2017 Industry Awareness of Hardware Exploitation

Sawblade Ventures, LLC
Austin, Texas

19MAR2018
Sawblade Ventures, LLC
Austin, Texas

Defense Advanced Research Projects Agency

DARPA Electronic Systems Need Better Hardware Protection

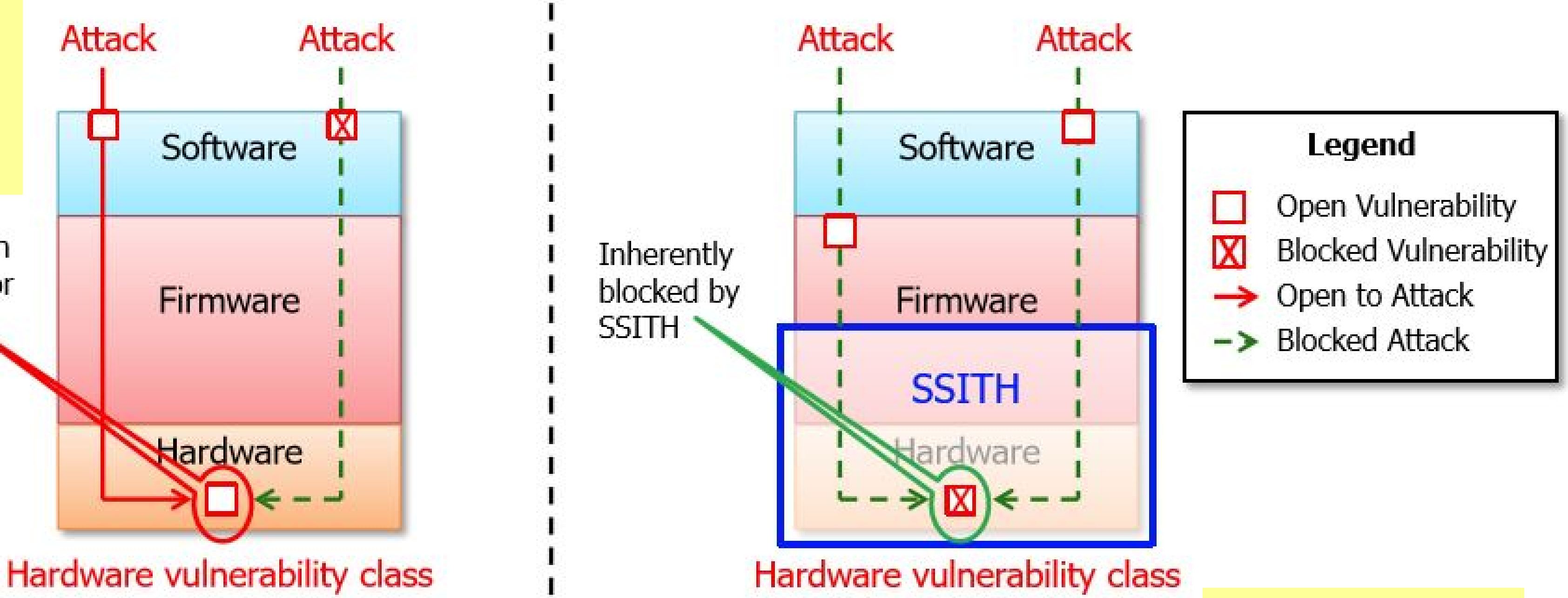
April 2017 DARPA issued a call for papers to confront the results of the Mitre Corporation's 2015 study of hardware classes vulnerable to software based attack.

Today: Patch and Pray

*2800 vulnerability instances
2800 software patches

Future: SSITH

SSITH will protect against all 7 hardware classes



*7 vulnerability classes
7 hardware solutions

This is a copy of a graphic from that announcement.

Sawblade technology are IP and tools for addressing these type issues since 2009.

But the tools have been dormant from 2011 to present.

