Integrated Circuit Security Threats and Hardware Assurance Countermeasures

Karen Mercedes Goertzel, Booz Allen Hamilton

Abstract. Too often, software and system developers take the quality of computer hardware for granted, never doubting that the logic of the integrated circuits (ICs) on which software runs and critical application data is stored will consistently function in a dependable (correct, predictable) and trustworthy (non-malicious, non-exploitable) manner. After all, ICs seem to be free of the kinds of design and implementation flaws so common in software, and impervious to subversion by malicious code. So ICs are believed capable of achieving high levels of assurance impossible in software. This belief underpins Trusted Processor Modules (TPMs) and Hardware Security Modules (HSMs) [1], devices conceived as high-assurance platforms for critical software processes and highly sensitive data that need strong protection against tampering, interference by untrusted processes, and leakage. But is such faith in IC quality really merited? In recent years, the hardware supply chain has been flooded with counterfeit ICs of substandard quality and, more recently, hardware Trojans have emerged as a threat to the trustworthiness of IC logic. As a result, engineers of critical software-intensive systems need to employ tools that give them deeper insight into the inner workings of the ICs on which their systems' software will run. And the developers of that software need to design and implement their code so it can survive not only threats from human attackers and malicious software code, but from substandard hardware counterfeits and malicious IC logic.

Background: Definitions

A few definitions are needed before the rest of this article will make sense:

• **Integrated Circuit (IC):** Also referred to as a semiconductor or chip. A microscopic array of electronic circuits and other components, such as components such as resistors, capacitors, diodes, and transistors, that have been diffused or implanted onto the surface of a wafer carved from an ingot of semiconducting material such as silicon. The integrated refers to the fact that all of an IC's components, circuits, and substrate material are manufactured from a single piece of silicon (by contrast with a discrete circuit in which components are manufactured separately from different materials, and later assembled). ICs range in complexity from simple logic modules and amplifiers to complex microcomputers that contain millions of circuits and components.

• **Application-Specific Integrated Circuit (ASIC):** An IC designed for a specific application, such as a specific product line of cell phones, automotive controllers, or cryptographic devices, and unable to function in any other application. ASICs may be entirely customized "from the ground up" for a specific application, customized to perform different functions within a broader general application area, or designed and produced according to a narrowly-specified design for a set of pre-manufactured devices, systems, or logic in a given platform. A few examples of ASIC applications include: cryptography using proprietary encryption and decryption algorithm, medical monitoring devices, and proprietary systems-on-a-chip (SOCs).

• **Field-Programmable Gate Arrays (FPGAs):** ICs in which the system logic can be changed after the IC has been manufactured and deployed. Because of their field-reprogrammability, FPGAs are increasingly preferred as an alternative to non-reprogrammable ICs and ASICs.

• **Intellectual Property (IP):** In the context of ICs, IP refers to the IC's design logic. This design, or IP, is applied to the IC's silicon wafer in the form of a mask (see discussion of IC manufacturing below). In the IC industry, the design is also referred to as "the silicon" for the IC (referring to the mask applied to the silicon wafer).

Background: How ICs are Manufactured

A quick précis of how ICs are manufactured will help put the remainder of this article into context [2]. The process of manufacturing ICs typically consists of more than 100 steps—in some upward of 400. Manufacturing takes place in a clean room in which even the light sources are filtered. A single, thin slice of silicon called a wafer is created (by slicing a silicon ingot produced through a series of high-temperature physical, mechanical, and chemical processes).

The complex, interconnected design of the IC is prepared in a process similar to that used to make printed circuit boards, but with much smaller dimensions and many layers superimposed on top of each other. Each layer's design is created on a computer-aided drafting machine. The resulting design image is then projected into a "mask", which includes images for all of the dozens or hundreds of ICs to be formed on the silicon wafer. The mask is then optically reduced and transferred to the surface of the silicon wafer through a process of chemical coating and irradiation. The silicon version of the mask is transparent in some areas and opaque in others, so that when the other photolithographic and photoresist steps are applied to the wafer's surface, they collectively prepare the wafer for etching (by a chemical solution or plasma gas discharge) and/or by doping (atomic diffusion). These steps are repeated until all of the mask images created for the IC design have been permanently embedded onto the surfaces of the successive layers of the IC. Dielectric films are also applied as insulators between the layers, and on the top layer, to protect the silicon.

