New & Old Challenges for Trusted and Assured Microelectronics

Saverio Fazzari
Booz Allen Hamilton
Arlington, Virginia
fazzari_saverio@bah.com

Robert Narumi
Raytheon Space & Airborne Systems
El Segundo, California
rtnarumi@raytheon.com

Abstract—In 2005, the Defense Science Board identified serious and pervasive vulnerabilities to US weapon systems in the future with the trend of microelectronics moving offshore for the fabrication of integrated circuits, development of EDA software, outsourced design work, and development of IP cores. As predicted, domestic sources for trusted microelectronics have diminished with commercial, industrial, and military markets and have become more reliant on non-domestic sources for microelectronics. The potential threats of malicious insertions by untrusted supply chain led to the DARPA Trust in Integrated Circuits program in 2007 to develop tools and techniques to ensure trust and integrity of ASIC and FPGA designs. Today, the threats to supply chain and hardware security are even greater with hardware vulnerabilities exposed, hardware hacking communities, and diminishing domestic manufacturing sources that do not provide state-of-the-art technologies to address C-SWAP (cost-size-weight and power) requirements of future military systems. Current initiatives and options to use untrusted, off-shore sources are evaluated against trust & assurance, protection of intellectual property, and 20-30 year life cycle requirements, and new research and development areas for test validation platforms, attribution, and chain of custody for trusted and assured microelectronics.

Keywords—trusted microelectronics, assurance, hardware Trojans, vulnerabilities, security, ASICS, military systems, Gartner Hype Cycle

For more than 60 years, development and production of advanced microelectronics for U.S. military and aerospace systems have relied on on-shore, domestic manufacturing sources. From the mid-1950s through the early 1980, the United States was the undisputed leader in virtually all segments of the semiconductor industry including manufacturing equipment and supplies [1]. However, as foreign competition flourished and the defense integrated circuit market declined over the years, the number of domestic manufacturing sources for state-of-the-art technologies has also diminished. Back in 1975, military usages accounted for 17% of worldwide semiconductors (ICs and discretes) with sales of $4.2 billion [2]. Today in 2018, the defense market for microelectronics represents less than 0.1% share of the total global market [3].

Concerns for system security date back as early as 1974 when the US Air Force published the results of a vulnerability assessment on Multics, an operating system built with security as its primary goal offering considerably stronger security than most commercially available today [4]. Despite hardware security controls such as segmentation hardware and a master mode, and software security controls including protection rings, access control lists, and enciphered passwords, hardware, software, and procedural vulnerabilities were exposed deeming Multics on Honeywell HIS 645 and 6180 computer systems not certifiably secure as an open use multi-level system [5]. However, the analysis formed the basis for defining the standard for Class B2 security in the Trusted Computer System Evaluation Criteria (TCSEC) and other operating systems [4]. The report considered inserting trap doors through weaknesses in the security controls, to perpetuate access into a system.

While personal computers, game consoles, and satellite/cable set boxes entered the consumer electronics marketplace in the late 1970s, 1980s, and 1990s, computer hackers would look for hardware and software vulnerabilities to break copy protection schemes, discover and explore undocumented modes, and to circumvent hardware to illegally access paid services. Websites [6] and books [7] posted instructions for people to learn how to hack. During the 1990s, satellite-TV pirates had also exploited a backdoor in DirecTV smartcards providing access to paid television programming [8].

Concerns into hardware backdoors and hardware Trojans were not publically discussed in news articles or research papers until the 2000s. According to a New York Times article in 2009 [9], unnamed US military and intelligence agency executives said “Trojan horses hidden in equipment circuitry is among the most severe threats the nation faces” and “in the future and possibly already hidden in existing weapons, clandestine additions to electronic circuitry could open secret back doors.” The article also claims possible Trojan horse kill switches may have been used in an Israeli Air Force attack in 2009, to read encrypted electronic messages through a hardware backdoor in an encryption machine made by Swiss company Crypto AG in 1980s, and other examples of hardware and software Trojan horses.