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

*2015 MITRE-recorded hardware vulnerabilities (CVE)

DARPA SSITH System Security Integrated Through Hardware and Firmware (SSITH) Linton Salmon April 21, 2017

Electronic Systems Need Better Hardware Protection

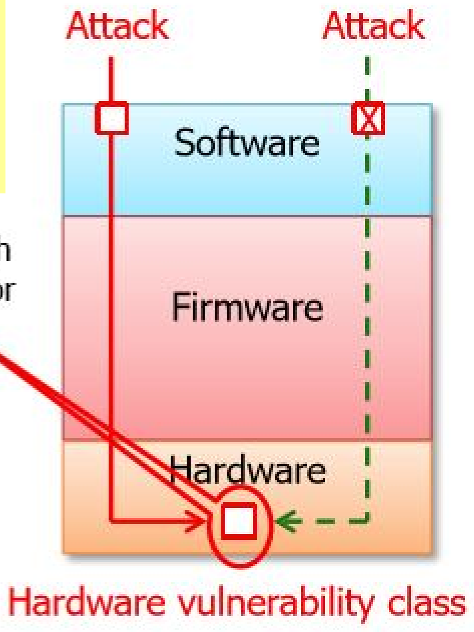
Hardware industry jarred awake In 2017.

Today: Patch and Pray

*2800 vulnerability instances
2800 software patches

The Equifax hack May - July 2017 was made possible by missing one patch event.

