CHASE Survey of Technology Needs

Shahed Enamul Quadir
ECE Department
University of Connecticut
Storrs, CT, USA

Daniel DiMase
Honeywell, Inc.
Smithfield, RI, USA

John Chandy
ECE Department
University of Connecticut
Storrs, CT, USA

Abstract: *This paper presents a summary of industrial consensus on future technology needs in the area of security of integrated circuits and electronic assemblies and supply chain risk management based on a survey conducted in late 2015. Counterfeits and Hardware Trojans have been identified as areas needing continued research and focus. Also, this study shows that embedded systems security and cyber physical systems security is an emerging area of interest and importance.*

Keywords: hardware security; counterfeits; hardware Trojans; reverse engineering; embedded systems; cyber physical systems security.

1. Introduction

Over the course of two months in late 2015, the Center for Hardware Assurance, Security and Engineering (CHASE) at the University of Connecticut conducted a survey of its advisory board and industry professionals to determine the technology needs in the area of IC counterfeits, hardware assurance, cyber physical systems security, and embedded systems security. We received responses from 20 invitees. The survey was focused on six major areas: Counterfeit Electronics; Hardware Security; Reliability; Secure Computing; Embedded Systems Security and Infrastructure Security. The survey asked responders to rate several technology topics on a scale from 1 to 5 where 1 meant "Not Important" and 5 meant "Very Important" as an area deserving research investments in the near future. The average rating across all areas was 3.79 with a standard deviation of 0.29. Below, we will give a short description of those areas that had average rating > 4.10 - i.e., those rated as important areas and therefore, more research efforts should be carried out those areas.

2. Counterfeit Electronic Components and Supply Chain

2.1 Emerging Technologies Used by Counterfeiters

Counterfeits ICs broadly fall into seven types: recycled, remarked, overproduced, out-of-spec, cloned, forged documentation, and tampered. Recycled and remarked types are the most widely discussed counterfeit types [1]. Currently, counterfeiters are able to utilize sophisticated and well financed tools and technologies for recycling. ICs and other components are taken off from PCB boards under very high temperatures. Then the components are subject to cleaning, sanding, remarking, repacking and sold on the market as new. Also, new parts of a commercial grade could be remarked to upgrade as industrial or defense grade. Counterfeiters have developed both simple and specialized techniques, tools and equipment for counterfeiting including: sandpaper, fiberglass scratch brush, laser, milling machine, dry and wet etch chemicals, optical high/super resolution microscopy (Digital), X-ray machines, scanning electron microscope (SEM), transmission electron microscopes (TEM), scanning capacitance microscopy (SCM) and focused ion beam (FIB) [2]. The equipment is used by the more sophisticated counterfeiter performing reverse engineering and circuit edits to produce clones or tampered counterfeit parts. As researchers develop technologies to mitigate counterfeiters, they will continue to innovate new techniques to evade those countermeasures. Continued work in keeping up-to-date with the latest counterfeit technologies is paramount to developing effective anti-counterfeit strategies.

2.2 Development of Low-cost Counterfeit Detection Techniques (Electrical Test, Visual Inspection, Margin Test, etc.

Counterfeit detection tests broadly fall into two categories: physical/mechanical and electrical performance based tests. Using physical and electrical test methods, significant numbers of counterfeit ICs can be detected [1]. For example, low power visual physical inspection can be used to examine the exterior part of the component and flag many signs of counterfeits. The SAE G19 Counterfeit Electronic Parts Committee has explored a number of test methods ranging from very simple and low-cost to those that take significant amounts of time and money. G19 has newly identified tampering as a counterfeit type of interest and additional new tests are needed to detect tampering effectively. Particularly, low-cost solutions that can detect multiple defect types are especially needed. As counterfeiters start using more advanced mechanisms that are not easily detected by physical and electrical test methods, new detection techniques are needed – specifically, those that are designed for security and low-cost. For example, new optical photon-counting security tagging and verification of integrated circuits (IC) using optically encoded QR codes [3] might present such a low-cost mechanism.

