Everything begins in the chip.

Chip Security Vulnerability:
How to Close the Gap Between Design Software & Design Hardware

CTEA Electronics Symposium at Flex
Austin, Texas
November 8, 2018
Keith Guidry, CTO Sawblade Ventures, LLC
CIVILIZATION LIVES IN THE CHIP
HARDWARE SECURITY EVOLVES

We depend on bad actors to motivate our good actors.

Good actors don’t have the reach bad actors have.
ROOT CYBERPHYSICAL RISK

2007 ➔ VARIANTS
2005 Flame to 2016 Industroyer

Threatened:
Industrial Control Software (ICS)
DCS / PLC / RTU / SCADA

STUXnet

MALWARE

ACROSS AIR GAP

VIA INDUSTRIAL NETWORK

INTO ICS

2010

Different threat motivations than against financial or commercial systems

- Attack on Industrial Process Equipment and Operations
- First Published Nation-State Cyberphysical Attack
- Ancestor of Numerous Cyberphysical Attack Methods

Industrial Ethernet - IIoT at greatest risk
DARPA initiative SSITH seeks to block software borne attacks on legacy and new hardware.

This initiative kicked off the cyberphysical protection efforts by DARPA and US national interests.

This is also the imperative that brought about calls for hardware security in September of 2017.

SSITH addresses hardware vulnerabilities at their source and will address current and future vulnerabilities.

*2015 MITRE-recorded hardware vulnerabilities (CVE)
DARPA SSITH THEME

A significant portion of vulnerabilities recorded are software attacks on hardware.

Electronic System Vulnerabilities

- Software Only 37%
- Other 9%
- Unknown 11%
- Hardware + Software 43%

Data from MITRE/NIST CVE website

- Common Vulnerability Exposure (CVE-MITRE) commercial and DoD entries in 2015:
  - 6,488 recorded vulnerabilities in 2015
  - 43% were software-assisted hardware vulnerabilities

SOURCE: DARPA System Security Integrated Through Hardware and Firmware (SSITH) Proposers Day Overview page 3
CHIP INDUSTRY RECKONING

ARM CEO: Tech Industry Must Build an Immune System to Prevent a Cybercrime Pandemic

By Tekla S. Perry
Posted 27 Oct 2017 | 13:16 GMT

“... urging the tech industry to accept the fact that it has a social contract with users, that security is a collective industry responsibility and that security systems have to allow for human error.”

“‘It’s not just a software problem,’ (Simon) Segars said. ‘If we can do more in hardware, if we design things with the assumption that a compromise is going to happen, we can make the [security] software simpler.’”

2017 2018

THE WALL STREET JOURNAL

Businesses Rush to Contain Fallout From Major Chip Flaws

Software patches to plug holes could slow computers, experts say

By Sam Schechner, Stu Woo and Jay Greene
Updated Jan 5, 2018 9:02 a.m. ET

Businesses and institutions raced to patch computer systems and braced for expected slowdowns in system performance as they—and much of Silicon Valley—tried to gauge the fallout from the disclosure this week of two, long-hidden vulnerabilities affecting chips running most of the world’s computers.
## SECURITY APPROACHES

### Commercial Approach to Security

<table>
<thead>
<tr>
<th>Software</th>
<th>DARPA Formal Method Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual application security evaluation</td>
<td>Software Assertion: System is secure against software attacks</td>
</tr>
<tr>
<td>Overall system security is evaluated heuristically</td>
<td>Assumption: OS executes microcode as instructed</td>
</tr>
</tbody>
</table>

### Firmware

| Security a minor consideration |
| Firmware security frequently independent from software or hardware |

### Hardware

| Major security effort is in circuit verification |
| Verification is focused on functionality |
| Malicious intent to create errors is often ignored |
| Security communicated through specification sheets |

---

**HACMS**

- **Firmware**
  - Assertion: OS executes microcode as instructed
  - Assumption: SoC performs only specified operations

- **Hardware**
  - Assertion: SoC performs only specified operations with hardware vulnerability protection
  - Assumption: IP performs only as per spec
    - Transistors perform as per models

**SSITH**
Sawblade believes:

... the best way to achieve a secure chip is to establish communications with the outside world from inside the chip.

... the best way to achieve secure firmware is to create per-use firmware structure per specified software process.

