnerabilities to modify the PCBs at any point during the PCB lifecycle. Adversaries include, but are not limited to, system integrators, individuals, groups, governments, fabrication facilities, and counterfeiting parties. Adversaries can produce out-of-spec parts, clones, tampered PCBs, recycled parts, and so on, to gain unlawful advantages. Attacks such as IP piracy, Trojan insertion, cloning, and overproduction could provide back-door access for

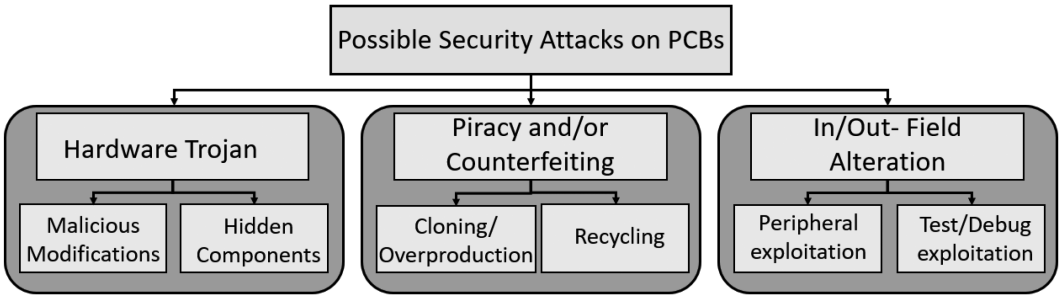

Fig. 5. Possible attacks on PCBs.

adversaries to execute a stealthy attack or cause denial of service. Thus, OEMs have lost control over the PCB lifecycle as the supply chain has opened up to third-party entities around the world.

Supply chain security is a difficult challenge. The IT industry is inexorably international and anyone involved in the process could subvert the security of the end product. Moreover, PCBs are highly prone to defects. For this study, reliability defects are considered out-of-scope. Rather, this article will focus on existing and upcoming vulnerabilities of the supply chain and possible countermeasures.

3 WHAT OTHER ATTACKS WERE POSSIBLE?

Fortunately, the attack described in the Big Hack story was discovered and addressed relatively early [The Bloomberg Businessweek 2018]. The Big Hack not only required a vision for years but also a deep understanding of the target's design process. The effects of such an elaborate attack on critical infrastructures could have been far worse. Hence, it is important to carefully examine the PCB supply chain and its vulnerabilities.

There is a trade-off between cost and security: one must choose between a sparse supply of expensive but secured electronics or an abundant supply of inexpensive but unsecured electronics. Driven by revenue, companies usually chose the latter, which makes the job of an antagonist much easier. Thus, the supply chain is left vulnerable to attacks such as hardware Trojan insertion, piracy/counterfeiting, and in/out-field alteration as depicted in Figure 5. The Big Hack affected many top-rated companies and, in turn, revealed the weaknesses of quality assurance processes and supply chain control. Identifying vulnerabilities and developing appropriate countermeasures can prevent such devastating attacks.

There is an urgent need for developments of hardware assurance, though many companies are hesitant to disclose the extent of that need due to the reputations they must uphold. One thing is for certain: The Big Hack was not the first incident to raise the alarm against existing assurance processes. Examples of previous attacks that have also greatly affected the security community are discussed below. Then, several other possible attack scenarios are given to emphasize the importance of assurance and security in the supply chain.

3.1 Other Attacks

In 2014, Marc Heera, a Florida man, was charged by the FBI for selling a cloned version of the Hondata s300. The fake vs. the real version of the Hondata s300 are shown in Figure 6 [The FBI 2014]. These look-alikes contained circuit boards that were reportedly made in China. The Hondata s300 was a plug-in module for a car engine computer, which was responsible for reading data from the car's sensors. Thus, the plug-in played a key role in the automatic adjustment of the air-fuel mixture, idle speed, and other factors for improving performance. Alarmingly, the module

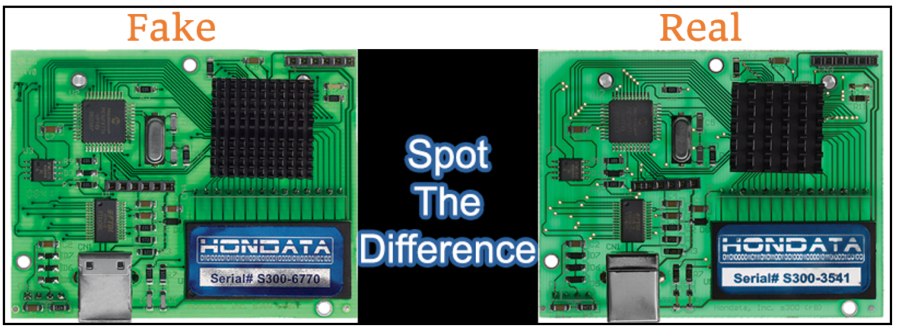

Fig. 6. Honda s300 cloned and real system [Jack Laidlaw 2017].

also gave the user privileged access to monitor the engine and even customize the system through Bluetooth. Such privileged accesses, given to the cloned module, could impose serious safety concerns such as failure to start, random limits on engine rpm, and hijacked car brakes or steering wheels. Such critical failures in the field due to the cloned plug-ins could compromise the safety of the drivers/passengers.

In 2010, Ehab Ashoor, a Saudi citizen, was convicted for the purchase of cloned Cisco Systems gigabit interface converters [Tehranipoor et al. 2017]. These counterfeit systems were meant to be used by the U.S. Department of Defense for transmitting troop information, relaying it to remote fields, and forwarding it to command centers to Marine Corps networks in Iraq. Such malicious devices in secure electronic systems could prove to be fatally catastrophic.

There are several other attacks that took advantage of PCB vulnerabilities. For example, the Joint Test Access Group (JTAG) test access port has been repeatedly exploited for access to the PCB's internal features, information, and secret keys [Rosenfeld and Karri 2010]. In one instance, the TAP was used to hack Xbox's by disabling the Digital Rights Management policy [Rosenfeld 2012]. These attacks open up a new discussion on what other attacks were possible.

3.2 Emerging Attacks

The above-mentioned attacks are only a few of the incidents that have been reported. The question then arises, how would one detect an even stealthier attack? The financial, data, and privacy losses due to such attacks could be used as indicators, but they are difficult to quantify as they often affect multiple individuals, groups, and companies. Even after detection, it is difficult to determine if all the victims have been identified, if there will be further losses, and if there will be more victims in the future. Hence, in the following, we briefly discuss other possible PCB attacks:

3.2.1 Hardware Trojan—Kill Switch. A kill switch can be used to cause denial of service. This can cause the destruction of entire databases, networking systems, weapons, or other critical infrastructures during emergencies or conflicts.

3.2.2 Hardware Trojan—Infiltrate Communication Lines. A hacker can infiltrate a communication line to alter, corrupt, or delay signals. This can cause a product to fail in the field. Moreover, spies can use infiltrated communication lines to gain access to classified information.

3.2.3 Piracy/Counterfeiting—Cloning PCBs. An adversary with access to a pirated PCB design file can clone the PCB to make a profit. This drives business away from honest companies that invest significant amounts of resources for research and development. Unlike counterfeit electronics of the past, modern clones are very sophisticated [Tehranipoor et al. 2015]. These cloned

Table 1. PCB Testing

Testing Technique	PCB Stage	Human Factors	Hardware Trojans	Cost
In-Circuit Testing	Populated boards	Bed-of-nails development/Flying probe test programming; board transport for test setup	Only detects Trojans that alter tested nodes	≈ $20k+ [Matric 2019]
Functional Testing	Populated boards	Software programming; board transport for test setup	Only detects Trojans that alter tested board functions	≈$50k+ [Matric 2019]
JTAG Testing	Populated boards	Higher design requirements; software programming; board transport for test setup	Only detects Trojans that alter tested nodes	≈$119+ [JTAGTest n.d.]
Bare-board Testing	Unpopulated boards	Board transport for test setup	Testing is done on bare board, hence cannot detect Trojans	≈$2k+ [Hroundas 1986]
Visual Inspection	Populated/ Un-populated boards	Software programming; potentially no board transport for test setup automation possible	Can potentially detect all types of Trojans, if using multiple imaging modalities	≈$12k+ [Verma 2002]

PCBs could facilitate a nation-wide attack. Clones, which have likely not undergone rigorous testing, are typically less reliable than the genuine products. Moreover, clones may host malicious software, firmware, or hardware, which could prove fatal in the field if the clones are used in security-sensitive, critical infrastructures.