Once all the layers have been processed, the individual ICs on the wafer are tested for electrical functioning; those that fail are marked in ink for discard after the wafer is cut apart by a diamond saw into individual IC chips.

Each chip is then bonded onto a mounting package, which provides the IC with its contact leads—ultrathin wire leads (exponentially thinner than human hairs) connected to the package either by ultrasonic bonding or thermocompression. The mounting package is then encapsulated with a plastic coating for protection (or the chip may be assembled in a ceramic package, e.g., for

certain military or aerospace applications), marked with identifying part numbers and other data, and tested again before being sealed into anti-static plastic bags for storage or shipment.

Security Threats in IC Manufacturing and Supply Chain

As with software, IC logic is subject to design weaknesses and also to implementation flaws (or defects), which in the case of ICs are introduced during physical fabrication or manufacturing. And like software weaknesses and flaws, IC weaknesses and flaws can be exploited as vulnerabilities by human attackers. Like software, which is frequently pirated, then sold as genuine (licensed), ICs can be counterfeited with the fakes sold as genuine. Moreover, it has emerged in the last few years that like software under development by rogue programmers, ICs are also susceptible during their manufacture; in the case of FPGAs, malicious logic can be inserted even after the IC's deployment [3].

And as with software, these problems are extremely difficult to detect once the hardware has been manufactured and fielded. Indeed, the expense and time required to inspect ICs for malicious circuits or counterfeiting indicators is even greater than the cost of reviewing source code and testing executables, because of the level of expertise and the cost of specialized equipment required.

Unlike the software development lifecycle, which constitutes at most a half dozen or so stages or phases, the manufacturing process of an IC typically involves approximately 100-400 steps, each of which is susceptible to subversion by malicious actors. Such subversions may take the form deliberate design deficiencies (which, as with software, are probably only preventable through use of labor- and expertise-intensive formal methods) or malicious tampering during fabrication.

Each IC may contain as many as a billion transistors. At the rate of one transistor per second, it would take 38 years for someone to inspect all of the transistors on a single IC—an inspection process that is so difficult, tedious, and error-prone that the likelihood of finding even one tainted transistor among so many is extremely unlikely. In principle, an electronic device containing multiple ICs can be undermined by a handful of rogue transistors. This explains why ICs have become an increasingly attractive target to attackers.

Unclassified documentation of "built in" malicious logic—so-called "hardware Trojans" and "kill switches" in ICs—has yet to emerge outside of research papers. In 2007, researchers at University of Illinois at Urbana-Champaign made history by proving the feasibility of maliciously modifying hardware logic. The researchers developed two general-purpose methods for designing malicious processors, and used the resulting hardware Trojans to implement attacks that stole passwords, escalated privileges, and enabled automatic logins to computers containing the ICs. The nature of the modifications required involved the addition of a relative handful of logic gates to a pristine baseline IC. For example, the login attack that granted the researcher complete access to the targeted computer required the addition of only 1,341 logic gates to that computer's IC—0.08% of the total 1,787,958 logic gates used in the IC. In larger processors containing billions of gates, such a relatively tiny number of additions would be practically impossible to detect.

All ICs, but FPGAs in particular because they contain a significant portion of their own system-level, are vulnerable during manufacture to subversion by malicious design tools, which could be used to load a subverted design into the FPGA, in order to sabotage it (e.g., by causing it to short circuit). Unfortunately, as most hardware design-tool developers have few or no checks in place to ensure that their tools contain no such attacks on the specific functionality of ICs, the only available countermeasure at this point is to acquire only FPGAs with known-trusted cores (i.e., cores developed by trusted tools). Some FPGA manufacturers (e.g., Xilinx) digitally sign their FPGA cores to authenticate their trusted design. However, the typical FPGA chip may include multiple IP cores, both trusted and untrusted, and a digital signature used for core authentication does nothing to prevent the core's susceptibility to tampering or to snooping by other cores in the system. Interference between cores can be prevented by using a separate chip for each core; however, this approach increases power consumption and physical size, and does not prevent snooping via inter-chip communication lines on the board [4].