2.3 Counterfeit Detection Technology Assessment (Quantitative Metrics, Historical Test Data, Tools and Methodologies)

A set of tests is performed to detect a counterfeit component which is known as counterfeit defect coverage (CDC) [1]. Test, cost, and risks associated with counterfeiting and the application risks are considered as constraints and to find the optimum set of detection methods, an algorithm is used which could maximize CDC from a risk-based perspective. Test time and cost are more important metrics for low and very low risk applications instead of maximizing CDC. However, a higher confidence level could be obtained for medium- and high-risk applications by adjusting a higher test time and cost limit to get maximum CDC. The CDC methodology has been incorporated into the forthcoming SAE AS6171 Standard on Suspect/Counterfeit Electronic Parts Test Methods. As new test methods are developed and more counterfeit data is accumulated, the various metrics and assessment tools will need to be updated and refined. In addition to the CDC, the counterfeit type coverage (CTC) is an important metric that assesses the likelihood of covering a particular counterfeit type with a set of tests [6]. Current methods use a simple weighting factor, but a more methodical approach to identify type coverage is needed. Frequency based methods that take into account statistical coverage across a random population and use more fine-grained scales can be used to drive the CTC metric. Better tools are needed to understand CTC beyond a simple weighting factor so that it is a more accurate predictor of the likelihood that a defect would be present.

3. Hardware Security and Trust

3.1 Hardware Trojan Detection and Prevention

A hardware Trojan can be designed as a time bomb to disable and/or destroy a system at some future time. Hardware Trojans can be inserted at any stage of the design flow by an adversarial third party to tamper the original design [4]. It is important to establish a root of trust from design house to supply chain. To distinguish malicious alterations in the design, authors in [5] have used power as the side-channel signal. To make the Trojan(s) more observable on outputs, [6] proposed voltage switching on supply rails to alter the circuit logic. Additional gate delay could be introduced by Trojan(s) which is exploited in [7] and it will alter the delay signature of the path where it occupies. In pre-silicon stage, a four-step approach is proposed to filter and locate malicious insertion(s) implanted in a third party Intellectual Property [4]. Furthermore, Trojan prevention approach could be used to make it more difficult (ideally impossible) to insert hardware Trojans at the fab. The authors in [8] proposed a technique called built-in self-authentication (BISA). This technique could be used to fill unused spaces in a circuit layout with functional standard cells instead of non-functional filler cells during layout design. Therefore, BISA could prevent hardware Trojan insertion in limited available spaces.

In spite of the amount of work that has been done on hardware Trojan detection and prevention, by no means is this a solved problem. While existing techniques can detect certain types of Trojans in limited configurations or layouts, it is still quite easy for adversaries to insert Trojans at almost any stage of the IC design and fabrication process. Further work is still needed to address this serious vulnerability in current and future integrated circuits.

3.2 Run-time Security Analysis, Authentication, & Verification

While technologies to make systems and devices less vulnerable to attack are important, it is also critical to detect attacks (both known and unknown) in run-time. These include run-time detection of tampering, counterfeits, Trojans, side-channels, probing, and other attack vectors. In order to prevent tampering, obfuscation techniques are used to make a design or system more complicated. Several different obfuscation approaches are discussed in the literature [9] [10]. The HARPOON (HARdware Protection through Obfuscation Of Netlist) method could be used against piracy and tampering [10]. To control post-fabrication of the ICs that are produced in outsourced plants, IC hardware metering protocols have been put in place to prevent IC piracy [11]. In addition to vulnerability detection, efficient run-time techniques are needed for authentication of devices and systems. Physical unclonable functions (PUFs) have been developed as an enabler for key generation, authentication, and verification. However, many PUFs do not exhibit the expected reliability necessary for authentication or key generation. Continued work is necessary in this area to develop reliable technologies that can enable more efficient methods for on-line security vulnerability analysis and authentication. Further work is needed to develop reliable and cost-effective authentication and verification methods.

3.3 Reverse Engineering and Anti-reverse Engineering

Reverse engineering (RE) is the process of examining an original object in order to fully understand its nature and functionality [2]. RE could be done for the following reasons: verification, fault analysis, research and development, and education about the workings of an existing product. But, RE could be performed to clone, pirate or counterfeit a design, to develop an attack, or insert a hardware Trojan. If the functionality of a cloned system is close enough to the original, for example, then the counterfeiters could sell large amounts of counterfeit products. As a result of these concerns, researchers, companies, and the defense departments of many nations are persistently seeking anti-RE techniques to prevent adversaries from accessing their protected products and systems. Anti-RE techniques should have the ability to monitor, detect, resist, and react to invasive and noninvasive attacks. Tamper resistant materials and sensors have been used to resist theft or reverse engineering (RE). Also, obfuscation software and hardware security primitives have been used for the protection of systems and software. Some other methods for protecting these systems are as follows: bus encryption, secure key storage, side channel attack protection, and tamper responding technology. As with counterfeiting, anti-reverse engineering technologies are always a step behind reverse engineering techniques and more advanced technologies need to be explored in both RE and anti-RE.