Hardware attacks that reroute information pose a dire threat even after they are detected. Such hardware attacks may only be the beginning of a greater threat. For example, leaked war strategies, weapon designs, troop locations, and access keys could be analyzed at any point thereafter to inform future attacks. Hardware can be replaced but it is nearly impossible to recover leaked information. Hence, it is critical to authenticate PCBs quickly and accurately before they are deployed to the field.

Moreover, modern PCBs are becoming more complex as they feature highly integrated designs, multiple layers, complicated structures, hidden vias, and embedded passive components. This complexity provides more hiding opportunities for adversaries to implant hardware Trojans. This further complicates the authentication process. Hence, it is critical to consider the current state and the future of hardware assurance technologies.

4 WHAT COULD HAVE BEEN DONE?

Two important questions to consider include: (1) Is it possible to detect a hardware attack before it occurs?; (2) Is there a way to protect the security of the PCB supply chain in the future?

Numerous PCB assurance techniques have been proposed over the years and a summary of them is shown in Table 1 [Aksu 1976; Pedder 1998; Shahparnia and Ramahi 2004; Smith 1995]. Approximate price ranges are also provided for all the testing techniques; however, it is important to note that these costs vary based on a variety of factors such as PCB size, shape, material, number of layers, complexity, and so on. These methods are detailed and evaluated below. Further, we propose a novel solution (visual inspection) that is complementary to the existing works and has many additional advantages for the future of the electronic supply chain.

4.1 In-circuit Testing

In-circuit Testing (ICT) involves the use of electrical probes to check the resistance, capacitance, or other electrical quantities at each node on a populated PCB [Buckroyd 2015]. This determines whether each component in the design file is placed correctly on the physical PCB. ICT can be

performed using either a bed-of-nails test fixture or a flying probe setup. A bed-of-nails setup involves a test fixture with an array of small, spring-loaded pins [Millennium Circuits Limited 2019]. Each pin makes contact with one node in the circuitry of the PCB. When pressed against the pins, contact is made with thousands of individual test points simultaneously. A flying probe test involves a pre-programmed automatically moving probe in a fixtureless setup [Stark et al. 2014].

4.1.1 Advantages. ICT can effectively detect defective solders, short circuits, open connections, and missing components.

4.1.2 Disadvantages. ICT is difficult to perform for densely populated, multi-layered boards and can be expensive due to the costs associated with having to develop different test setups for different PCB's. Since ICT assumes that a correctly assembled board should work, it only tests the assembly and not the functionality of the PCB. Thus, ICT is ineffective for detecting connection faults, non-electrical defects, and hardware Trojans that do not affect the tested nodes.

4.2 Functional Testing

Functional testing is typically performed later in the PCB manufacturing cycle as a final check. A functional tester simulates the electrical inputs of the intended working environment, interfaces them to the PCB, and then measures the electrical outputs [Cal Houdek 2016]. Hence, functional testing evaluates the functionality of the product, independent of the assembly of the board. Functional testers typically consist of an interface to the PCB, a cabinet, cabling for the connection between all the instruments, a CPU, and monitors.

4.2.1 Advantages. Functional testing can identify functional defects, measure the PCB power consumption during operation, and uncover problems within the analog and digital circuitry.

4.2.2 Disadvantages. The functional testing setup is different for different boards, thus the exact hardware needed will vary depending on the PCB [Adam Cort 2002]. Hence, to ensure high detection rates, it requires time, resources, software programming knowledge, and a deep understanding of the PCB and its working environment. A major drawback is that functional testing relies on connectors, which are prone to reliability issues due to wear-and-tear. Moreover, its effectiveness is influenced by the testing scope, simulated inputs, and how an "acceptable" output is defined. Hence, functional testing is ineffective for detecting hardware Trojans that do not alter the tested board functions.

4.3 JTAG Boundary Scan Testing

Boundary scan testing involves testing a PCB's integrated circuits and wire lines through a JTAG test access port [Gupta 2019; Hassan et al. 1988]. Though JTAG boundary scan does not test all nodes, it provides the equivalent of ICT without the use of fixtures.

4.3.1 Advantages. JTAG allows the reuse of test patterns from system-level to board-level and from board-level to chip-level. Since boundary scan testing is fixtureless and does not test all nodes, it is less expensive and faster than ICT.

4.3.2 Disadvantages. Including a JTAG test access port on a PCB increases the cost and area overhead. Since JTAG boundary scan only tests chips structurally and PCB traces, it is ineffective for detecting hardware Trojans that do not affect the tested nodes.

4.4 Bare-board Testing

Bare-board testing involves checking if circuit connections appear as noted on a bare circuit board [Johnston 1996]. This process requires a netlist and a multimeter to perform a continuity test. These determine short circuits and open circuits by "charging" a net and then probing each net to measure the induced capacity [Chintan Panchal and Parth Rao 2014].

4.4.1 Advantages. This type of testing is inexpensive and easy to perform in comparison to the other testing techniques listed above.

4.4.2 Disadvantages. Since a bare PCB board is evaluated, neither the function nor the assembly of the final product are tested. Therefore, bare-board testing cannot be used to detect faults or malicious implants that occur during assembly. Further, unpopulated versions of the boards and netlists may not be available.

4.5 Automated Visual Inspection

Visual inspection involves the use of imaging modalities, which will be further discussed in a later section, to evaluate PCB's at the surface, volumetric, or material level [Quadir et al. 2016]. The produced images are then analyzed for defects. Historically, this analysis has been manually conducted by subject matter experts (SMEs). Due to its reliance on human factors, manual visual inspection is tediously time-consuming and prone to error. Therefore, the area of automated visual inspection, which relies on computer vision instead of SMEs, is a vastly growing field featuring a variety of techniques.

4.5.1 Advantages. Compared to manual visual inspection, automated visual inspection features several benefits such as high speed, persistence, and objectivity. The most significant advantage of automated visual inspection is its versatility in detecting malicious implants especially when golden netlist/CAD file is available.

4.5.2 Disadvantages. The main disadvantage is that visual inspection cannot verify functionality.

Each PCB assurance method listed above has their own benefits, limitations, and scenarios where they are considered effective. As hardware attacks are becoming increasingly complex due to advances in technology, there is a growing need for more advanced detection methods. Thus, the security of future PCB supply chain may lie in a combination of these methods. Ideally, such advanced solutions are non-destructive, require minimal human input, and can detect all types of malicious implants or defects on a PCB. Of the reviewed methods, automated visual inspection has the potential to require the least amount of human input, because it does not involve board-specific fixtures or external test setups, making it ideal for testing a large volume of PCBs. Moreover, it does not require the PCBs to be at any particular stage of manufacturing whereas ICT, functional testing, and JTAG boundary scanning require fully populated boards and bare-board testing requires a completely unpopulated board. In contrast, automated visual inspection can be used to identify malicious implants, hardware attacks, or defects throughout the manufacturing process, before or after deployment. Hence, we believe it could play a key role in securing PCB supply chain in an increasingly globalized and technologically advanced world. Thus, the rest of this article, will focus on automated visual inspection.