Automated IC test equipment can test millions of transistors per second for certain types of manufacturing fidelity. But such equipment is designed only to detect the IC's deviations from a narrow set of specifications. Any anomalies that involve aspects of the IC that are not covered by tests to verify and validate the IC against its specifications will go undetected. This not only leaves design weaknesses (especially in older IC designs), embedded hardware Trojans, "kill switches", and other misbehaviors and alterations undetected, but renders them virtually impossible to detect due to their sheer theoretical numbers. Hardware attackers often exploit the sheer complexity of modern ICs to insert their Trojan circuits, and use special or unlikely events at run time to trigger the deeply-buried malicious logic.

Inspections of suspected counterfeit ICs are somewhat more realistic. They begin with an analysis of the packaging and paperwork, then move on to several levels of inspection of the IC itself, including checking surface markings for permanency, and checking physical dimensions against known-genuine samples. Other techniques include external and internal visual analysis and radiographic inspection, material analysis, electrical testing, and accelerated life testing. Many of these tests involve specialized, often expensive equipment, such as scan electron microscopes, energy dispersive x-ray spectroscopes, Fourier transform infrared spectroscopes, s-ray fluorescence energy dispersion mechanisms, acoustic microscopes, and electrical test equipment (e.g., for Group A electrical testing and electrostatic discharge surface inspection). De-capsulation exposes the die to visual inspection under a metallurgical microscope, to reveal die markings for information such as the design year, which can then be checked with the OEM to verify whether the IC is authentic.

While IC manufacturers are likely to have some or all of the equipment necessary for IC counterfeit inspection, as such equipment is also used in IC quality and stress testing, purchasers of ICs are seldom so provisioned, nor skilled enough to use such equipment to perform the various tests. For this reason, as with the software industry, in which companies such as Veracode, Cigital, and Aspect Security (to name a very few) can be contracted to perform software analyses, an increasing number of firms (e.g., Process Sciences Inc., EQuality Process, IC Detect

Analytical Services, Silicon Cert Laboratories, ACI Technologies, Trace Laboratories) offer contract hardware analysis services to organizations that lack the resources or expertise to perform counterfeit electronics tests and analyses in-house.

The cost of fabricating ICs has driven many original equipment manufacturers (OEMs) such as Intel, Motorola, Texas Instruments, and others, to "go fabless", i.e., to outsource the fabrication and testing of their ICs to offshore foundries in countries such as China, Taiwan, South Korea, Malaysia, and the Philippines, in which labor costs are much lower. As with outsourcing of software development, this raises the question of how the fabless OEMs can assure that the ICs they received from the foreign foundry conforms exactly to the design (known as "the silicon") that they provided to the foundry—with nothing added or omitted? Moreover, increasingly OEMs are even outsourcing the design of their ICs, which raises questions about the trustworthiness not only of manufacturing, assembly, and packaging processes and tools, but of design kits and design libraries.

Because most of ICs used throughout the worldwide information and communications infrastructure are produced in unsecured facilities outside the U.S., national and homeland security establishments are increasingly concerned about the possibility of sabotage and subversion during the IC manufacturing process. However, there are also those who question how much the U.S. really has to fear with regard to subversion/sabotage of ICs or other electronic components by foreign manufacturers.

According to Martin Libicki of the RAND Corporation, "Unlike computer hacking, many of whose techniques are published on the Web and in print, the insider and component methods are essentially the province of state intelligence agencies and therefore highly protected. It is unclear how well they have worked. Consider what damage a deliberately corrupted component would have on China's reputation, much less the reputation of the guilty supplier. One discovery may create the incentive to recycle everything acquired from the now-suspect source. [It is a form] of deception and of the sort that the once-deceived is unlikely to fall for as easily again [5]."

Security Threats Specific to Integrated Circuits

The predominant threats to the security properties of ICs are:

- Counterfeiting (threat to authenticity and often, due to deficient quality of counterfeits, dependability)
- Reverse engineering to extract IP or discover sensitive data, such as cryptographic keys, contained in on-chip memory (threat to intellectual property and data confidentiality)
- Tampering to sabotage IC operation or insert malicious functionality, such as Trojans or kill switches (threat to integrity and trustworthiness)

Each of these threats is explored below.