3.4 Circuit Level Vulnerability Analysis against Trojan, Probing, and Side-channel Attacks

IC designs increasingly include third party soft IPs, and it is possible that an adversary could change the netlist to insert Trojans [4]. Also, using a probing station, an adversary could read data within the circuit [12]. Furthermore, probing could be used to extract cryptographic keys to break the IC security. To bypass the theoretical strength of cryptographic algorithms, side channel attacks are used which aim at nonprime, side-channel inputs and outputs [13]. Several powerful side-channel attacks, for example, Simple power analysis (SPA) and Differential power analysis (DPA), are used to break cryptographic implementations. Currently, it is difficult to analyze a circuit or layout and determine its vulnerability to Trojans, probing, or side-channel techniques.

4. Embedded Systems Security

4.1 Secure Systems Verification & Validation - Formal Methods

It is highly desirable to be able to prove the security of a system. To date, such proofs have been difficult to show. Formal method techniques have been used to provide highly secure and reliable guarantees at the operating system and application levels for a secure microkernel (seL4) [XX]. To form a trustworthy embedded system, seL4 could provide the secure software layers (system and application services) for some existing and emerging application domains and devices, for example, smartphones, cyber physical military systems, and medical devices. However, there are questions whether the approaches used for seL4 could scale for ultra complex hardware/software systems. At the hardware level, there are no known formal techniques to establish any level of security guarantee. Tehranipoor and others have begun work on vulnerability analysis of IC designs with the use of a framework called Design Security Rule Check (DSeRC). Further work is needed to develop security guarantees for all levels of a system – from the integrated circuit to an embedded system to the application software and the entire cyber physical system. When considering systems security for a cyber physical system, a holistic approach is needed. A systems engineering approach that includes security considerations of electronic parts and assemblies and their corresponding software, firmware and hardware is needed. The approach should consider all areas of concern to enable resiliency for more robust systems capable of surviving and recovering from attacks. Unintended vulnerabilities can be introduced with the integration of complex hardware, software, and firmware supporting the cyber physical system. DiMase et al. note that standard work with a holistic, systems engineering perspective for cyber physical systems security is needed. This includes the integration of cross-cutting capabilities such as risk assessment and management, decision analysis, employee training and certification, and education and outreach [17].

4.2 Network Layer Security

Securing networks is the biggest challenge in any computing system. These networks form the entry point for any bad actor and thus pose the single most important potential vulnerability for a system. Issues include denial of service attacks, man-in-the-middle attacks, layer 2 flooding, VLAN hopping, ARP poisoning, web application attacks, etc. The magnitude of the probblem is enormous and as old attacks are patched, new forms of attacks appear on a daily basis. Several network-layer security threats have been studied in literature [14] and their aftermaths. Network level security is an active research area as approaches to make networks more robust are developed. However, new approaches are needed particularly in predicting and detecting ne attacks, developing defensive strategies, creating new mitigations, etc.

4.3 Detection and Isolation of Hardware Subversion and Tampering

Several techniques could be used for detection and isolation of hardware tampering and subversion. For example, to resist theft or tampering, tamper resistant materials and sensors have been used [15]. To separate the top layer of the electronic devices, hard barriers like ceramics, steel, and bricks could be used. And tampering attempt might be thwarted by the destruction of the protective devices. Single chip coatings have also been applied to protect against probing attacks. Furthermore, to protect a device, many different packaging techniques could be used, for example, brittle packages, aluminum packages, polished packages, bleeding paint, as well as holographic and other tamper responding tapes and labels [15]. Also, several sensors could be used against tampering, for example, voltage sensors, probe sensors, wire sensors, PCB sensors, motion sensors, radiation sensors, and top layer sensor meshes. To block X-ray imaging attempts, materials like epoxy with potting, coating, and insulating have been used.

4.4 Key Management

To deal with supporting the establishment and maintenance of generation, distribution, installation, storage, use, and recovery of keys between authorized parties, the set of techniques and procedures is defined by key management [16]. A cryptographic system could be symmetric or asymmetric. An asymmetric system uses public and private keys for authentication. Hierarchical digital certificates are used for authentication which is known as public key infrastructure (PKI) system. World wide web traffic used PKIs certification which is in the form of SSL and TLS. Keys are the lifeblood of any information organization and managing them securely is critical. Several challenges remain to be addressed to control and manage encryption keys including simplifying key management and implementing security policy correctly.