5 WHAT SHOULD BE DONE—ADDRESSING VULNERABILITIES

Careful consideration must be given to ensure a suitable automated visual inspection method for the task at hand. Automated visual inspection techniques can be subdivided into two main steps:

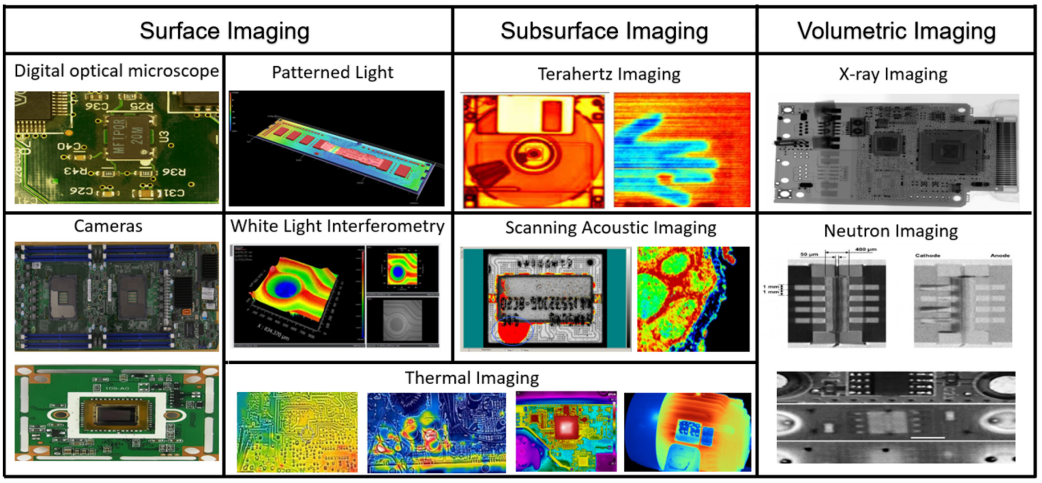

Fig. 7. Different imaging modalities that can be used for automatic visual inspection.

(1) PCB evaluation using imaging modalities as shown in Figure 7 and then (2) image analysis using computer algorithms. These steps will be discussed in the following sections.

5.1 Image Acquisition

Image acquisition is the first step in automated visual inspection of PCBs. There are a myriad of imaging modalities available for image acquisition. Modalities involve an imaging source, such as light or sound, and a sensing system. Different modalities vary in the type of information that is captured and processed.

Imaging modalities can be divided into three major categories: (1) Surface Imaging, (2) Subsurface Imaging, and (3) Volumetric Imaging. Figure 7 and Table 2 present an overview of several prominent imaging technologies such as surface imaging, subsurface imaging, and volumetric imaging, where the in-depth review is provided below.

5.1.1 Surface Imaging. This category primarily consists of sensing equipment that operate in the optical or infrared electromagnetic (EM) spectrum. Here, EM radiation is directed toward a surface and the reflected rays are captured by a detector placed near the source. The reflected waves vary based on the characteristics of the surface. This variation is eventually used to construct an image. Hence, surface imaging can be used to evaluate external board markings, defects, component labels, addition, deletion, and change.

(1) **Digital Optical Microscope:** Digital optical microscopes involve the emission of visible light from a source. The imaging speed is affected by the size of the PCB and the magnification used for imaging.
   (a) **Advantages:** Optical microscopes are relatively inexpensive and can capture high-resolution images. They quickly evaluate small, external features on the PCB such as component labels, scratches, vias, individual pins, traces, and board text.
   (b) **Disadvantages:** It can be difficult to capture the entire surface of a large PCB in one image with a digital optical microscope. Typically, several smaller images must be taken and stitched together using image processing. This may result in image artifacts and inconsistent illumination in the final image.

Table 2. Summary of Different Imaging Modalities

Imaging Modality		Speed[a]	Mag[b]	Dim[c]	Cost[d]	Applications
Surface Imaging	Digital Cameras	Seconds	2–10×	2D	≈$100–$5k *	Localization, identification
	Digital Optical Microscope	Minutes	12–2,500×	3D	≈$500–$10k *	Localization, identification, defect analysis
	Structured Light Imaging	Minutes	1–200×	3D	≈$1k *	Localization, placement validation, dimension measurement
	White Light Interferometry/Laser	Seconds	1–200×	3D	≈$20k–$50k *	Localization, placement validation, dimension measurement
Subsurface Imaging	Thermal Imaging	Minutes	2–20×	2D	≈$2k–$20k	Realtime performance evaluation, short/open circuit detection
	TeraHertz Imaging	Minutes	2–10×	3D	≈$2k–$70k [TerahertzStore n.d.]	Identification, distinguish materials/composition
	Scanning acoustic microscopy	Minutes	2–250×	3D	≈$10k–$30k *	Identify integrity of materials, cracks check, delamination
Volumetric Imaging	X-ray	Hours	2–10×	3D	≈$1k–$6k [NeutronOptics-Grenoble n.d.]	Traces/Vias interconnection verification, netlist authentication
	Neutron Imaging	Hours	2–10×	3D	≈$1k–$6k [NeutronOptics-Grenoble n.d.]	Capacitors verification, identify materials

[a]Imaging speed: the time cost of taking one image. [b]Magnification. [c]Image dimension. [d]Cost is estimated based on the online available commercial products. *Price provided by Google Shopping.

(2) **Cameras:** Cameras also image in the visible light range. An array of sensors within the camera captures light energy and converts it to electrical energy. The captured electrical energy is then used to construct an image. Cameras include smartphone cameras as well as digital single-lens reflex (DSLR) cameras. With recent advances in digital photography, cameras are now offering higher resolution and zooming capabilities. In addition, cameras allow videos and panoramas to be taken.
   (a) **Advantages:** Cameras are a quick, portable, and inexpensive way to evaluate a PCB. Further, videos allow data to be collected while the light sources, samples, or sensors are moved over time. This data can be used to extract depth information.
   (b) **Disadvantages:** Compared to optical microscopes, cameras have a relatively low magnification. Hence, it is a challenging task to accurately evaluate objects that are smaller than board text. Moreover, cameras are inherently prone to vibration, which greatly affects image quality. Therefore, cameras must be mounted on a fixed stage and secured with stabilizers.

(3) **Structured Light Imaging:** Structured light imaging involves projecting patterned light onto the surface of a PCB [Peng 2007]. This patterned light is distorted on the nonuniform surface of the sample. These distortions are detected and used to develop a 3D map of the PCB's surface.
   (a) **Advantages:** Most importantly, structured light imaging provides depth information on the PCB's surface. Additionally, scanning can be done in large 750 × 500 cm^2 sections, modeling the entire PCB in minutes with a resolution as low as 2.5 μm [Geng 2011; Rocchini et al. 2001].
   (b) **Disadvantages:** Structured light imaging can be relatively expensive. Further, patterned light-based measurement alone does not produce an optical image. As such, it

cannot identify components or read part numbers unless it is combined with another imaging modality.

(4) **Laser/White-Light Interferometry:** Interferometry involves the projection of a moving light beam or laser onto the PCBs [Wyant 2002]. Characteristics of the beams that are reflected from incident surfaces are collected and used to determine a 3D map of the PCB's surface and can provide similar information as structured light imaging.
   (a) **Advantages:** Laser interferometry offers resolution as low as 2 μm [Park et al. 2007]. This is slightly better than the resolution of structured light imaging.
   (b) **Disadvantages:** Similar to patterned light-based measurement, interferometry is also relatively expensive and does not, alone, produce an optical image.

5.1.2 Subsurface Imaging. The imaging modalities in this category provide information on some of the internal features of the PCB [Sun et al. 2014]. Subsurface imaging is a very diverse field, consisting of a variety of different sources and sensors that operate in the thermal, EM, or audio spectrum. Hence, subsurface imaging can be used to verify components within packaging and check for material continuity.

(1) **Thermal Imaging:** Thermal imaging uses an infrared sensor to measure the irradiated heat from individual components and traces while the PCB is in operation [Lloyd 2013; Vollmer and Möllmann 2017]. Infrared sensors include commercially available infrared cameras and microscopes for low and high-resolution imaging, respectively. It provides the runtime characteristics of components within packages as well as traces that are hidden behind components. This is done by using spectral information that is present in the other surface imaging techniques.
   (a) **Advantages:** Thermal imaging measures reliability defects and malicious attacks that discharge heat such as power-to-ground, shorts, and rerouted traces. In addition, thermal imaging cameras are fast and portable while thermal imaging microscopes have a high resolution.
   (b) **Disadvantages:** Thermal imaging alone cannot be used to identify a component. Moreover, it is relatively expensive.