IC Counterfeiting

It has been estimated that upwards of 5% of all commercial ICs are counterfeit. Counterfeiting typically refers to the production of near-identical replicas of genuine products or of product data (e.g., certificates of authenticity)—replicas that are close enough in appearance to the original to be mistaken as genuine by a typical user, reseller, tester, or other non-expert observer. The ability to copy an IC's IP (which is, remember, its design) is exploited by unscrupulous IC fabricators, particularly those offshore, for use in counterfeiting or "overbuilding". Overbuilding, also referred to as "run-in fraud", is a form of IP piracy and IC counterfeiting in which a subcontractor to an IC manufacturer copies the IP from the ICs they are subcontracted to manufacture, then inserts that IP into cheaper ICs purchased on the open market. The manufacturer then sells the ICs containing the pirated IP in direct competition with the original equipment manufacturer.

When it comes to ICs, however, most counterfeits are not replicas, but are legitimate ICs that have been altered and/or misrepresented in some way. Often, they are salvaged from discarded computer boards or electronic devices, or from the "sweepings" of IC foundries ("sweepings" are ICs rejected during manufacture, usually because they fail testing), resurfaced, and relabeled with another, newer revision number, and then delivered with documentation that misrepresents their true performance (e.g., speed, tolerance), mechanical characteristics (e.g., compliance with the Restriction of Hazardous Substances [RoHS] Directive), or pedigree (e.g., Texas Instruments vs. Fairchild Semiconductor), or ability to withstand extreme conditions, i.e., high temperatures or high clock speeds, expected of the genuine ICs that they are imitating. As a result, counterfeit chips are often more susceptible to failure or compromise than genuine ICs.

The threat of counterfeiting and overbuilding is so great that most IC OEMs have invested heavily in developing mechanisms to protect their in-chip IP. Such mechanisms include encryption, obfuscation, watermarking, and fingerprinting. Most OEMs also include mechanisms, such as bitstream encryption and authentication, for securely uploading the programming bitstreams used to reprogram FPGAs. Bitstream authentication ensures that an FPGA will accept only those programming bitstreams whose integrity can be validated via Message Authentication Codes. Some OEMs also provide their customers with authenticated remote hardware update channels that prevent the uploading of subverted update bitstreams that contain malicious design logic. In hardware obfuscation, the description or structure of the hardware is modified in a way that intentionally conceals its functionality if an attempt is made to reverse engineer the IC. Hardware IP watermarking consist of the IP owner's identifying information being embedded and concealed in the description of the IC, where it can be later detected to verify the IC's pedigree [6].

One authentication mechanism for ICs that has emerged from the research community is the Physical Unclonable Function (PUF). PUFs are unique physical characteristics that manifest as process variations in each of the ICs in a run fabricated from the same silicon mask. An IC's PUF serves as its unclonable identifier, which can be authenticated via a one-way challenge-and-response function in which the IC must correctly locate the output from one or more challenge inputs; this output should be unique to the IC, due to the uniqueness of its PUF's process variation, and thus provides the basis for unique authentication of that IC's PUF-based identifier [7].

In the end, however, there may be a far more obvious clue that an IC is counterfeit: its price. Most counterfeits, be they purses or pills or processors, sell for markedly less than the genuine article.

Reverse Engineering

Physical reverse-engineering attacks are used to glean information about the IC's operation, and can be invasive or non-invasive. Invasive attacks, or destructive physical inspection attacks, are performed by "depackaging", i.e., partially or completely removing the packaging of the IC, either through use of acids, solvents, or other chemicals, through physical abrasion via planing, grinding, or chemical or mechanical polishing, or by evaporating the packaging material with a laser cutter. Once the IC has been depackaged, the circuitry can be scanned as each IC layer is progressively revealed through grinding. Ability to access the circuitry also enables "reconnaissance" attacks, such as reverse-engineering the circuits of the IC, or locating positions of interest to be targeted in electromagnetic attacks. In addition, the metal tracks of the IC can be probed to measure signals and voltages or to actively inject signals. A focused ion beam (FIB) can also be used to drill fine holes in the IC's insulating layer to expose the fine metal tracks without disturbing the IC's other components; a FIB can also be used to alter the IC's circuitry or to reenable disabled self-test circuitry.