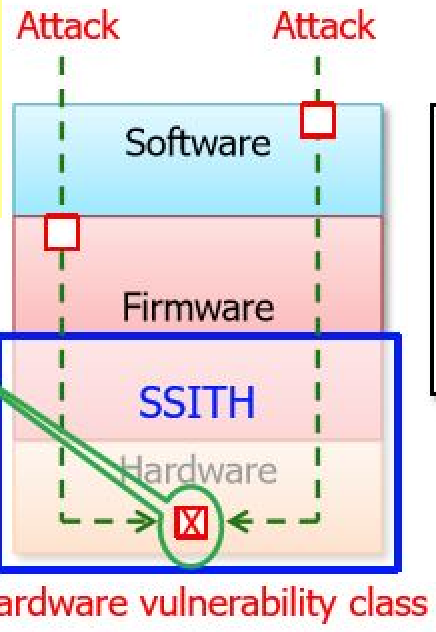
Found through open source or literature



Future: SSITH

SSITH will protect against all 7 hardware classes

Inherently blocked by SSITH



*7 vulnerability classes
7 hardware solutions

Legend

□ Open Vulnerability
☒ Blocked Vulnerability
→ Open to Attack
--> Blocked Attack

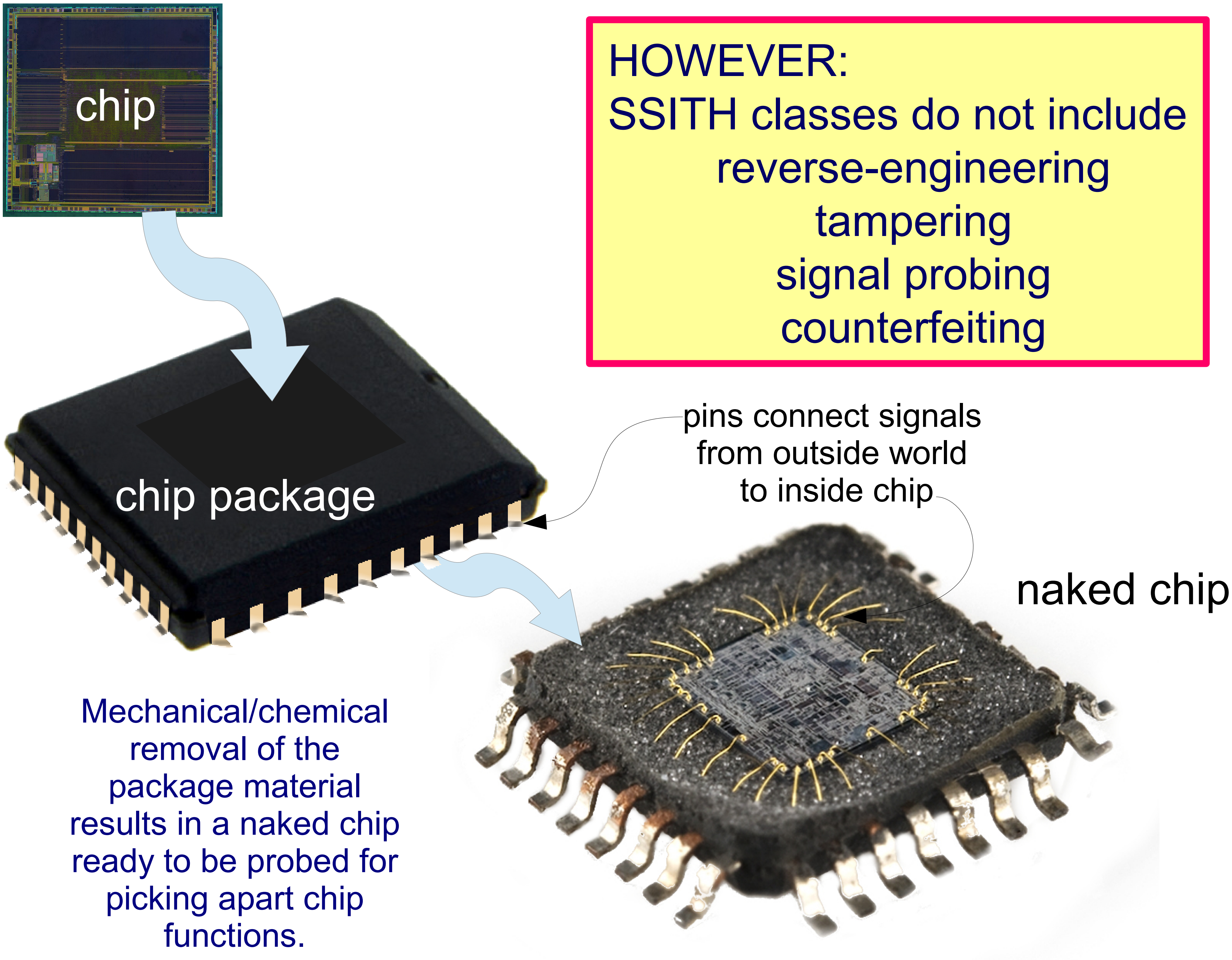
the future is always far away when needed Now.

Hackers are accelerating exploit research to get in before DARPA can identify winners and losers.

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

*2015 MITRE-recorded hardware vulnerabilities (CVE)

DARPA SSITH System Security Integrated Through Hardware and Firmware (SSITH) Linton Salmon April 21, 2017

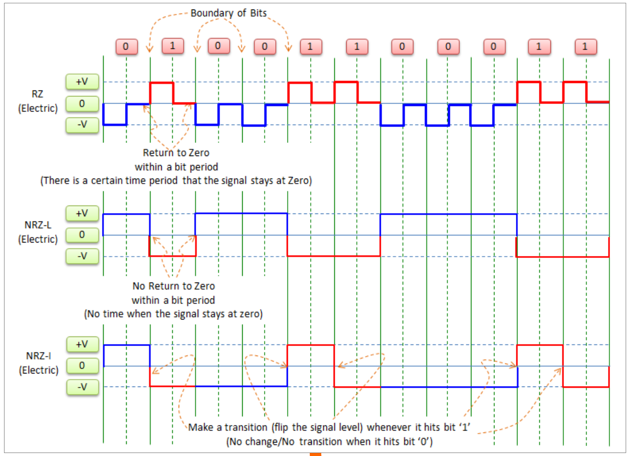


HOWEVER:
SSITH classes do not include
reverse-engineering
tampering
signal probing
counterfeiting

Mechanical/chemical removal of the package material results in a naked chip ready to be probed for picking apart chip functions.