... the best way to achieve secure transaction processing is to create per-use autonomous policing fabrics inside the chip.
SOFTWARE BORNE ATTACK

Spectre
- Exploitation does not leave any trace in traditional log files
- Hard to distinguish from regular benign applications
- Has L1TF been exploited in the wild?

Foreshadow
- Foreshadow tricks SGX enclave into sending out secrets

Meltdown

2017

2018

We don't know.
SOFTWARE BORNE ATTACK

2018
(Most Recent)

Hacks sniff for L1TF instructions.

SW Solution: Stop using acceleration.

Intel CPUs fall to new hyperthreading exploit that pilfers crypto keys

Side-channel leak in Skylake and Kaby Lake chips probably affects AMD CPUs, too.

DAN GOODIN - 11/2/2018, 6:00 PM
HARDWARE BASED DEFENSE

HW technology **must** protect against BEHAVIOR:

- **Invasive attacks** – glitching and error injections
  - By monitoring key signals, providing real-time detection and defense countermeasures as an operative whole or in granular part

- **Attempts to modify the bootloader or operation of the system during power up/down and reset periods for any block of functionality**
  - By performing granular event monitoring, checksumming, hashing and timing analysis during deterministic period whether as an operative whole or in granular partial operation

- **Man-in-the-middle attacks and attempts to run either hardware or software separately**
  - By enabling software and hardware initiated challenge response protocols using timing analysis and hardware-based signatures
?What if you could 24/7/365...

... Verify your device is working the way it was designed to work... throughout the life of the chip? And change the test regime at will.

Clearblue was created to automate the injection of formal design tooling into a host microcircuit.

Enhances design understanding and exploitation of granular logic processes within microcircuits.

Capable of creating granular digital-twinning fabrics to overwatch and supervise host components.
SAWBLADE OVERVIEW

- Patented hardware-embedded flexibility/reconfiguration architecture
- $27.5M investments in intellectual property and automation tools
- Countermeasures and control are autonomous or user-executed
- Hardware embedded security to monitor/measure/manipulate
- Prevent counterfeiting or spoofing of microelectronic devices
- Impossible to detect or disable (real-time reconfiguration)

- Secure processes and storage with framework awareness and component awareness
- Unique ability to police every action the computer takes in micro-detail real-time 24/7
- Works in conjunction with software to create anti-threat metrics, solutions, analytics
- Presents embedded hardware device for security framework integration
- Security control to any electronic device's internal operating functions
- Delivers cybersecurity to any electronic circuit large or small
HOWEVER, SSITH does not prevent physical tampering, counterfeiting or reverse-engineering of the hardware.

Sawblade can achieve SSITH goals as well as defend against:
- Physical tampering
- Counterfeiting
- Reverse engineering

SSITH addresses hardware vulnerabilities at their source and will address current and future vulnerabilities.
SAWBLADE SOLUTION

Sawblade's hardware solution is:
• Embedded instrumentation
• Monitor and manipulate
• Multi-layered and networked
• Re-programmable
• Customizable IP logic
• Rewireable
• For the life of the chip
SAWBLADE QUALITIES

- Operates independent from the processor or software
- Monitor critical functions at granular hardware level
- Not subject to software borne attacks or hardware probing
- Hardware and software activation and control in hardware
- Real-time HW/SW multi-level functionality and behavior
- Creates tamper-resistant hardware and software subsystem
- Fault tolerant security with HW assisted fail-safe or fall-back
SECURE BY 24/7 VERIFICATION

Example methods SAWBLADE Tools and IP enable protection:

**Twinning**: masked overwatch of host operations

**Obfuscation**: traveling configuration

**Calculated Noise**: traveling signal emanations

**Reconfiguration**: traveling signal structure

**Rerouting**: traveling signal path

**Rewiring**: traveling construction

**Personality**: traveling assurance

**Profile**: chip operations time-frame pattern listing

**Property**: unique configuration of host traces
OUR GOAL: A SELF-AWARE CHIP

current hardware is only data aware for its designed operational purpose

NEEDED: create electronic data that is forensically discernible

AT THE BARE MINIMUM:

electronic hardware must be made threat-aware
Everything begins in the chip.

Chip Security Vulnerability: How to Close the Gap Between Design Software & Design Hardware

CTEA Electronics Symposium at Flex
Austin, Texas
November 8, 2018
Keith Guidry, CTO Sawblade Ventures, LLC
Sawblade Ventures
Austin, Texas 78749
sawbladeventures.com