5. Conclusions

We have presented the results of a survey that concludes that counterfeit products and hardware Trojan continue to pose a great threat and a lot of research and development need to be done in this area. Addressing counterfeits is still an important issue – particularly identifying new emerging counterfeit threats and technologies. Though Hardware Trojan detection and prevention has been studied for several years, it is clear that more work needs to be done. What is new in this study is the importance of embedded systems security and cyber physical systems security as an emerging area of interest. Particularly, methodologies to verify and validate embedded systems security are sorely lacking. In addition, security analysis and verification for hardware systems was also brought out as an important research need. Another new point of emphasis is the need to bring in risk analysis as part of counterfeit as well as hardware security assessments. We hope the results of the survey can help guide future research to protect state-of-the-art military systems and intellectual property from foreign enemies and counterfeiters.

References

1. U. Guin, D. DiMase, and M. Tehranipoor, “A comprehensive framework for counterfeit defect coverage analysis and detection assessment,” *Journal of Electronic Testing*, vol. 30, no. 1, pp. 25–40, 2014.
2. S. E. Quadir, J. Chen, D. Forte, N. Asadizanjani, S. Shahbazmohamadi, L. Wang, J. Chandy, and M. Tehranipoor, “A survey on chip to system reverse engineering,” *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 13, no. 1, p. 6, 2016.
3. A. Markman, B. Javidi, and M. Tehranipoor, “Photon-counting security tagging and verification using optically encoded qr codes,” *IEEE Photonics Journal*, vol. 6, no. 1, pp. 1–9, 2014.
4. M. Banga and M. S. Hsiao, “Trusted RTL: Trojan detection methodology in pre-silicon designs,” in Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on. IEEE, 2010, pp. 56–59.
5. R. Rad, J. Plusquellic, and M. Tehranipoor, “Sensitivity analysis to hardware Trojans using power supply transient signals,” in *Hardware- Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on*. IEEE, 2008, pp. 3–7.
6. M. Banga and M. Hsiao, “Vitamin: Voltage inversion tech. to ascertain malicious insertions in ICS,” *HOST*, vol. 9, pp. 104–107.
7. J. Li and J. Lach, “At-speed delay characterization for ic authentication and Trojan horse detection,” in *Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on*. IEEE, 2008, pp. 8–14.
8. K. Xiao and M. Tehranipoor, “BISA: Built-in self-authentication for preventing hardware trojan insertion,” in *Hardware-Oriented Security and Trust (HOST)*, 2013 IEEE International Symposium on. IEEE, 2013, pp. 45–50.
9. A. R. Desai, M. S. Hsiao, C. Wang, L. Nazhandali, and S. Hall, “Interlocking obfuscation for anti-tamper hardware,” in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*. ACM, 2013, p. 8.
10. R. S. Chakraborty and S. Bhunia, “Harpoon: An obfuscation-based SoC design methodology for hardware protection,” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 28, no. 10, pp. 1493–1502, 2009.
11. F. Koushanfar, “Integrated circuits metering for piracy protection and digital rights management: An overview,” in *Proceedings of the 21st edition of the great lakes symposium on Great lakes symposium on VLSI*. ACM, 2011, pp. 449–454.
12. J.-M. Cioranesco, J.-L. Danger, T. Graba, S. Guilley, Y. Mathieu, D. Naccache, and X. T. Ngo, “Cryptographically secure shields,” in *Hardware-Oriented Security and Trust (HOST)*, 2014 IEEE International Symposium on. IEEE, 2014, pp. 25–31.
13. M. Tehranipoor and C. Wang, *Introduction to hardware security and trust*. Springer Science & Business Media, 2011.
14. H. Yang, J. Shu, X. Meng, and S. Lu, “Scan: self-organized network layer security in mobile ad hoc networks,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 261–273, 2006.
15. S. H. Weingart "Physical security devices for computer subsystems: A survey of attacks and defenses." *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer Berlin Heidelberg, 2000.
16. T. Lalith, R. Umarani and G. M. Kadharnawaz. "Key Management Techniques for Controlling the Distribution and Update of Cryptographic keys." *International Journal of Advanced Computer Science and Applications-IJACSA* 1.6 (2010): 163-166.
17. DiMase D, Collier ZA, Heffner K, Linkov I (2015) Systems engineering framework for cyber physical security and resilience. Environment Systems & Decisions 35(2):291-300.