Hardware Security Through Chain Assurance

Yaw Obeng[1], Colm Nolan[2], David Brown[3]

[1]Engineering Physics Division, Physical Measurement Laboratory, National Institute of Standards and Technology,
100 Bureau Drive, Gaithersburg, MD 20899

[2]IBM, IBM House, Shelbourne Road, Ballsbridge, Dublin 4, Ireland,

[3]Intel Corporation, 2200 Mission College Blvd., Santa Clara, CA 95052-8119

Email: yaw.obeng@nist.gov Phone:+1-301-975-8093

***Abstract*— This paper examines the current issues pertaining to the hardware security and how they could affect the overall security of applications such as the internet of things. Specifically, we review the ongoing industry-led activities aimed at mitigating the hardware threats through supply chain assurance. The impact of emerging technologies on hardware-based needs, and the need for technical standards are discussed from brand owners' perspectives. The paper is illustrated with the ongoing work of the International Technology Roadmap for Semiconductors (ITRS) Emerging Research Devices (ERD) hardware security working group, the counterfeit risk mitigation efforts from iNEMI, and the High-Density Package User Group (HDPUG), as well as published standards from SEMI and the Open Group. All these efforts are aimed at mitigating counterfeits in the electronics supply chain through product traceability and authentication. Finally, we will discuss how existing and emerging technologies can be used for product authentication throughout the supply chain.**

I. Scope of Hardware Security Issues

Hardware security is a critical design consideration, just like performance, power, and reliability. For example, hardware security threats in the integrated circuit (IC) supply chain, including hardware counterfeiting, IP piracy, and reverse engineering cost the US economy more than $200 billion annually [1]. Due to increased globalization, the whole IC design flow and application phases are distributed world-wide; the resultant reduced/loosened control over the IC life cycle make hardware security a serious concern. Major threats include IP piracy, IC cloning and overproduction, hardware Trojans, and counterfeiting. Hardware vulnerabilities significantly increase the risk of hardware-level attacks – which could in turn invalidate software-centric cybersecurity solutions. The hardware security problems are amplified by the rapid growth in the interconnected sensors in "More-Than-Moore" (MTM) applications. Thus, there is a need to empower brand owners, enforcement entities, and the public to authenticate products through a supply chain authentication system that integrates multiple sources of information – e.g., various brand owners, governments, etc. Such a system would provide more cohesive and effective countermeasures against malicious products in the supply chain. This requires anti-counterfeit solutions based on standards that can be easily implemented across the supply chain.

In this paper, we review the ongoing industry-led activities aimed at mitigating the hardware threats. The semiconductor industry anticipates that implementing security at the hardware-level would be an efficient path forward for rapidly and unambiguously distinguishing between legitimate and counterfeit products at every supply chain stage. How emerging technologies could impact hardware-based needs, and the need for standards are discussed. The paper is illustrated with the ongoing work of the International Technology Roadmap for Semiconductors (ITRS) Emerging Research Devices (ERD) hardware security working group, the counterfeit risk reduction efforts from iNEMI, the counterfeit protection strategies from the High-Density Package User Group (HDPUG), as well as published standards from SEMI and the Open Group, all aimed at mitigating counterfeits in the electronics supply chain.

MTM applications have their origin in the convergence of wireless technologies, advancements of microelectromechanical systems (MEMS) and digital electronics [2]. Such application platforms will comprise many small, inexpensive single-function devices and sensors, with varying operating systems, CPU types, memory, etc. How these devices connect to other devices, and the device-human interfaces, are changing how we work and live. There is a flood of appliances which could be connected to the internet. However, unsecured smart devices could negate the convenience of the interconnectivity; as the number of intelligent devices rises, the potential damage that could be caused by lack of security will continue to increase. Because of the interconnection between these devices a hack of a smart-connected appliance could be dangerous and a lot more threatening than a simple PC hack. Thus, security must be the foundational enabler for the MTM platforms, without which the ever expanding platform base could create vulnerabilities across all interconnected systems. Even one small security gap could create massive ripple effects with unimaginable grave consequences. Hardware security is a critical component of the security envelope. Table 1 lists some potential hardware-level security primitives for interconnected device platforms and their categorization into levels of hardware security issues. Generally speaking, implementing security at the hardware level generally tends to be very efficient, e.g., physically unclonable functions (PUFs) can enable higher security level function [3].