(2) **Terahertz Imaging:** This modality utilizes the terahertz range of the EM spectrum to image the surface and subsurface of the PCB [Hu and Nuss 1995]. One application of terahertz imaging is analysis of material properties such as dielectric characteristics.
   (a) **Advantages:** Terahertz imaging can penetrate through plastics. It can be used to evaluate components within packages non-destructively. In addition, terahertz imaging can quickly perform elemental analysis on the material due to the uniqueness of the Terahertz refractive index for each material.
   (b) **Disadvantages:** The biggest limitation is that terahertz imaging cannot penetrate through metals, which are common materials on PCBs. Moreover, terahertz imaging systems can be relatively expensive.

(3) **Scanning Acoustic Microscopy:** Scanning acoustic microscopy involves focusing a beam of sound waves toward the sample. The transmitted power is then detected by a transducer probe that scans over the surface of the PCB. This method is able to obtain a resolution of 5 μm [Günther et al. 1989].
   (a) **Advantages:** Scannning acoustic microscopy evaluates the continuity of the PCB surface. Hence, it can identify cracks, voids, and delamination [Lemons and Quate 1974].
   (b) **Disadvantages:** Scanning acoustic imaging is relatively slow as the speed depends on the path of the transducer probe and the size of the board.

5.1.3 Volumetric Imaging. The modalities in this category typically involve radiation or subatomic particles that penetrate through a sample. The signals are then captured by a detector placed on the other side of the sample, opposite the source. The attenuated signals detected by the sensor vary based on the internal characteristics of the PCB. This variation is used to construct a 3D image of the sample. Hence, volumetric imaging can be used to evaluate internal structures, connections, materials, and hidden defects.

(1) **X-Ray Imaging:** X-ray has been used in the non-destructive reverse engineering for PCB assurance [Asadizanjani et al. 2015]. X-rays systems are available in two forms: 2D and 3D. 2D X-ray captures singular cross-sectional slices of a sample whereas 3D X-ray CT captures many projections to build a 3D volumetric model. X-ray penetration depth depends on the sample material, filter material, and the emission voltage used for scanning. X-ray Laminography, a special case of 3D X-ray, can better scan the details of flat samples in particular PCBs.
   (a) **Advantages:** The biggest advantage is that X-ray can be used to evaluate the internal structures within the PCB. This allows for detection of hardware Trojans and defects that are hidden within the layers.
   (b) **Disadvantages:** Reconstructed X-ray images have artifacts at boundaries between high- and low-density materials. Moreover, X-ray images have only one color channel, require several processing steps for 3D reconstruction, and cannot be used alone to identify components on a PCB. In addition, 3D X-ray imaging is comparably slow, expensive, and requires a high degree of maintenance.

(2) **Neutron Imaging:** Neutron imaging is a relatively new modality that uses neutrons in an atom. Similar to X-Ray, neutron imaging can be also used to obtain 2D projections as well as 3D volumes using computed tomography.
   (a) **Advantages:** Neutron imaging, similar to X-ray imaging, can be used to evaluate the internal structures within the PCB. In addition, given enough energy, neutron imaging is powerful enough to penetrate heavier elements that X-rays cannot [Anderson et al. 2009].
   (b) **Disadvantages:** Neutron imaging systems, similar to X-ray systems are also slow, expensive, and require a high degree of maintenance. Moreover, neutron imaging cannot penetrate through the plastics that X-rays can [Anderson et al. 2009].

While these are the common techniques used to evaluate PCBs, it should be noted that there are also other imaging modalities [Grzyb et al. 2014]. The selection of imaging modalities is driven by factors such as cost, application, and the desired detection speed and accuracy. Data captured with one imaging modality may highlight one type of hardware defect/Trojan while completely overlooking another. In summary, PCB information acquired using different imaging modalities should be explored, and the combination of imaging modalities could prove promising to address PCB assurance as a whole. Such combinations are called sensor fusion or image fusion and can provide multi-spectral information that can help identify various types of defects at once, when used with proper image analysis algorithms.

5.2 Image Analysis

Once the imaging modality is chosen, images of the PCBs are acquired. The acquired images are then analyzed for potential vulnerabilities and malicious components. Figure 8(a) presents a flowchart of the Automatic Bill of Materials (AutoBOM) process. This flowchart is divided into three phases: imaging modality (for full details see Section 5.1), image analysis, and authentication. Image analysis and authentication are explained in detail below. The image analysis phase is the most

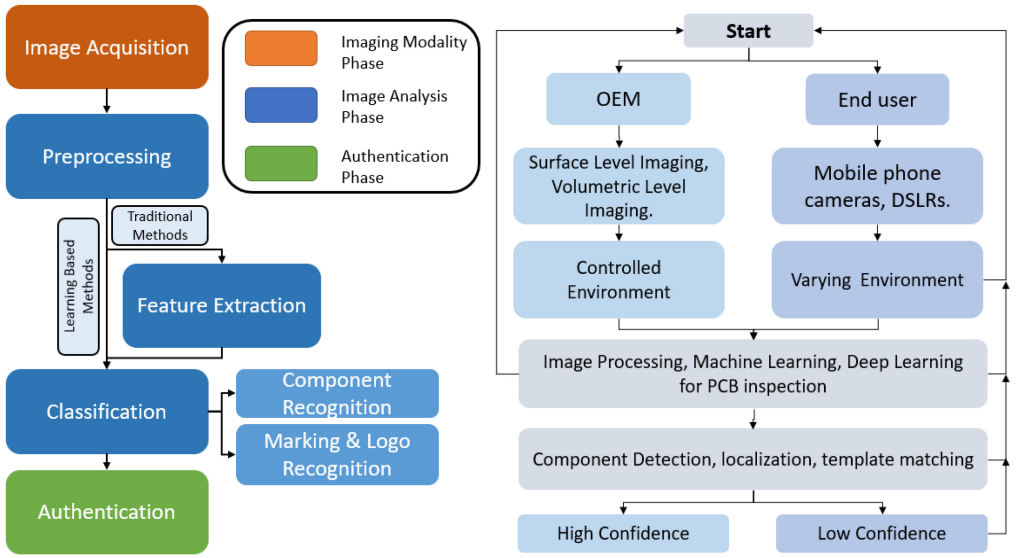

Fig. 8. (a) Steps taken in AutoBoM generation; (b) OEM vs. End User.

intricate of the three phases as subdivided below: *Preprocessing, Feature Extraction, and Classification.* Approaches to the aforementioned substeps depend on the imaging modality, resolution, and data availability. Extensive prior research has been conducted on object detection and classification in the parent field of image analysis. However, limited literature is available on the use of image analysis methods for PCB component detection [Moganti et al. 1996]. Hence, we will present the importance of the preprocessing, feature extraction, and classification substeps in the following sections. In addition, a review of the most widely used algorithms and challenges will be included for each substep.

5.2.1 Preprocessing. This is the first step in any image processing application. The purpose of preprocessing is to improve the quality of the image for object detection, without losing relevant image information. Preprocessing can include noise removal, illumination correction, and contrast enhancement. The algorithms used for preprocessing will depend on the choice of imaging modality.

Challenges in Preprocessing: The amount of preprocessing necessary varies from image to image and is dependent on the chosen image modality. Therefore, a "one-size-size-fits-all" approach is not feasible. Optimal image processing requires human assessment by SMEs.

5.2.2 Feature Extraction. The goal of feature extraction is to represent objects within an image with a low-dimensional representation that captures the salient characteristics of those objects. Ideally, the feature representation simplifies object classification. Feature representations capture the charactersitics of the objects to be detected such as their color, texture, or shape. The chosen feature representation should be invariant to scale, illumination, occlusion, and rotation. Such feature representations improve the accuracy of object classification.