Non-invasive attacks are carried out by monitoring physical properties—or signals—associated with physical phenomena that arise while the IC is running. These physical signals can be analyzed to gain information about the IC's state and the data it processes. Signals can be derived from device timing/clock rate, electrical voltage levels/power consumption (simple and differential), temperature levels, electromagnetic (EM) radiation, acoustics, and light emission. What an attacker looks for is anomalies, such as variations in power consumption or glitches in clock frequency; the attacker may also exploit the IC's detectable signals to deliberately cause errors in the device's operation. Non-invasive attacks are referred to as side-channel attacks, and cryptologists have long studied the timing, supply voltage, and electromagnetic side channels of cryptographic devices to determine whether they can be exploited to discover cryptographic keys and to detect surreptitious data leaks. More recently, researchers have investigated the use of side-channel analyses, including as gate, temperature, timing channel, and performance analyses, to detect the presence of hardware Trojans and kill switches.

While difficult to prevent, physical attacks are so technologically sophisticated, and require such substantial resources, expertise, and patience, that they remain rare. For example, while it is conceivable that focused ion beams can be used to alter the wiring and bypass security features of an IC, accomplishing this type of attack requires expensive equipment and significant knowledge, especially when targeting a modern IC that has been fabricated with nanoscale feature sizes. The exception to the "difficulty" rule involves FPGAs, which are particularly susceptible to having their IP copied in the same way that software code can be copied. Conventional SRAM-based FPGAs are particularly susceptible because their memory is volatile, which means it must be re-initialized every time power is applied. Each re-initialization requires an external bitstream to be loaded into the FPGA. That external bitstream provides an easily exploitable, non-invasive conduit by which the FPGA's IP can be captured and copied.

The most secure FPGA has a single chip, with the non-volatile memory located on the FPGA chip itself. The FPGA's strong encryption capability is used not only for encrypting IP and programming bitstreams, but also the data in the on-chip memory. The non-volatile memory registers also store the encryption keys and the identifiers used to authenticate bitstreams. Encryption also protects IP and data stored in FPGAs that are subjected to physical "sand-and-scan" reverse engineering or data extraction attacks [8].

Tampering

Tampering to alter the functionality of an IC other than an FPGA is always done to the design of the IC, because it is virtually impossible to tamper with fabricated chips in a way that is fine-grained enough to alter the hardware's logic without simply destroying the hardware. Post-manufacture tampering is a greater concern for FPGAs whose system programming can only be modified safely if certain secure IC programming and data protections are provided to control access to the FPGA's IP and the data stored in its on-chip memory [9].

Due mainly to IC manufacturers' concerns over physical tampering to extract IP, an increasing number of ICs now have countermeasures against physical attacks built in. For example, the IBM 4758 co-processor "wraps" its hardware within a tamper-sensing and tamper-reactive "shell". Others have their IP encrypted so that even if the IC is physically attacked, its IP cannot be deciphered by the attacker [10]. Techniques for obfuscation of logic in ICs have also emerged, and are being improved upon to strengthen IC self-protection against intellectual property reverse-engineering [11].

Several interesting anti-tamper mechanisms have been emerging from DoD's Anti Tamper (AT) research initiative (the focus of which is to develop technologies that can prevent reverse engineering and extraction of IP from ICs used in sensitive DoD systems and applications) [12]. One such mechanism is IC metering, which provides a set of security protocols designed to enable an IC design house to maintain control of an IC after its fabrication. Such control may be passive, such as and may constitute limiting the number of ICs fabricated and the properties they exhibit, or it may be active, such as building into the IC the capability to automatically disable itself at run-time if any indication of tampering is detected [13].

Like time bombs and logic bombs in software, the intentional corruption of hardware generally occurs during its design, implementation, or manufacturing—well before the malicious logic is activated. But unlike software, with the exception of FPGAs, sabotaged ICs cannot be patched, so they remain a threat indefinitely. Remediating well-crafted IC-level vulnerabilities or malicious insertions would likely require physically replacing the compromised hardware. The skill required to replace hardware, particularly in deeply embedded systems, would ensure that compromised ICs remain in active use even after the discovery of the vulnerability or Trojan.

Also, because the IC represents the lowest layer in the computer system, malicious logic at the IC level can provide a means to bypass, subvert, or gain control over all software running above it—allowing sophisticated and stealthy attacks to be crafted specifically to evade software-based defenses. Any "defense in depth" that

involves only multiple layers of protection implemented by software, even low-level software such as VMs and kernel-level processes, can at best deter but not prevent attacks that originate from within the processor on which the software is installed.

