ECS Transactions, 72 (3) 113-117 (2016)
10.1149/07203.0113ecst ©The Electrochemical Society

Hardware Security to Mitigate Threats to Networked More-Than-Moore Sensors

Yaw Obeng
Engineering Physics Group, Physical Measurement Laboratory, Nation Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899

Author's Contact Information: Email: yaw.obeng@nist.gov Phone: 301-975-8093

Keywords: security ; design ; emerging technology ; hardware security;

Abstract: Networked sensors (a. k. a., Internet of Things (IoT)) represents a new era in the evolution of telecommunications made possible by the reduced cost of performance in electronic devices. This is the era where even the most mundane items are connected to, and communicate with each other, on massive networks. This paper examines the issues pertaining to, and efforts at improving, the hardware security of the interconnected devices. The paper highlights a number of academia and semiconductor industry-led ongoing work on improving hardware security.

The Internet of Things (IoT) represents a new era in the evolution of telecommunications, made possible by the reduced cost of performance in electronic devices. Even the most mundane items are communicating with each other through a network of sensors made possible because of the convergence of wireless technologies, advancements of microelectromechanical systems (MEMS) and digital electronics, i.e. More-than Moore technologies. The net result is an emerging system comprised of many small, inexpensive single-function devices, with varying operating systems, CPU types, memory, etc. How these devices connect to each other, and to humans, are changing how we work and live. Unfortunately, the weaknesses of the underlying networks have been exposed through exploitations of hardware operation weaknesses(1). By and large, unsecured smart devices threaten the convenience of the More-than-Moore technology platforms. Thus, security must be the foundational enabler for such technologies; without ample security measures, the ever expanding sensor network could create massive vulnerabilities. Hardware security is a critical component of the security envelope. Major threats from hardware vulnerabilities could also invalidate software-centric cybersecurity solutions. Implementing security improvements at the hardware level through design changes generally tends to be very efficient than after deployment fixes, and can enable higher level function in some cases.

There have been a number of academia-led efforts to leverage unique current-voltage (I-V) characteristics associated with beyond-CMOS transistors to design novel security primitives into emerging devices. For example, the inherent ambipolarity of some nanoscale devices can be leveraged to deliberately change device characteristics post-deployment(2-4). In symmetric graphene FETs (SymFET)-like devices, it is conceptually possible to create polymorphic

electronics, with multiple functionalities built into the same cell(5-7). Polymorphic gates can conceal the functionality of a digital circuit even if the adversary has access to an entire netlist (8). SymFET-based “protector circuits’’ have been developed to help prevent power supply fault injections(8). In another example, the unique electronic properties of resistive RAMs (and memristors) have been used to perform lightweight user authentication in units that are secure and reliable against environmental variations such as temperature, noise, unbalanced set/reset, filament formation variation and device aging(9). There are other device concepts and primitives, such as those based on negative capacitance FETs, that can lead to improved hardware security(10). In all these examples, new and emerging materials provide the unique properties and phenomena that make these circuits possible.

In addition to device design changes and IP security, manufacturing and supply chain security, and product traceability offer opportunities to improve network security. 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. Since the entire integrated circuit (IC) design flow, manufacturing and application phases are currently distributed world-wide, there is a need to authenticate products against malicious products in the supply chain. The diffused supply chains of the manufacturing process increase the complexity of verifying products and materials authenticity. This requires hardware authentication solutions based on standards that can be easily implemented across the supply chain. It must be implemented and supported throughout the entire manufacturing supply chain, comprising raw material providers, parts suppliers, end-item manufacturers, system integrators, shippers, border crossings, seaports, truck inspection and weigh stations, distributors, maintenance service providers, retailers, and consumers, etc. There are several product authentication technologies in the marketplace, but for these to be useful they should provide a level of security against consumer deception where the legitimacy of the product materials and components ensure it does not impose additional hazards in terms of security or safety.

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 with 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 sophistication.

The following are illustrative examples of industry-lead efforts towards addressing the aforementioned issues. The Open Interconnect Consortium (OIC) sponsored open source software framework enabling seamless device-to-device connectivity. In a different effort, the High Density Packaging User Group (HDPUG) has evaluated most of the hardware authentication technologies currently available, and determined the best known methods and examples for each technology(11). iNEMI has surveyed the possible points of entry of counterfeit components in the supply chain and assessed the impact on the industry at various points of use. They have also developed a set of risk assessment calculators that can be used to quantify the risks of procuring counterfeit parts(12). 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. The SEMI T20 and its associated subsidiary standards describe: the overall system, object labeling, authentication service communication, and authentication service body (ASB) qualifications to enable data exchange(13). 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. If properly adhered, the open standard will help assure against maliciously tainted and counterfeit products throughout the product life cycle including: design, sourcing, build, fulfillment, distribution, sustainment, and disposal(14).