Challenges in Feature Extraction: Similar to preprocessing, feature extraction is dependent on the choice of image modality. In addition, domain knowledge is necessary to inform the most suitable

feature representation. Feature representations that are suitable for the classification of one type of component may not be sufficient for the classification of another. Finally, it may be impossible to choose a feature representation that perfectly separates objects into their distinct classes based solely on images taken using a single modality.

5.2.3 Classification. The goal of the classification phase is to categorize and group similar components. Resistors, capacitors, transistors, and ICs should each be grouped into different classes. Moreover, the markings and labels should be read so the detected components can be cross-referenced with datasheets and online resources to yield a Bill of Materials (BOM).

Recognition of text on the PCB board, and on the components themselves is vital for authentication [Mori et al. 1999; Smith 2007]. Counterfeit parts can be detected by cross-referencing the component serial number with the OEM. Furthermore, malicious additions and removal of components can be identified by comparing the detected BOM with the expected BOM. For a more detailed analysis, the texture of the components can be compared with golden samples. For example, the logo on a suspect component can be compared to the logo of an ideal component to determine counterfeiting. However, there are many cases where the golden sample does not exists and other assurance methods should be developed.

Conventional Approaches vs. Learning-based Approaches: Traditionally, classification was performed by comparing patterns and features between two images. Methods such as template matching were used for direct image-to-image comparison, whereas feature matching was performed using correlation and distance metrics. However, with the advent of deep learning, systems capable of simultaneously performing both feature extraction and classification have emerged. Such methods are efficient and can outperform human-selected features. Due to the following reasons, their role in image processing and computer vision has become widespread.

Challenges in Classification: Despite optimal preprocessing, feature extraction, and classification method choices, it is still possible to have classification errors due to model overfitting. An overfitted model may have a high performance during development but will have a low performance during deployment. To avoid overfitting, enormous datasets of labeled images are necessary. If such large datasets are infeasible to obtain, then another way to avoid overfitting involves the use of simplier classification models. Also, the development of a dedicated system to address overfitting is a challenging task.

5.2.4 Authentication. After image acquisition and analysis, the final step is to perform authentication. The objective here is to present the results from image analysis in a readable format that can be analyzed by a computer or SME. There are two possible scenarios of interest in physical inspection; Scenario 1: when there is a golden sample, Bill of Materials, layout, or CAD file available for cross-verification (this is usually the case for OEMs, CEMs, and partner companies with access to product IP and design specifications), and Scenario 2: when there is no such golden sample or data for cross-verification (this is the case for end users such as individuals or consumer companies). Figure 8(b) presents a workflow of the two different cases within PCB verification. It is essential to understand both scenarios, as this will help inform which imaging modalities and imaging algorithms will be used, along with their benefits and limitations. While there is a need to authenticate PCBs in both cases, the accuracy and thoroughness of the inspection will vary.

The process of authentication can be separated into the storage phase and the authentication phase. After image analysis, there is a need to store the obtained information. In the case of PCBs and microelectronics, there are two common options:

(1) **Bill of Materials:** The Bill of Materials (BOM) is a spreadsheet or document that lists all components used to fabricate the PCB. The BOM provides the name, location, and placement of each component on the board.
(2) **Computer-aided Design:** CAD is a much more comprehensive model of the entire PCB. It provides information on the entire PCB layout, including traces and vias from all layers, in addition to the location of all the components.

Both BOM and CAD are widely used in the electronics community. Therefore, it is important to present information obtained from the image analysis phase as either a BoM or a CAD. In addition to the information format, the processing of the information for authentication is also dependent on the requirement specifications. As previously mentioned, there are two possible scenarios based on the user type. OEMs and CEMs have access to the golden sample information such as a BoM, CAD files, or even a golden PCB. However, consumers, end users, and independent groups may not have this golden sample information for comparison. The following two scenarios are described below:

(1) **OEM Scenario—Presence of Golden Sample Information:** Golden sample information such as BOMs and CAD models are available to cross-verify the data obtained from a Device Under Test (DUT). If no BoM is present, then images of golden samples can also be used directly for matching or the images can be sent through our AutoBom framework to generate a BoM first and then used for matching.
(2) **End User Scenario—Absence of Golden Sample Information:** When there is no golden sample present, the end users can only use the DUT PCB to perform authentication. The DUT is sent through the three steps of our AutoBom framework and the details obtained are formatted into a BoM or a CAD. This can be stored and sent to an SME for analysis or to the OEM company for cross-verification.

The presented AutoBOM framework can be used by various parties, regardless of their access to golden sample information. OEMs and end users must both make use of multi-modal imaging and complementary image analysis techniques to assess the PCB authenticity.

6 AUTOBOM EXAMPLES

As discussed in the above section, the performance of automated visual inspection is affected by various factors such as imaging modality and the image analysis methods used. In this section, we present two initial examples of AutoBoM for PCB component detection using conventional image analysis methods and a deep learning method, as shown in Figure 9.

In the following examples, the PCB is imaged with a Leica DMV 6 digital optical microscope. Since the components vary in height, the microscope is focused on the smallest components, e.g., capacitors or resistors.

Conventional method: As shown in Figure 9(a), the focus of this example is to detect resistors, capacitors, solders, and ICs. The first step of the conventional method involves removal of unwanted noise using background subtraction. In this example, we used color thresholding to remove green pixels, thus subtracting the PCB board and traces. The subtracted mask is presented in Figure 9(b). Next, morphological operations are used to smooth the contours and further remove redundant information. The foreground mask is then used to extract the areas of interest (AOIs) containing components, shown in Figure 9(c). Then, salient features can be extracted from these AOIs to classify and authenticate the components, Figures 9(d) and 9(e). In this example, color and shape features are used as by Wu et al. [2010] and Youn et al. [2014].

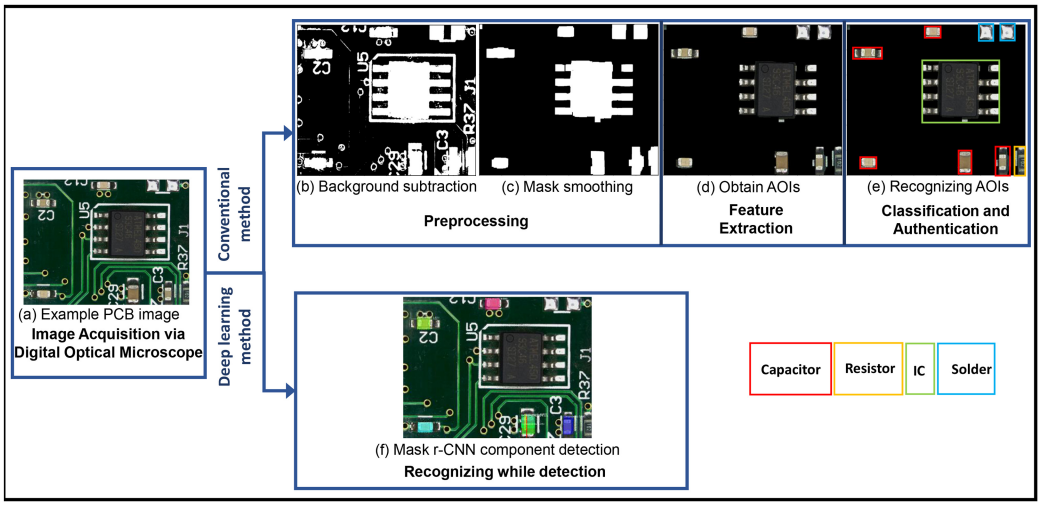

Fig. 9. AutoBoM examples using conventional method and deep learning-based method.