978-3-9815370-6-2/DATE16/ ©2016 EDAA

There are non-hardware security issues, such as software applications and operating systems tempering, license manipulation and theft, and network and systems level issues such as denial of service, port scans worms and exploits, etc., which are beyond the scope of this paper. However, common to the two sets of issues are those pertaining to security and privacy concerns. All the on-going hardware security efforts rely on software for the overall security of the sensor networks. This further assumes that the devices that connect to network are uniquely identifiable; for example, each connected device has a genuine and unique MAC addresses, etc. Unfortunately, many counterfeit electronics have spoofed MAC addresses. Thus, the current efforts may not be sufficient, and electronics supply chain must be further secured against hardware and other cyber-physical threats by mitigating counterfeit introduction.

The diffused supply chains due to globalization of the manufacturing process increases the complexity of verifying products and materials or components. Furthermore, the increased sophistication of counterfeiters has made it more difficult to detect counterfeit products and to verify the presence of malicious content in electronic products. What is needed is the ability to empower brand owners, enforcement agents, and the public to reliably authenticate products and components through a supply chain authentication system that integrates multiple sources of information, such as from brand owners, governments, and other authentication service bodies. Such a system would provide more cohesive and effective counter-measures against counterfeits in the supply chain. Any anti-counterfeiting solutions must be implemented and supported throughout the entire manufacturing supply chain. Product authentication protocols should provide a level of security against consumer deception and the legitimacy without imposing additional hazards in terms of security or safety. This requires that the anti-counterfeiting solutions be based upon standards that can be easily implemented across the supply chain. Such solutions must rapidly and unambiguously distinguish between legitimate and counterfeit products at every stage of the supply chain. Thus, research must be conducted to identify potential technical solutions to provide enhanced hardware security features.

TABLE I. Some Potential Hardware-Level Security Primitives for Interconnected Device Platforms

Security/Trust	Reliability	Design	Anti-Tamper
Hardware	IP Use	Crytpo Cores	Materials
Firmware	Materials	Crypto Libraries	IP Use
Software	Manufacturing Process Flow	Wirebox Crypto	Software / Hardware Binding
Design	Design	Confidentiality	Software obfuscation
Fabrication	Power Density	Power use pattern	Traceability
Assembly			Authentication
Test			Unclonable Functions
Configuration			Built-in unique IDS

II. Current Gaps

Detecting counterfeit products, especially ICs, may be extremely difficult if not impossible even if comprehensive functional tests are used. The IC may respond as designed to applied stimulus signals, however, the circuit may have additional malicious functions added for the purposes of intentionally inducing malfunctions or a “back door” for extracting secure information. Also, counterfeit ICs may be manufactured in a marginal fabrication process where the reliability of the product may be severely compromised causing the product to fail unexpectedly. Such a failure would be devastating in critical applications such as medical implants, automotive control systems, military, or aerospace. Thus, testing and measurement techniques will need to be developed and continuously improved for the detection of counterfeit or malicious content as the attacks gain in sophistication. For example, special standardized test vehicles for characterization reliability can be integrated into the unused chip real estate on integrated circuit (IC) products for periodic monitoring and evaluation. The currently available information and measurement techniques tend to have inherent biases leading to potentially skewed information [4]. The International Technology Roadmap for Semiconductors (ITRS 2.0) intends to roadmap hardware security.

Another gap identified in the semiconductor industry supply chain, by the SEMI traceability committee, is a need for a cyber-security management system (Cyber Security Manager (CSM)) that will enable organizations to develop, deploy, and scale secure applications and online services. The CSM will also help manage digital identities, and automate and centralize the management of cryptographic keys and digital certificates. Such a system will enhance security and should be scalable, interoperable and easily deployed and administered.

The lack of a concerted effort towards providing integrated solutions to the identified hardware security issues is another gap that that is being addressed.