For example, attackers might introduce a sequence of predetermined bytes into the IC to activate embedded malicious circuits, enabling leaks of highly-sensitive data or cryptokeys, to halt the processor at critical or random processing times, to scan for electromagnetic signals that provide the external cues for processor shut-downs, or to facilitate reverse engineering of the IC design. More sophisticated hardware Trojan logic has been devised that enables attackers to escalate privileges, turn off access control checks, and execute arbitrary instructions, thereby gaining a path to taking control of the machine, and establishing a foothold for subsequent system-level attacks. An IC with such a hidden Trojan circuit installed in a firewall could facilitate remote exploits; e.g., a packet sent from a predetermined network address or a key encoded as a series of requests to different ports could be used as the trigger for the Trojan to "reset" the firewall, thereby granting full unprotected access to the network [14].

But because the results of many hardware attacks manifest identically to "normal" hardware failures, such attacks may be misattributed to manufacturing defects or design flaws rather than malicious logic.

Hardware Assurance for ICs

As a recognized discipline, hardware security assurance—as distinct from hardware quality assurance or system safety assurance—is at a point in its maturity comparable to that of software security assurance a decade ago. Aside from antitamper mechanisms for device-level hardware such as smart cards, cryptographic devices, trusted processor modules, and hardware security modules (used in automatic teller machines), hardware security assurance largely focuses on ICs and IC assemblies, though until very recently, the main focus has been anti-counterfeiting and IP protection, including the application of post-silicon validation techniques [15] to post-manufacturing discovery of flaws in ICs indicative of counterfeiting or malicious circuits.

With the recent proof by researchers of the practicability of hardware Trojans, however, the need for a hardware manufacturing counterpart to a secure software development lifecycle has become clear. If this growing awareness and concern over malicious hardware follows a similar trajectory to that for malicious software, we should expect the discipline of hardware security assurance to further coalesce and advance in the next few years.

Because most IC manufacturing is done outside of the United States and Europe, predominantly in China, U.S. and NATO buyers of ICs lack both visibility into and control over the supply chain for the ICs on which they so heavily rely. Depending on the criticality of the purpose to which ICs will be put, reliance on commodity ICs may simply be too risky, even if unambiguous knowledge of IC pedigree and provenance throughout the supply chain could be obtained (which it cannot). When total control over and visibility into production of ICs for critical applications are vital, alternatives to commodity ICs can be designed and fabricated by trusted foundries.

In the U.S. by the Department of Defense (DoD), the Department of Energy (DOE), and the National Aeronautics and Space Agency (NASA) have already made significant progress in hardware assurance for ICs through their trusted foundry initiatives: DoD's Trusted Foundry Program, administered by the Trusted Access Program Office at the National Security Agency (NSA), with foundry accreditations performed by the Defense Microelectronics Activity (DMEA) [16], and DOE's Trusted Foundry at the Sandia National Laboratory Microsystems Center. In addition, research programs such as DoD AT and the Defense Advanced Research Projects Agency's (DARPA's) Trust in Integrated Circuits program [17] focus on advancing the technologies needed to increase trustworthiness of ICs intended for mission critical, security critical, and safety critical applications (e.g., cryptographic devices, weapon systems, nuclear power plants).

DoD AT and DARPA Trust in ICs are producing tamperproof and tamper-resistant IC technology that, while it may not scale to extremely high-volume manufacturing general-purpose ICs from companies such as Intel and Motorola, has successfully transitioned into commercially-produced ICs with anti-copying, antitamper, anti-reverse engineering IP protections, such as CPU Tech's Acalis [18] and Altera's Stratix and Arria [19] FPGAs.

Outside the U.S., significant advances in hardware security assurance are being made in the private sector—specifically in the payment and bank card industry, with particular focus on the security of ICs used in smart cards.

Conclusion

At a conceptual level, security assurance deficiencies in the manufacturing and supply chain for logic-bearing integrated circuits are directly comparable to security assurance deficiencies in the software development life cycle and supply chain, and like software security assurance deficiencies, hardware security assurance deficiencies in IC production have troubling implications that go far beyond concern over reduced quality. Intentional threats to ICs, both in- and post-production, threaten the dependable, trustworthy operation not only of the ICs themselves, but of any embedded and non-embedded software-intensive systems in which they are a core component. Threats to IC security manifest as counterfeiting (threat to IC authenticity, and by extension dependability), tampering and malicious circuitry (threats to IC trustworthiness), and reverse engineering (threat to confidentiality of intellectual property and sensitive data).