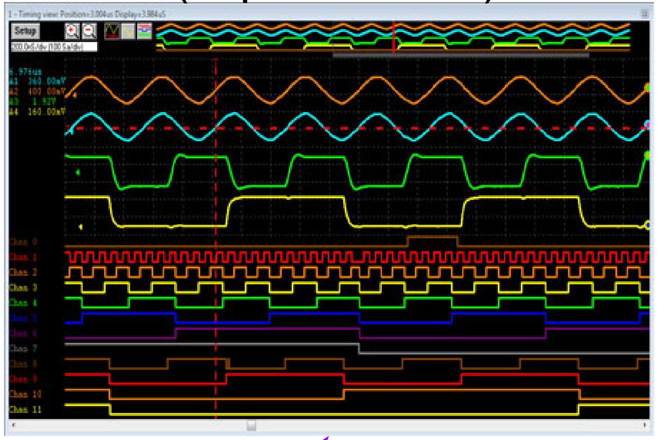
Becoming one of Software's biggest problems: The stripped chip is vulnerable to operational secrets theft.

signal analysis
(stimulus data)



Boundary of Bits
0
1
0
0
1
1
0
0
0
1
1
RZ
(Electric)
+V
0
-V
Return to Zero
within a bit period
(There is a certain time period that the signal stays at Zero)
NRZ-L
(Electric)
+V
0
-V
No Return to Zero
within a bit period
(No time when the signal stays at zero)
NRZ-I
(Electric)
+V
0
-V
Make a transition (flip the signal level) whenever it hits bit '1'
(No change/No transition when it hits bit '0')

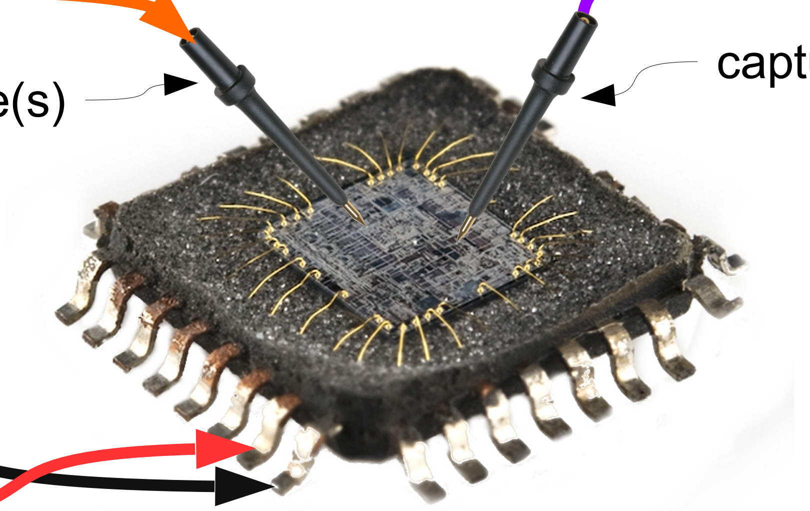
signal analysis
(captured data)



This is a standard method used by manufacturers to test random production lots for faults etc.

stimulus probe(s)

capture probe(s)

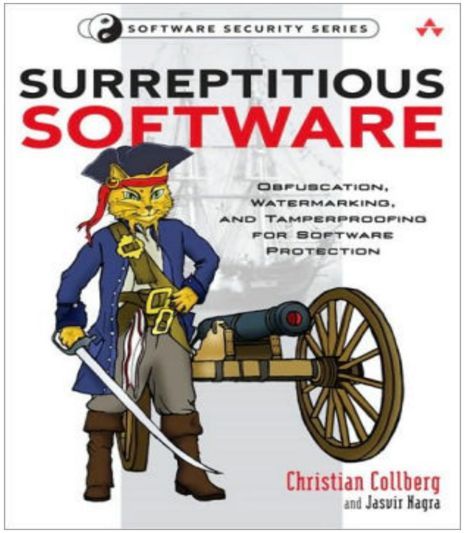


This method is also used by hackers to explore the inner workings of the chip to reveal vulnerabilities and opportunities to exploit them.