III. Examples of Industry-Led Solutions

Some efforts are being made made to coordinate the disparate on-going effort of the different consortia / organizations to address security issues. Specifically, efforts are being made to developed holistic standards that encompass hardware, software and network. For example, the Open Interconnect Consortium (OIC) has sponsored an open source software framework enabling seamless device-to-device connectivity [5]. The consortium aims to facilitate the collaboration of the open source community and industry standards to drive interoperability of devices connected to the internet through a common communication framework based on industry standard technologies to wirelessly connect and intelligently manage the flow of information among devices, regardless of form factor, operating system or service provider.

The High Density Packaging User Group (HDPUG) has evaluated most of the hardware authentication technologies currently available, based on their key features, reasons for use, perceived challenges to implement, best known methods and examples. Each technology has its strengths and weaknesses that depend on the specific risk and ultimately the decision comes down mitigating whichever risks the manufacturer or customer remain concerned about. Whereas the HPUG does not purport to be an exhaustive piece of research of each of these technologies, rather it informs users and will result in better decisions regarding which technologies are best suited to their needs [6].

iNEMI has taken a comprehensive view of the counterfeit components problem by surveying the possible points of entry in the supply chain and assessing the impact of counterfeit components on the industry at various points of use. It developed a set of risk assessment calculators that can be used to quantify the risks of procuring counterfeit parts. The risk calculators are aimed at all segments of the supply chain and can be used by component manufacturers, product designers, distributors, loss estimators, industry groups and end users [7].

SEMI has developed and published a number of technical standards to help deter counterfeiting by validating the integrity of goods at the point of purchase. These standards help trusted manufacturers of authentic goods use strongly-encrypted batch numbers. The SEMI T20 and its associated subsidiary standards describe: (1) the overall system, (2) object labeling, (3) authentication service communication, and (4) authentication service body (ASB) qualifications [8].

Finally, the Open group has created an open standard containing a set of organizational guidelines, requirements, and recommendations for integrators, providers, and component suppliers to enhance the security of the global supply chain and the integrity of electronic products, which if properly adhered to will help assure against maliciously tainted and counterfeit products throughout the product life cycle encompassing the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal [9].

IV. Conclusions

While hardware security is becoming a critical design consideration, just like performance, power, and reliability, etc., privacy cannot be neglected. These critical issues may be tackled by mitigating counterfeit components entering the supply chain, and onto the internet. The good news is that there many, albeit disparate, industry-lead efforts towards securing the supply chain but these efforts must be coordinated and holistic.

Addendum

Official contribution of the National Institute of Standards and Technology; not subject to copyright in the United States.

Certain commercial equipment, instruments, or materials are identified in this report in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

References

[1] Estimating the global economic and social impacts of counterfeiting and piracy", Frontier Economics Ltd, London., February 2011.

[2] Emerging Research Devices and Architectures for More-Than-Moore Applications, Chen, A., ECS Transactions, 50 (14), 3-10, 2012.

[3] "PUFs at a Glance" U. Ruhrmair, D. E. Holcomb, Proceedings of the Design, Automation and Test in Europe Conference and Exhibition (DATE), March 24-28, 2014, Paris, France pp. 1- 6.

[4] The Economic Impact of Counterfeiting and Piracy, OECD Publishing, June 2008.

[5] www. http://openinterconnect.org/

[6] "Evaluation of Product Authentication Technologies: A Detailed Evaluation Of The Current And Emerging Technologies", Obeng, Y. et al, presented at SMTA / CALCE Symposium on Counterfeit Parts and Materials, Technical Symposium and Expo: June 23-24, 2015, College Park, MD.

[7] "Counterfeit Components – Assessment Methodology and Metric Development", Nolan C. et al., presented at IPC APEX Expo, Las Vegas, NV March 25-27, 2014.

[8] "New SEMI Standards to Combat IC Chip Counterfeiting", http://www.semi.org/en/Issues/IntellectualProperty/ssLINK/CTR_032693, accessed November 11th, 2015.

[9] Open Trusted Technology Provider™ Standard (O-TTPS) Assessment Procedures Version 1.1", Document Number: X1316, The Open Group, 8 New England Executive Park, Burlington, MA 01803, April 2015