In addition, the 2005 Defense Science Board (DSB) Task Force report on High Performance Microchip Supply [10] expressed a concern that opportunities for adversarial clandestine operations were “enormous and increasing” as the US military dependence on advanced technologies progressively move offshore. For the Department of Defense’s strategy of information superiority to remain viable, trusted and assured supplies of integrated circuit components are required even from untrusted foreign sources. “Trusted” ICs and microelectronic components are defined as “those that can be employed by a user with confidence that they will perform as
expected and are free from compromises, denials, or exploitation” and while “assured” supplies meant “manufacturing capabilities that are available to produce needed quantities of microelectronics components throughout the life of their system applications.” The shift from United States to foreign IC manufacture opens up the possibility of Trojan horses and other unauthorized design inclusions that could endanger the security of classified information embedded in chip designs and could be used by an adversary to disrupt military systems at critical times.

As outlined in this report, the trustworthiness of chip designs needs to be verified with confidence that classified or mission critical information has not be compromised, reliability is not degraded, or unintended design elements inserted into chips by an adversary agent during design or fabrication. The report encouraged research for the cases in which the designs were created outside the trusted flow. In 2007, Defense Advanced Research Projects Agency (DARPA) Microsystems Technology Office (MTO) launched the Trusted, Uncompromised Semiconductor Technology (TrUST)\(^1\) program to address the fundamental problem of determining whether a microchip manufactured through a process that is inherently “untrusted” (i.e., not under our control) can be “trusted” to perform operations only as specified by the design, and no more [15]. The program focused on three areas: (1) Hardware Validation: Techniques that can quickly and accurately determine whether an IC provided is the same as one available in a gold standard design (2) Design Validation: Trusted Design of ASIC hardware and FPGAs, and (3) System Integration: Integrating techniques into a comprehensive end-to-end system capability. The program focused at solutions both in the near term and advanced technologies that can be used to detect the risks. One of the big concepts was to determine what to detect and how measurements would occur. The idea which was revolutionary at the time was to detect changes not threats. The belief was that any change could be a threat so all of them need to be detected. The measurement mechanism was to be using probability of detection to evaluate the likelihood of correct detection.

Over three phases, performers on the TRUST program developed new tools and techniques to uncover changes in ICs inserted by the government in controlled test articles, with speed and accuracy improvements on larger designs and more demanding probability of detection and false alarm metrics. From the effort, some tools and techniques were transitioned to various government labs and universities and some were commercialized. Raytheon and its subcontractor Analytical Solutions, Inc. (now MicroNet Solutions, Inc.) also demonstrated the utility of its TRUST in Fabrication and TRUST in Design tools to reverse engineer a chip to verify its contents against an archived design database.

From this initial program from 12 years ago to address trust, DARPA has continued expanding a portfolio of microelectronics protections. DARPA programs aim to verify the origin and function of sensitive devices, to obscure the purpose of these devices, to protect intellectual property (IP), and to expand DoD’s supplier base. The resulting technologies from these programs are anticipated to help ensure the provenance, security, and reliability of the electronic components most likely to drive military capabilities over the next decade [11].

As shown in Figure 1, DARPA proposes multiple countermeasure groups, such as verification and validation. Individual tabs represent a non-comprehensive list of DARPA and other government programs as well as commercial protection efforts [16].

In addition, the Intelligence Advanced Research Projects Activity (IARPA) [14] has advanced tools and techniques to ensure trust in its Trusted Integrated Circuits (TIC), Rapid Analysis of Various Emerging Nanoelectronics (RAVEN), and Tools for Recognizing Useful Signals of Trustworthiness (TRUST) programs.

Since 2003, the Trusted Foundry Program (TFP), established as a joint effort between the DoD and the National Security Agency, and managed by the Defense MicroElectronics Activity (DMEA), provides US government acquisition programs access to ASIC and foundry services from trusted suppliers\(^2\). In its Trusted Foundry Access 2

---

\(^1\) The DARPA Trusted, Uncompromised Semiconductor Technology (TrUST) program is also noted as TRUSTed Integrated Circuits, TRUST in Integrated Circuits, and TRUST.

\(^2\) To be accredited by the DMEA as a trusted source, a supplier will (1) provide an assured “Chain of Custody” for both classified and unclassified ICs, (2) ensure that there will not be any reasonable threats related to

\[\text{726}\]
(TFA2) contract awarded in April 2016 with a period of performance through March 2023, TFA facilitates advanced access on a case-by-case basis (trusted FPGAs, microprocessors, and other complex standard products with no critical program information) to leading edge semiconductor technologies such as Fab 8 14LPP GlobalShuttle [15]. For ICs containing critical program information, the most advanced nodes available is 45nm RF CMOS through Global Foundries U.S. 2 LLC, East Fishkill (EFK). Unfortunately, GlobalFoundries and other U.S. fabs are not keeping pace with the global market. GlobalFoundries suspended its efforts for a 7nm foundry trailing TSMC at the end of 2018 with 95% market share of the 7nm chip market.