The semiconductor industry has also identified the need for a concerted effort to provide non-hardware solutions to the identified networked hardware security issues. Suggestions include a cyber-security management (CSM) system 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 digital certificates. Such a system should be scalable, interoperable, easily deployed and administered. The standards development must be holistic and should encompass hardware, software and network.

Conclusions

Hardware security and privacy are becoming a critical design consideration, just like performance, power, and reliability, etc. These critical issues must be tackled in part 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 can be better coordinated to provide a more holistic solution to the problem. These requirements are best managed based upon industry-led standards that can be easily implemented across the supply chain. Also, research must be conducted to identify potential technical solutions to provide enhanced hardware security features.

References

1. Greenberg A. Hackers Remotely Kill a Jeep on the Highway—With Me in It http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ 2015 [cited 2016 February, 19]. Blog].
2. Colli A, Pisana S, Fasoli A, Robertson J, Ferrari AC. Electronic transport in ambipolar silicon nanowires. physica status solidi (b). 2007;244(11):4161-4.
3. Martel R, Derycke V, Lavoie C, Appenzeller J, Chan KK, Tersoff J, et al. Ambipolar Electrical Transport in Semiconducting Single-Wall Carbon Nanotubes. Physical Review Letters. 2001;87(25):256805.
4. Seabaugh AC, Qin Z. Low-Voltage Tunnel Transistors for Beyond CMOS Logic. Proceedings of the IEEE. 2010;98(12):2095-110.
5. Stoica A, Zebulum RS, Guo X, Keymeulen D, Ferguson MI, Duong V. Taking evolutionary circuit design from experimentation to implementation: some useful techniques and a silicon demonstration. IEE Proceedings - Computers and Digital Techniques [Internet]. 2004; 151(4):[295-300 pp.]. Available from: http://digital-library.theiet.org/content/journals/10.1049/ip-cdt_20040503.
6. Pei Z, Feenstra RM, Gong G, Jena D. SymFET: A Proposed Symmetric Graphene Tunneling Field-Effect Transistor. Electron Devices, IEEE Transactions on. 2013;60(3):951-7.
7. Fallahazad B, Lee K, Kang S, Xue J, Larentis S, Corbet C, et al. Gate-Tunable Resonant Tunneling in Double Bilayer Graphene Heterostructures. Nano Letters. 2015;15(1):428-33.
8. Yu B, Gaillardon PE, Hu XS, Niemier M, Jiann-Shiun Y, Yier J, editors. Leveraging Emerging Technology for Hardware Security - Case Study on Silicon Nanowire FETs and Graphene SymFETs. Test Symposium (ATS), 2014 IEEE 23rd Asian; 2014 16-19 Nov. 2014.
9. Arafin MT, Qu G. RRAM Based Lightweight User Authentication. Proceedings of the IEEE/ACM International Conference on Computer-Aided Design; Austin, TX, USA. 2840839: IEEE Press; 2015. p. 139-45.
10. Kobayashi M, Hiramoto T, editors. Device design guideline for steep slope ferroelectric FET using negative capacitance in sub-0.2V operation: Operation speed, material requirement and energy efficiency. VLSI Technology (VLSI Technology), 2015 Symposium on; 2015 16-18 June 2015.
11. Obeng YS. "Evaluation Of Product Authentication Technologies: A Detailed Evaluation Of The Current And Emerging Technologies", Obeng, Y. et al, presented at S College Park, MD: MTA / CALCE Symposium on Counterfeit Parts and Materials, Technical Symposium and Expo: June 23-24, 2015, ; 2015 [February 22, 2016]. Available from: http://www.calce.umd.edu/symposiums/SCEPJune2015_presentation.html.
12. Nolan C. Counterfeit Components – Assessment Methodology and Metric Development Las vegas: IPC Apex Expo; 2014. Available from: http://thor.inemi.org/webdownload/2014/APEX/Counterfeit_Components_032614.pdf.

13. Semi.org. New SEMI Standards to Combat IC Chip Counterfeiting 2009 [November 11th, 2015]. Available from: http://www.semi.org/en/new-semi-standards-combat-ic-chip-counterfeiting-0.
14. Group O. Open Trusted Technology Provider™ Standard (O-TTPS), Version 1.0, "Mitigating Maliciously Tainted and Counterfeit Products 2013 [November 11th, 2015]. Available from: https://www2.opengroup.org/ogsys/catalog/c139.