Stuxnet Legacy: Faith Versus Fear

by Keith Guidry, CTO, Sawblade Ventures, LLC

Past

While industrial control systems run civilization's most critical infrastructure, including utility power plants and energy pipelines, they had avoided serious attention from hackers for many decades. This was a period of blissful ignorance for semiconductor makers until 2010 when the Stuxnet worm attack was publicized. Stuxnet rattled cybersecurity experts and woke up world governments to the serious threat and dangerous capabilities of modern cyber adversaries. Stuxnet code also became a valuable commodity for malicious actors seeking to learn how to exploit electronic control systems for industrial automation.

As Stuxnet corrupted the operation of the equipment being controlled into functionally unsafe modes, Stuxnet's most insidious property was that of stealth. The worm actively prevented the tracking and reporting of the actual behavior of the motor controls being attacked. This meant equipment operators were blind to the impending damage and were convinced the machinery worked properly even while it was being destroyed.

The worming method is extremely complex, drawing on multiple layers of engineering skill to achieve the damage. [1]

Naturally, software manufacturers took steps to close vulnerabilities and continue that work. Unfortunately, the attack surface is immense given the nature of software and interfacing methods in contact with the hardware electronics. A casual review of the necessary patches and methods imposed on the information processing structure immediately shows the daunting nature of attempts to protect hardware components (semiconductor circuits) by software means. [2]

Since Stuxnet's revealing, many variants of the worm are now available on the black market. The blueprint for software vectors injecting malicious code into hardware systems have been available for study, experimentation and sale for more than eight years as of this writing. During this time, software builders have worked mightily to counter such threats. Hardware builders have primarily relied on data protection measures for trusted data operations. These have not always been adequate. [3]

Given the number of legacy computers running old versions of various operating systems, existing worm implants from years ago may still be viable, waiting for a day when they would be activated remotely in concert. While this might hopefully be limited to isolated impact and only financial damage, the increasingly interconnected nature of devices provides ready vectors for infection by individuals with terrorist aims funded by significant players. But 'hope' is not a plan. Without a countermanding overwatch within new devices, even the latest hardware is vulnerable to dangerous infection.

Traditional faith in software initiatives to meet hardware attacks has been damaged and eroded by repeated failure. [4][5][6]

Fear of future threat by loss of semiconductor foundry assurance is building continuously. Counterfeit chips containing stolen or reverse engineered intellectual property are an increasing threat to data processing interests. As global supply chains become more vulnerable, counterfeit components become unknown parts of the control systems for machinery capable of causing major damage to lives and property. Traditional functional safety assurance turns to anxiety as the lowest bidder in the procurement process may be an unknown risk; a risk that is unknowable until failure.

As Internet of Things (IoT) initiatives spread, so do the attack vectors available to hackers and malevolent actors. This underlying fear damages what was hoped to be immediate robust and widespread adoption for edge computing elements, creating doubt in engineering efforts that were once blissfully ignorant of hardware threats. What was an obvious beneficial investment opportunity in task and treasure may suddenly become the downfall for investors at the mercy of malformed chips.

Efforts are being made to counter software invasion into hardware. Government efforts are driving technologists to rethink the threat vectors and resolve a way to stop software borne attacks on hardware:
"The objective of the (DARPA – Defense Advanced Research Projects Agency) SSITH (System Security Integrated Through Hardware and Firmware) Program is to develop hardware design tools that provide security against hardware vulnerabilities that are exploited through software in DoD and commercial electronic systems. SSITH seeks to leverage current research in hardware design and software security to propel new research hardware security at the microarchitecture level. Security approaches will limit the permitted hardware to states that are assured to be secure while maintaining the performance and power required for system operation." [7]

The nagging idea that 'we don't know what we don't know' is eating away at faith in technology vendors who must bring security and safety to their customers. That problem has become so threatening as to compel DARPA to declare modern Information Technology security and defense efforts a "Patch and Pray" operation. [8]

Beyond this DoD (Department of Defense) effort, however, is a semiconductor manufacturer's need to drill farther down into the host circuitry to protect from attacks that are not just software borne but are a result of signal probing, reverse-engineering, counterfeiting, and tampering efforts by sophisticated semiconductor embeds. This is necessary given the dawning reality that any actor possessing sufficient resources can be expected to gain access to the hardware itself; a scenario long dismissed by industry experts. Such actors have a wealth of available specialty equipment obsolete for most modern manufacturing methods but well suited for probing and reverse-engineering of chip structure, architecture and operation.

Prolog

At the time of the Stuxnet revelation, methods developed using DAFCA (Design Automation for Flexible Chip Architecture) tools and intellectual property were being vetted by industry, military and national security entities to demonstrate detection and counter-measures capable of pro-actively stopping such attacks. Had this technology been employed in the integrated circuits within the attacked Supervisory Control and Data Acquisition [SCADA] system, the Stuxnet worm would have been neutralized by active counter-measures made available within the integrated circuits – independent from any software running through the system.

This security, safety and active defense capability employs a fabric of networked granular programmable hardware instrumentation capable of monitoring and modifying the operations of the host circuit. This parasitic automation approach has the benefit of observing activities not seen by software, while at the same time enforcing rules that cannot be altered by malicious or defective software. The defensive hardware fabric is not visible from the application or operating system software. Through hardware obfuscation techniques, the fabric cannot be detected or corrupted by any method including reverse-engineering or cloning of the circuitry.