Per DoD 5200.44 [18], “integrated-circuit-related products and services shall be procured from a trusted supplier using trusted processes accredited by the Defense Microelectronics Activity (DMEA) when they are custom-designed, custom-manufactured, or tailored for a specific DoD military end use.” There is no policy requirement for a “trusted” field programmable gate array (FPGA) or a commercial off-the-shelf (COTS) component leaving the burden to validate the trust, assurance, authenticity, and reliability by prime contractors and subcontractors per Federal Acquisition Regulation, the Defense Federal Acquisition Regulation, the basic DoD Acquisition Policy (5000 series), and several other Instructions, Directives, and statutes.

In addition to restricting ASIC designs from containing critical program information per DoD 5200.44, companies must consider US Department of State International Traffic in Arms Regulation (ITAR) [19] and US Department of Commerce Export Administration Regulations (EAR) [20] guidelines when exporting designs for fabrication outside of the United States.

Under ITAR regulations, application specific integrated circuits (ASICs) and programmable logic devices (PLD) programmed for defense articles are listed as military electronics in the United States Munitions List (USML) Category XI. Additionally, EAR regulates controls of certain non-ITAR, non-USML, general purpose items with certain performance specifications that could be used for both defensive and non-defense articles such as monolithic microwave integrated circuits (MMIC), field programmable gate arrays (FPGAs), analog-to-digital converters (ADCs), digital-to-analog converters (DACs). Per CCL Category 3, masks and reticles, designed for integrated circuits are controlled by the EAR. Reasons for EAR controls vary by country. Companies seeking to export an ASIC design to be manufactured outside the United States should check specific controls per the EAR Commerce Country Chart.

Hardware security today is an interesting subject. It is firmly in the public eye with countless number of papers and research to address this field. The challenge is to understand how this work is being viewed. The Gartner hype cycle [21] is great way to look at the evolution of this field. It talks about the hype for the technology. The expectations of what hardware security could do was inflated and then fell as it became clear that perhaps many of the solutions are not viable. The technology solutions are being refocused to find the right kind of solutions. This concept is applied to many different technologies such as block chain and other things. It is important to understand the nature of this technology and how it is measured. Hardware security is view as important but is not clear why it important for a variety of reasons.

Today, reports of hardware backdoors and counterfeit parts continue often fueled by academia’s research into hardware vulnerabilities presented at the IEEE International Symposium on Hardware Oriented Security and Trust (HOST), and hardware hacking competitions such as Black Hat, DEFCON, and Hackaday.io. Chip manufacturers have admitted to unintended hardware vulnerabilities such that can compromise security including rowhammer, SPECTRE, MELTDOWN, and FORESHADOW. Software patches to these vulnerabilities are proposed as a solution but typically at the expense of performance. Also, chip designers can no longer assume intentionally inserted backdoors for test and undocumented features can be concealed as improvements in side-channel attacks, fuzzing, and fault testing expose their existence.

To counter IP theft and security threats and to spur new innovations in our microelectronics, the US government has launched initiatives over the past few years including DARPA Electronics Resurgence Initiative, Joint Federated Assurance Center (JFAC), DoD Microelectronics Innovation for National Security (MINSEC), TRUST HUB, AFWERX challenges, and more. These efforts are focusing on developing capabilities which take advantage of DoD research as well as leveraging the commercial interest in this area. All of the efforts are trying to advance the capabilities for both design as well as the need to create next generation electronics.

Historically, cases of unintended hardware vulnerabilities are more prevalent than reports of hardware Trojans.
Exploitation of either of these are different for commercial versus military systems, and as new systems are developed, the future state for trusted, assured, and protected microelectronics relies and depends on better understanding of the real hardware security problems, risks, and consequences. New innovations can help mitigate hardware vulnerability risks that can authenticate designs through fabrication to obfuscate, reconfigure, and morph functionality in ways that are more difficult to reverse engineer. However, with academia and the hacking community investigating new ways to uncover intentionally placed backdoors for test and manufacturing, undocumented functionality, and security keys, chip designers today have more challenges than cost, size, power, and weight to address trust, assurance, and protection over 20-30 year life cycle requirements. Research and development for test validation platforms, attribution, and chain of custody will also be required to safeguard our intellectual property and security.

REFERENCES