Deep Learning method: Another example for AutoBoM involves a Mask r-CNN (mask region-based convolutional neural network)—readers are referred to He et al.'s work for the detailed network structure [He et al. 2017]. In our preliminary experiments, transfer learning is applied during the training phase due to data availability. Compared to the conventional method, mask r-CNN is an "end-to-end" training process. The network, itself, first learns the most salient features of the components from human-labeled regions in the training images. The mask r-CNN then uses those features to automatically detect and classify components in unlabeled test images, shown in Figure 9(f) as colored regions. Note, for this image, only the capacitors were found, where the locations are designated by different colored regions. The discussed network does not detect ICs, solders, or resistors, because there was a lack of labeled training data. Though deep learning is ideal for automating AutoBoM process, e.g., it does not require selection of preprocessing or feature extraction algorithms, it requires a substantial training dataset that accurately simulates real-inspection scenarios.

Preliminary AutoBoM results are promising in controlled environments but there is significant performance degradation in real-inspection scenarios. For instance, there are a number of factors encountered in the field that significantly affect accuracy, such as board color, board texture/material, lighting conditions, and density of components. Hence, much work is needed to produce a more robust method. For instance, at the industrial scale where five million PCBs may be created for military air crafts, a 1% accuracy degradation means 50,000 more air crafts fail in the field—a catastrophic consequence. Hence, it is crucial for an AutoBoM method to consistently output an accuracy as close to 100% as possible.

7 FUTURE RESEARCH DIRECTION

Malicious implants, such as the one described in the Big Hack report, are difficult to detect and can be used to gain covert access to critical systems in which the infected PCBs are deployed. Therefore, assurance is vital for ensuring the integrity of the global electronics supply chain [Bhunia and Tehranipoor 2018; Rahman et al. 2019]. Given the shortcomings and challenges with the existing assurance techniques, below we briefly describe the future research direction necessary to effectively detect and prevent malicious implants in PCBs.

7.1 Detection

As stated earlier, there are numerous vulnerabilities in the PCB supply chain and a myriad of detection methods used in an ad hoc fashion. Such vulnerabilities can grant malicious entities backdoor access to proprietary details, confidential information, and control over critical infrastructures. Techniques such as ICT, bare-board testing, and functional testing, and so on, are currently used in industry to assure the quality and reliability of PCBs but not necessarily their trustworthiness and security. With the advancement in design and assembly technologies as well as the increased complexity of the global electronics supply chain, malicious alterations would be less likely to be detected using traditional post-production validation methods. To ensure high confidence in detecting stealthy malicious implants, the following research and development efforts are needed by the community.

Comprehensive taxonomy of malicious implants: Currently there lacks a comprehensive taxonomy of potential malicious implants that could be injected into PCBs. The implants can manifest on PCBs as added components, alterations to existing components, thinned traces, and so on. These alterations could cause information leakage, system hijacking, denial of service, and so on. A detailed taxonomy can help drive the development of tools and methodologies to effectively identify such malicious implants. Further, benchmarks can be developed for each possible vulnerability. These benchmarks will allow the research community and practitioners to evaluate their techniques and share their findings. Such efforts can pave the way to develop metrics to evaluate effectiveness of the detection techniques against each vulnerability.

Database of PCBs and implants: Another important challenge to address is the lack of available test PCBs and implants. There is a great need for a number of test PCBs of different sizes, level of complexity, number of layers, population of parts, and so on. Additionally, the community needs test PCBs featuring a variety of Trojans and implants with varying degrees of detection difficulty (easy, medium, and hard-to-detect). Such test PCBs can be used by researchers and practitioners to evaluate their techniques and to compare with others, thus, establishing a baseline for fair comparison.

Comprehensive detection methods: Ideally, the placement, functionality, and integrity of each component is evaluated at every step to test for any malicious component/trace additions, subtractions, substitutions, or relocations from the original base design when a golden netlist is available. However, when there is no golden netlist, as in commercial off-the-shelf components (COTS), such detailed analysis may not be possible. It is extremely challenging to examine the rationale behind the presence of each component/trace on the PCB when only specs are available. One tamper detection technique is presented by Immler et al. [2019]. Here, Immler et al. developed a battery-less cover that is tamper-resistant and it encompass multiple chips on a PCB. The integrity of the PCBs after power-up is verified by this cover and it also protects the chips during run-time. While Immler et al.'s method is promising, there are several improvements that could be made for more robust security, as stated by the authors. Some of those alterations include: different choice of materials for the cover, and use of updated manufacturing, design, and assembly technologies.

Appropriate selection of PCB assurance methods is crucial. For example, automated visual inspection, which incorporates pin-to-pin knowledge of PCBs, can enable real-time testing on assembly lines. This would replace human oversight and, thus, prevent unauthorized physical PCB alteration during assembly. Such fully automated processes could reduce production costs in the long run and improve consistent production quality. One critical liming factor of using imaging capabilities for PCB assurance in the supply chain is the lack of portability of the imaging systems. Such systems are usually large and bulky. There is need for innovative solutions that are

inexpensive, portable, and easy to use. Ideally, an engineer using such a system should only need to take appropriate images and connect to cloud for remote image processing to establish assurance at any point in the transition between different entities in the supply chain.

In this article, we presented a framework for a non-destructive, fast, automated PCB assurance system that can meet the security community's needs. The proposed technique heavily depends on the image acquisition, image analysis, machine learning, and authentication stages. During the image acquisition phase, it is vital to carefully choose which modality should be used and how images are collected, since various modalities collect different types of information. A comprehensive assurance method should incorporate a multi-modal approach to reveal malicious implants that lie between layers as well as any active components that are masquerading as passive ones. In the image analysis phase, algorithms that extract information from the acquired images must be chosen based on the imaging modality selection. Such automated inspections could potentially be used to check every layer of every board, both visually and functionally, before inserting a PCB in an electronic system. Though some modalities such as X-ray can be cost prohibitive and complex for an end user, companies are moving toward developing portable and easy-to-use-tools. In addition, other modalities such as Terahertz computed tomography has shown potential as an alternative to X-ray for extracting the internal structure of PCBs. Such advancements require the community to develop algorithms for the new modalities. These algorithms should incorporate prior knowledge such as physical or functional information in the imaging mode to reduce the imaging time and, more importantly, the size of the data, which can be easily in the range of hundreds of GB for only one sample.

7.2 Prevention

While it is vital to develop methods to detect malicious implants in PCBs at different points in the supply chain, such methods usually lack high confidence in detection, because PCBs are not designed with easy detection in mind. Thus, applying design-for-trust strategies as preventive techniques is imperative. Such techniques are needed to reduce the overall cost of detection and resources needed to respond to a detected malicious attack by preventing the attack from occurring in the first place. They should address the inherent vulnerabilities of the PCBs to malicious alteration. We believe preventative techniques should be classified into three major categories: (1) material-based, (2) layer-based, and (3) circuit-based.

Material-based: Material-based methods can involve a variety of physical/chemical shields to protect the boards. For example, glass epoxy resins can be incorporated within PCB layers during fabrication to conceal the internal circuitry from X-ray imaging [Shen et al. 2018]. Such methods against X-ray imaging make it difficult for an adversary to gain internal circuitry knowledge of the board, which, in turn, makes it difficult for them to insert malicious implants.

Layer-based: Layer-based approaches are widely used for integrated circuits (ICs) [Gilberg et al. 1990], and a similar concept can be extended to the PCB level. In PCBs, designers can shuffle critical traces on different layers. This obscures the circuit by strategically concealing the most critical components deep within the layers [Guo et al. 2015]. This could protect the PCB from non-destructive surface reverse engineering techniques. Replacing a resistor or capacitor on the target BUS/interconnect has proven to be sufficient to implant a malicious chip [Greenberg, Andy 2018]. Therefore, adding dummy interconnects/layers and obfuscating traces/vias, can prevent direct access to BUS or interconnects to some extent. However, these approaches are not provably secure and, thus, cannot protect PCBs against destructive reverse engineering methods. Innovative techniques are needed to effectively obfuscate traces and circuit functionality. One could use

a reconfigurable fabric on PCB and move much of the functionality and trace connection between the layers into an FPGA so the function becomes hidden from the attacker. In Guo et al. [2015], the authors have proposed a key-based PCB interconnect obfuscation technique to hide the connectivity between the board's ICs. We believe further research is needed by the community to combine layer-based approaches with other methods (material-based and circuit-based) to effectively protect PCBs from all types of malicious implant insertion.