The dependability and trustworthiness of all hardware functions on which critical software relies should be verified and validated. Pre- and post-silicon IC testing tools and techniques have emerged—and continue to emerge—for detecting indicators of counterfeiting indicators and malicious inclusions in ICs. Unlike software testing, however, IC tests are unlikely to be within the abilities of system testers; instead, expert test labs will have to be enlisted. Alternately, assurance of ICs can be achieved through acquisition from verifiably trustworthy IC suppliers, be they accredited trusted foundries or commodity suppliers with a demonstrated commitment to secure IC production, which includes the full range of necessary hardware assurance processes and tests, as well as full supply chain traceability and transparency.

Ideally, all ICs destined for use in critical systems would be individually tested, and if they failed any hardware security assurance test, rejected. In reality, 100% test coverage for all ICs

may be possible only in systems in which ICs will be deployed in (very) limited quantities. For most system deployments, only a sampling of ICs (one hopes, large enough to be meaningfully representative) can possibly be tested. In such cases, trends analysis of results across the ICs in the tested sample will help the tester determine whether a tendency towards failure is likely to appear across the entire lot of ICs, and whether it may indicate a broader systematic deficiency in the manufacturing or supply chain practices of a particular IC vendor.

Testing as early in the system development lifecycle as possible will allow time and maximum scope for IC replacement (at the individual IC or whole-lot level) or supplier substitution. Moreover, critical systems must be architected to enable dynamic replacement of failed/suspect hardware, ideally with minimal operational disruption.

Furthermore, software developers should become knowledgeable about the threats to IC security, and the deficiencies in hardware security assurance practices in IC manufacturing that make ICs susceptible to those threats, so that they can design and implement critical software to include countermeasures that can mitigate the potential impacts of defective and anomalous hardware operations, so their software can survive any failures or subversive hardware operations that may originate from counterfeit or malicious ICs.

Further Reading

Goertzel, Karen Mercedes, *et al. Security Risk Management for the Off-the-Shelf (OTS) Information and Communications Technology (ICT) Supply Chain.* Herndon, VA: Information Assurance Technology Analysis Center, 17 August 2010.

Tehranipoor, Mohammad. "Mohammad Tehranipoor on Integrated Circuit Security". *YouTube*, 3 May 2012. <http://www.youtube.com/watch?v=d9Ib4s7sHWM>

University of Connecticut Center for Hardware Assurance, Security, and Engineering (CHASE) Website. <http://www.chase.uconn.edu>

EuroSmart. *Security IC Platform Protection Profile* (Version 1.0, BSI-PP-0035, 15 June 2007). <http://www.commoncriteriaportal.org/files/ppfiles/pp0%20035b.pdf>

European Joint Interpretation Working Group (JIWG). *The Application of CC to Integrated Circuits*, Version 3.0 Revision 1, CCDB-2009-03-002, March 2009. <http://www.commoncriteriaportal.org/files/supdocs/CCDB-2009-03-002.pdf>

ABOUT THE AUTHOR

Karen Mercedes Goertzel, CISSP, is an expert in application security and software and hardware assurance, the insider threat to information systems, assured information sharing, emerging cybersecurity technologies, and information and communication technology (ICT) supply chain risk management. She has performed in-depth research and analysis and policy and guidance development for customers in the U.S. financial and ICT industries, DoD, the Intelligence Community, Department of State, NIST, IRS, and other civilian government agencies in the U.S., the UK, NATO, Australia, and Canada.

Lead Associate
Booz Allen Hamilton
7710 Random Run Lane - Suite 103
Falls Church, VA 22042-7769
Phone: 703-698-7454
E-mail: goertzel_karen@bah.com