Parasitic automation fabrics may be applied and networked within silicon or FPGA circuits. Such embedded fabrics allow for reprogramming and reconfiguring of passive and active defense elements. These "personality" based methods may be extended by rerouting and rewiring of the host circuit at-speed throughout the life of the semiconductor circuits whether manufactured by foundry or FPGA (Field Programmable Gate Array) means.

An embedded fabric in overwatch duty on a host circuit can augment any existing embedded trust, data protection, operating process and functional safety criteria at the next revision of any legacy or new circuitry. This embedding may be employed at any circuit scale from the smallest sensor/processor circuitry to the largest SOC (System on a Chip) circuits to protect against software borne attacks. Data available from the fabric is available to outside software to extend the overwatch capabilities to handle new attack methods without resorting to revving up to another chip version.

The embedded fabric may granularly protect semiconductor intellectual property, operational information and processed data achieved by hardware access. Efforts to reverse engineer such augmented host circuits may be additionally obfuscated against counterfeiting and reverse engineering, rendering the fabric uncloneable. Probing efforts may be sensed and countered using a variety of obfuscation techniques such as boosted state engines, self-authentication, gate camouflage, calculated noise and other methods. New methods of protection may be created through ongoing research into host circuit protection by white hat deception and active defense methods. [9]

Summary

The future is played through on the mistakes of the past. Civilization's reliance on control hardware for manufacturing, commercial and consumer operations from the smallest scale to the largest demands the best approach available. To fail in the mission to protect system hardware at any scale is to render software security useless.

Software borne attacks are not the end of the trail. Efforts to probe into the hardware circuits are increasing as bad actors acquire low cost technology to achieve espionage efforts to copy and counterfeit semiconductor intellectual property to steal knowledge and data.

Technology customers in fear of relentless threats must be assured in a way that will justify their faith in the proffered solutions. This burden rests on the shoulders of semiconductor manufacturers and procurement/supply chain authorities for advancement and enforcement to counter the eroding of faith in critical electronic control safety functions.

References:

[1] Industrial Ethernet Book Issue 61 / 35 The Stuxnet worm and options for remediation,
Industrial Ethernet Book Issue 61 / 35, August 2010

[2] Microsoft Security Bulletin MS10-046 - Critical

Microsoft, Published: August 02, 2010, Updated: August 24, 2010

[3] Windows PCs remained vulnerable to Stuxnet-like attacks despite 2010 patch
By Lucian Constantin - Romania Correspondent, IDG News Service, Mar 11, 2015

[4] 'Irongate' attack looks like Stuxnet, quacks like Stuxnet ...
By Darren Pauli, The Register, 3 Jun 2016

[5] DHS and FBI detail how Russia is hacking into U.S. nuclear facilities and other critical infrastructure
By Taylor Hatmaker, Techcrunch, Mar 15, 2018]

[6] Flaw in global energy facility software shows critical infrastructure risks
By Taylor Hatmaker, Techcrunch, May 5, 2018

[7] System Security Integrated Through Hardware and Firmware (SSITH) Proposers Day
DARPA (Archived) April 21, 2017

[8] System Security Integrated Through Hardware and Firmware (SSITH), page 2
By Linton Salmon, DARPA, Apr 21, 2017

[9] Hardware Protection Through Obfuscation
Edited By Domenic Forte, Swarup Bhunia, Mark M. Tehranipoor, Springer, 2017

Additional Information:

The Great Brain Robbery
By Lesley Stahl, CBS News, January 17, 2016
"The Justice Department says that the scale of China's corporate espionage is so vast it constitutes a national security emergency, with China targeting virtually every sector of the U.S. economy..."

Plan for $10 Billion Chip Plant Shows China’s Growing Pull
By Paul Mozur, New York Times, February 10, 2017
"Although the semiconductors produced at the plant will be a generation behind the most cutting-edge chip technology, they are based on a special design that is likely to make them useful… increasingly being connected to computer networks."

Globalization in Retreat | China’s Next Target: U.S. Microchip Hegemony
By Bob Davis and Eva Dou, Wall Street Journal, July 27, 2017
"Some bids were so overvalued U.S. government officials joked the Chinese were willing to pay an 'espionage premium.'"

China’s Technology Ambitions Could Upset the Global Trade Order
By Jane Perlez, Paul Mozur and Jonathan Ansfield, New York Times, November 7, 2017
"When concerned officials in Washington began blocking… one American company found a way to help its Chinese partner around those limits… by licensing its exclusive microchip designs, rather than selling them."

China's Sinovel Convicted in U.S. of Stealing Trade Secrets
By Janan Hanna, Christie Smythe, and Chris Martin, Bloomberge, January 24, 2018
"Prosecutors said Sinovel, now China’s largest wind turbine manufacturer, contracted with a former AMSC employee in Austria to steal the code in 2011, and then refused to pay the U.S. firm for $800 million in products and services it had promised to buy. The software system, called Low Voltage Ride Through, or LVRT, was designed to help regulate the flow of electricity into a power grid."

Has China used British technology to build a railgun?
by Gareth Corfield, The Register, March 5, 2018
"The £8m sale of Dynex Semiconductor, an obscure British electronics firm based in Lincoln… may have helped China to develop a “supergun” capable of firing projectiles at almost 5,400mph and to make a huge step forward in the construction of its third aircraft carrier."

Contact: Sawblade Ventures, LLC – Austin, Texas – info@sawbladeventures.com