Circuit-based: Such approach against malicious implants may involve both prevention and detection-based approaches. In a preventive approach, a designer can add non-functional circuit elements, e.g., resistance, capacitance, vias, and so on, in the design. Additionally, as stated above, one can insert an FPGA to hide circuit functionality and connectivity. The advantage of adding dummy circuits is that they increase the structural reverse engineering overhead. Encrypting the communication protocols also protect the signals from the implants inserted by an adversary [Guo et al. 2019]. Further, a design house can also do functional analysis of the chip to identify the delay variation and compare the delay signature with a "golden sample." The challenge of using a golden sample is that the sample must be verified as free from all malicious modification and, thus, may not be available. Such verification can be completed through non-destructive reverse engineering.

We also believe the community should perform further research on developing countermeasures against malicious implants in PCBs that are capable of preventing probing, and tampering of the PCBs. Such countermeasures should ideally destroy all important information when the attacked PCB is turned on, halt all functions, and alert the system owner/designer. To aid in PCB implant detection and prevention, the community also needs to establish and follow strict requirements for the design and manufacturing processes. Requirements should include, but are not limited to, concealing critical traces and using hidden vias to obfuscate the circuit, establishing strict design rules, and so on. There are best practices and automated CAD tools available for designing state-of-the-art PCBs. The development of tools to automatically localize such design rule violations in a PCB under test can help engineers verify whether violation is done maliciously. In general, most preventative tamper detection techniques do not prevent malicious modification before the techniques are implemented. However, post hoc tamper detection techniques such as AutoBoM could help. AutoBoM could be very effective in detecting malicious change regardless of when the change is made. Since AutoBoM does not require the system to be powered on, such detection can occur at any point in time in the supply chain and life cycle. All in all, it is of utmost importance that the community coordinates stricter guidelines for evaluating outsourced materials and components and enforce, best design practices, and novel preventative techniques.

8 CONCLUSION

This article highlights the presence of vulnerabilities in PCB supply chain to attacks such as malicious implants. An adversary can potentially exploit these vulnerabilities to initiate a nationwide attack. PCB assurance is a growing field, with emphasis on the development of automated assurance methods. Therefore, PCB visual inspection methods, which have high potential for automation, could be considered the first line of defense against threats electronics supply chain. Further, our article laid the foundation for a PCB assurance framework that automatically extracts a Bill of Materials using image processing, computer vision, and machine learning. This method could offer several benefits, such as high accuracy and speed.

REFERENCES

Adam Cort. 2002. *Functional Testing of PCBs.* Technical Report. Retrieved from https://www.bloomberg.com/quote/SMCI:US.

Akin Aksu. 1976. Printed circuit board testing means. U.S. Patent 3,970,934.

Ian S. Anderson, Robert L. McGreevy, and Hassina Z. Bilheux. 2009. Neutron imaging and applications. *Springer Sci. Bus.Media LLC* 2209 (2009), 987–0.

Navid Asadizanjani, Sina Shahbazmohamadi, Mark Tehranipoor, and Domenic Forte. 2015. Non-destructive PCB reverse engineering using X-ray micro computed tomography. In *Proceedings of the 41st International Symposium for Testing and Failure Analysis (ASM'15)*. 1–5.

AWS Elemental. 2006. *Fast and Cost Efficient Easy to Scale*. Technical Report. Retrieved from https://www.elemental.com/.

Swarup Bhunia and Mark Tehranipoor. 2018. *Hardware Security: A Hands-on Learning Approach*. Morgan Kaufmann.

Allen Buckroyd. 2015. *In-Circuit Testing*. Butterworth-Heinemann.

Cal Houdek. 2016. *Inspection and Testing Methods for PCBs: An Overview*. Technical Report. Retrieved from https://caltronicsdesign.com/wp-content/uploads/2016/11/Inspection-and-testing-methods-for-PCBs-an-overview.pdf.

Chintan Panchal and Parth Rao. 2014. *Boundary Scan: Seven Benefits*. Technical Report. Retrieved from https://www.edn.com/electronics-blogs/day-in-the-life-of-a-chip-designer/4430199/Boundary-scan--Seven-benefits.

CISA. 2019. *Supermicro Releases Security Updates*. Technical Report. Retrieved from https://www.us-cert.gov/ncas/current-activity/2019/09/04/supermicro-releases-security-updates.

Fortune. 2016. 100-fastest-growing-companies. Fortune Magazines. Retrieved from http://fortune.com/100-fastest-growing-companies/2016/list.

Jason Geng. 2011. Structured-light 3D surface imaging: A tutorial. *Advances in Optics and Photonics* 3, 2 (2011), 128–160.

Robert C. Gilberg, Richard M. Knowles, Paul Moroney, and William A. Shumate. 1990. Secure integrated circuit chip with conductive shield. U.S. Patent 4,933,898.

Andy Greenberg. 2018. *Planting Tiny Spy Chips in Hardware Can Cost as Little as $200 A New Proof-of-concept Hardware Implant Shows How Easy it May be to Hide Malicious Chips Inside IT Equipment*. Technical Report. https://www.wired.com/story/plant-spy-chips-hardware-supermicro-cheap-proof-of-concept/.

J. Grzyb, K. Statnikov, R. Al Hadi, and U. R. Pfeiffer. 2014. All-silicon integrated THz harmonic source and receiver components for future active imaging modalities. In *Proceedings of the 39th International Conference on Infrared, Millimeter, and Terahertz waves (IRMMW-THz'14)*. IEEE, 1–2.

Ujjwal Guin, Ke Huang, Daniel DiMase, John M. Carulli, Mohammad Tehranipoor, and Yiorgos Makris. 2014. Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain. *Proc. IEEE* 102, 8 (2014), 1207–1228.

P. Günther, U. Ch Fischer, and K. Dransfeld. 1989. Scanning near-field acoustic microscopy. *Appl. Phys. B* 48, 1 (1989), 89–92.

Zimu Guo, Mark Tehranipoor, Domenic Forte, and Jia Di. 2015. Investigation of obfuscation-based anti-reverse engineering for printed circuit boards. In *Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference (DAC'15)*. IEEE, 1–6.

Zimu Guo, Xiaolin Xu, Mark M. Tehranipoor, and Domenic Forte. 2019. EOP: An encryption-obfuscation solution for protecting PCBs against tampering and reverse engineering. *Arxiv Preprint Arxiv:1904.09516*.

Aditya Gupta. 2019. JTAG debugging and exploitation. In *The IoT Hacker's Handbook*. Springer, 109–138.

Abu Hassan, Janusz Rajski, and Vinod K. Agarwal. 1988. Testing and diagnosis of interconnects using boundary scan architecture. In *International Test Conference 1988 Proceeding@ m_New Frontiers in Testing*. IEEE, 126–137.

Kaiming He, Georgia Gkioxari, Piotr Dollár, and Ross Girshick. 2017. Mask r-cnn. In *Proceedings of the IEEE International Conference on Computer Vision*. 2961–2969.

G. Hroundas. 1986. Economics of bare printed circuit board testing. *Circuit World* (1986).

Binbin B. Hu and Martin C. Nuss. 1995. Imaging with terahertz waves. *Optics Lett.* 20, 16 (1995), 1716–1718.

Vincent Immler, Johannes Obermaier, Kuan Kuan Ng, Fei Xiang Ke, JinYu Lee, Yak Peng Lim, Wei Koon Oh, Keng Hoong Wee, and Georg Sigl. 2019. Secure physical enclosures from covers with tamper-resistance. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2019, 1 (2019), 51–96.

Jack Laidlaw. 2017. *Counterfeit Hardware May Lead to Malware and Failure*. Technical Report. Retrieved from https://hackaday.com/tag/clones/.

Patrick Johnston. 1996. Printed circuit board design guidelines for ball grid array packages. *J. Surface Mount Technol.* 9 (1996), 12–18.