REFERENCES

1. Fisher, David A., et al. "Trust and Trusted Computing Platforms". Carnegie Mellon University/Software Engineering Institute Technical Note CMU/SEI-2011-TN-005, January 2011. http://www.cert.org/archive/pdf/11tn005.pdf -and- Edmison, Joshua N. *Hardware Architectures for Software Security.* Virginia Polytechnic Institute and State University Ph.D. Dissertation, 29 June 2006. <http://scholar.lib.vt.edu/theses/available/etd-10112006-204811/unrestricted/edmison_joshua_dissertation.pdf>
2. "Integrated Circuit". *Made How, Volume 2: How Products Are Made.* <http://www.madehow.com/Volume-2/Integrated-Circuit.html> -and- Intersil, "How Semiconductors are Made". <http://rel.intersil.com/docs/lexicon/manufacture.html>
3. Clark, Wesley K., and Peter L. Levin, "Securing the Information Highway". *Foreign Affairs* (November/December 2009). <http://www.international.ucla.edu/burkle/news/print.asp?parentid=112702>
4. King, Samuel T., et al. "Designing and Implementing Malicious Hardware". *Proceedings of the First USENIX Workshop on Large-Scale Exploits and Emergent Threats* (LEET). San Francisco, CA, 15 April 2008. <http://static.usenix.org/events/leet08/tech/full_papers/king/king.pdf>
5. Libicki, Martin C. *Cyberdeterrence and Cyberwar.* Santa Monica, CA/Arlington, VA/Pittsburgh, PA: The Rand Corporation, 2009. <http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf>
6. Huffmire, Ted, et al. "Managing Security in FPGA-Based Embedded Systems. *IEEE Design and Test of Computers* (Volume 25 Issue 8, November/December 2008).
7. Helinski, Ryan. "Physical Unclonable Functions". 27 October 2009. <http://www.ece.unm.edu/~jimp/HOST/slides/RyansPUFslides.pdf>
8. Mertz, Michael. "Secure in-system programming for FPGAs". *EE Times* (26 October 2005). <http://www.eetimes.com/design/programmable-logic/4014793/Secure-in-system-programming-for-FPGAs>
9. Landis, Dave. "Programmable Logic and Application Specific Integrated Circuits" (course notes). <http://cset.sp.utoledo.edu/cset4650oc/fpga_arch_intro.pdf>
10. Kastner, Ryan, and Ted Huffmire. "Threats and Challenges in Reconfigurable Hardware Security". *Proceedings of the 2008 International Conference on Engineering of Reconfigurable Systems and Algorithms (ERSA '2008).* Las Vegas, NV, 14-17 July 2008. <http://cisr.nps.edu/downloads/08paper_threatschallenges.pdf>
11. Rajendran, Jeyavijayan, et al. "Security analysis of logic obfuscation". *Proceedings of the 49th ACM Annual Design Automation Conference (DAC '12).* San Francisco, CA, 3-7 June 2012.
12. DoD Anti-Tamper Program Website. <http://at.dod.mil>
13. Koushanfar, Farinaz. "Integrated Circuits Metering for Piracy Protection and Digital Rights Management: An Overview". *Proceedings of the 21st Association of Computing Machinery (ACM) Great Lakes Symposium on Very Large-Scale Integration (GLSVLSI '11).* Lausanne, Switzerland, 2-4 May 2011. <http://aceslab.org/sites/default/files/GLS-VLSI.pdf>
14. Abramovici, Miron, and Paul Bradley. Integrated Circuit Security–New Threats and Solutions. *Proceedings of the Fifth Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW '09).* Oak Ridge, TN, 13-15 April 2009.
15. Mitra, Subhasish, et al. "Post-Silicon Validation Opportunities, Challenges and Recent Advances". <http://www.eecs.berkeley.edu/~sseshia/pubdir/postSi-dac10.pdf>
16. DoD Trusted Foundry Program Website. http://www.trustedfoundryprogram.org/index.php -and- U.S. Department of Commerce. Chapter VIII: Fabrication and Design of National Security Products. *Defense Industrial Base Assessment: U.S. Integrated Circuit Fabrication and Design Capability,* May 2009, pages 92-99. <http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/bis_ote_ic_report_051209.pdf>
17. Adee, Sally. "The Hunt for the Kill Switch". *IEEE Spectrum* (May 2008). <http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch> -and- Robinson, Brian, "Building Trust into Integrated Circuits". Defense Systems (February 2008). <http://defensesystems.com/articles/2008/02/building-trust-into-integrated-circuits.aspx>
18. Adee, Sally. "New Chip Brings Military Security to Commercial Processors". *IEEE Spectrum* (April 2009). <http://spectrum.ieee.org/computing/hardware/new-chip-brings-military-security-to-commercial-processors>
19. Altera. "FPGAs: About Stratix Series–Design Security". <http://www.altera.com/devices/fpga/stratix-fpgas/about/security/stx-design-security.html>