JTAGTest. [n.d.]. JTAGTest: Affordable JTAG testing and development solution. Retrieved from http://www.jtagtest.com.

Ramesh Karri, Jeyavijayan Rajendran, Kurt Rosenfeld, and Mohammad Tehranipoor. 2010. Trustworthy hardware: Identifying and classifying hardware trojans. *Computer* 43, 10 (2010), 39–46.

R. A. Lemons and C. F. Quate. 1974. Acoustic microscope-scanning version. *Appl. Phys. Lett.* 24, 4 (1974), 163–165.

J. Michael Lloyd. 2013. *Thermal Imaging Systems*. Springer Science & Business Media.

Matric. 2019. *ICT Testing: Cost, Advantages, & Drawbacks*. Technical Report. Retrieved from https://blog.matric.com/ict-testing-cost-advantages-drawbacks.

Millennium Circuits Limited. 2019. *PCB Testing Methods Guide*. Technical Report. Retrieved from https://www.mclpcb.com/pcb-testing-methods-guide/.

Madhav Moganti, Fikret Ercal, Cihan H. Dagli, and Shou Tsunekawa. 1996. Automatic PCB inspection algorithms: A survey. *Comput. Vision Image Understand.* 63, 2 (1996), 287–313.

Shunji Mori, Hirobumi Nishida, and Hiromitsu Yamada. 1999. *Optical Character Recognition*. John Wiley & Sons, Inc.

Neutron Optics Grenoble. [n.d.]. Inexpensive X-ray and neutron CCD cameras. Real-time 2D-imaging of samples in-beam. Retrieved from https://www.neutronoptics.com/order.html.

Hyo Seon Park, H. M. Lee, Hojjat Adeli, and I. Lee. 2007. A new approach for health monitoring of structures: Terrestrial laser scanning. *Comput.-Aided Civil Infrastruct. Eng.* 22, 1 (2007), 19–30.

David John Pedder. 1998. Structure for testing bare integrated circuit devices. U.S. Patent 5,764,070.

Tao Peng. 2007. *Algorithms and Models for 3-D Shape Measurement Using Digital Fringe Projections*. Ph.D. Dissertation.

Shahed E. Quadir, Junlin Chen, Domenic Forte, Navid Asadizanjani, Sina Shahbazmohamadi, Lei Wang, John Chandy, and Mark Tehranipoor. 2016. A survey on chip to system reverse engineering. *ACM J. Emerg. Technol. Comput. Syst.* 13, 1 (2016), 6.

M. Tanjidur Rahman, M. Sazadur Rahman, Huanyu Wang, Shahin Tajik, Waleed Khalil, Farimah Farahmandi, Domenic Forte, Navid Asadizanjani, and Mark Tehranipoor. 2019. Defense-in-depth: A recipe for logic locking to prevail. *Arxiv Preprint Arxiv:1907.08863*.

Keith Rebello. 2019. Suuply chain vulnerabilities. FICS Research Annual Conference on Cybersecurity. Retrieved from https://fics.institute.ufl.edu/conference/.

CMPPC Rocchini, Paulo Cignoni, Claudio Montani, Paolo Pingi, and Roberto Scopigno. 2001. A low cost 3D scanner based on structured light. In *Computer Graphics Forum*, Vol. 20. Wiley Online Library, 299–308.

Rosenfeld. 2012. Security and testing. In *Introduction to Hardware Security and Trust*. Springer, 385–409.

Kurt Rosenfeld and Ramesh Karri. 2010. Attacks and defenses for JTAG. *IEEE Design Test Comput.* 27, 1 (2010), 36–47.

Shahrooz Shahparnia and Omar M Ramahi. 2004. Electromagnetic interference (EMI) reduction from printed circuit boards (PCB) using electromagnetic bandgap structures. *IEEE Trans. Electromagn. Compat.* 46, 4 (2004), 580–587.

Haoting Shen, M. Tanjidur Rahman, Navid Asadizanjani, Mark Tehranipoor, and Swarup Bhunia. 2018. Coating-based PCB Protection against tampering, snooping, EM attack, and X-ray reverse engineering. In *Proceedings from the 44th International Symposium for Testing and Failure Analysis (ISTFA'18)*. ASM International, 290.

Kenneth R. Smith. 1995. Singulated bare die tester and method of performing forced temperature electrical tests and burn-in. U.S. Patent 5,475,317.

Ray Smith. 2007. An overview of the tesseract OCR engine. In *Proceedings of the 9th International Conference on Document Analysis and Recognition (ICDAR'07)*, Vol. 2. IEEE, 629–633.

Rainer Stark, Hendrik Grosser, Boris Beckmann-Dobrev, Simon Kind, INPIKO Collaboration et al. 2014. Advanced technologies in life cycle engineering. *Procedia CIRP* 22 (2014), 3–14.

Weiqiang Sun, Yong Yang, Zhe Wu, Tao Feng, Qianwei Zhuang, Lian-Mao Peng, Shengyong Xu, and Chong Kim Ong. 2014. Penetrative imaging of sub-surface microstructures with a near-field microwave microscope. *J. Appl. Phys.* 116, 4 (2014), 044904.

Supermicro. 1993. Super micro computer inc. Retrieved from https://www.supermicro.com/en/about.

Mohammad Tehranipoor and Farinaz Koushanfar. 2010. A survey of hardware trojan taxonomy and detection. *IEEE Design Test Comput.* 27, 1 (2010), 10–25.

Mohammad Tehranipoor and Cliff Wang. 2011. *Introduction to Hardware Security and Trust*. Springer Science & Business Media.

M. M. Tehranipoor, U. Guin, and S. Bhunia. 2017. Invasion of the hardware snatchers. *IEEE Spectrum* 54, 5 (May 2017), 36–41. DOI: https://doi.org/10.1109/MSPEC.2017.7906898

Mark Mohammad Tehranipoor, Ujjwal Guin, and Domenic Forte. 2015. Counterfeit integrated circuits. In *Counterfeit Integrated Circuits*. Springer, 15–36.

TerahertzStore. [n.d.]. Retrieved from https://www.terahertzstore.com/products/terahertz-cameras/terahertz-camera-for-thz-imaging-cea-leti-tzcam.htm.

The Bloomberg Businessweek. 2018. *The Big Hack*. Technical Report. Retrieved from https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

The FBI. 2014. *Florida Man Charged in Federal Counterfeit Case for Trafficking Bogus Automotive Devices "Reverse Engineered" in China*. Technical Report. Retrieved from https://archives.fbi.gov/archives/losangeles/press-releases/2014/florida-man-charged-in-federal-counterfeit-case-for-trafficking-bogus-automotive-devices-reverse-engineered-in-china.

Jonathan Vanian. 2018. Stock in server company super micro cratered after report alleging chinese hacking. Retrieved from http://fortune.com/2018/10/04/super-micro-shares-hacking/.

Amit Verma. 2002. Optimizing test strategies during PCB design for boards with limited ICT access. In *Proceedings of the 27th Annual IEEE/SEMI International Electronics Manufacturing Technology Symposium*. IEEE, 364–371.

Michael Vollmer and Klaus-Peter Möllmann. 2017. *Infrared Thermal Imaging: Fundamentals, Research and Applications*. John Wiley & Sons.

Huihui Wu, Guanglin Feng, Huiwen Li, and Xianrong Zeng. 2010. Automated visual inspection of surface mounted chip components. In *Proceedings of the IEEE International Conference on Mechatronics and Automation*. 1789–1794.

James C. Wyant. 2002. White light interferometry. In *Holography: A Tribute to Yuri Denisyuk and Emmett Leith*, Vol. 4737. International Society for Optics and Photonics, 98–107.

Seung Geun Youn, Youn Ae Lee, and Tae Hyung Park. 2014. Automatic classification of SMD packages using neural network. In *Proceedings of the IEEE/SICE International Symposium on System Integration*. 790–795.

Received October 2019; revised March 2020; accepted May 2020