power

naked chip

Chip Threat/Security Evolution



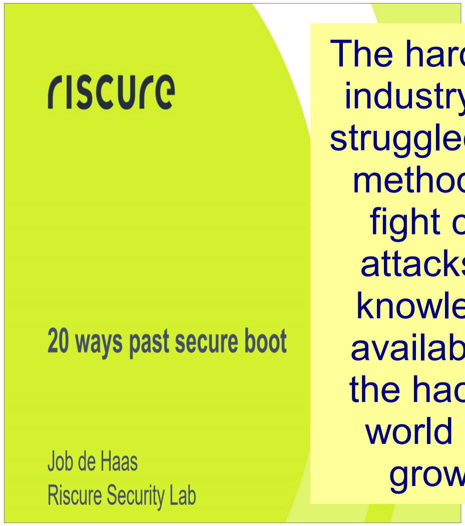
SOFTWARE SECURITY SERIES

SURREPTITIOUS SOFTWARE

OBFUSCATION, WATERMARKING, AND TAMPERPROOFING FOR SOFTWARE PROTECTION

Christian Collberg and Jasvir Nagra

2009



riscure

20 ways past secure boot

Job de Haas
Riscure Security Lab

2013

The hardware industry has struggled with methods to fight chip attacks as knowledge available to the hacking world has grown.

Point of Sale System Architecture and Security

Lucas Zaichkowsky
lucas@accessdata.com
Twitter: @LucasErratus

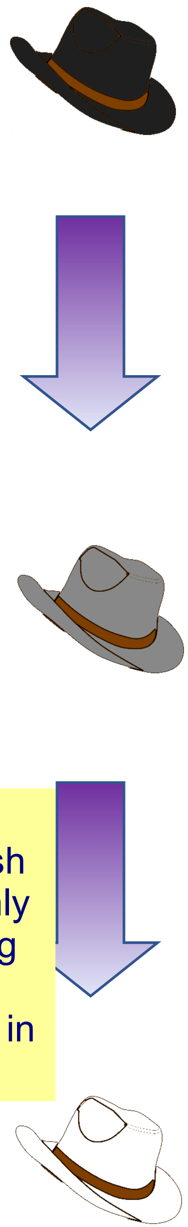
AccessData

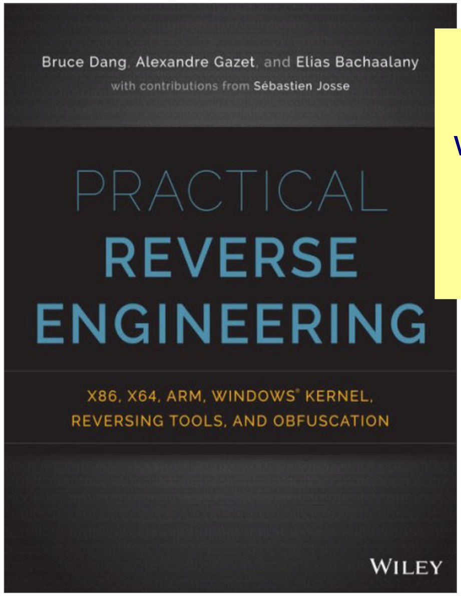
whoami

AccessData

- IT and InfoSec geek since mid-90s
- Evangelist and researcher
- Subject matter expert:
  - Electronic payment processing and PCI
  - Cyber espionage
  - Cybercrime
  - Enterprise IR

2014





Bruce Dang, Alexandre Gazet, and Elias Bachaalany
with contributions from Sébastien Josse

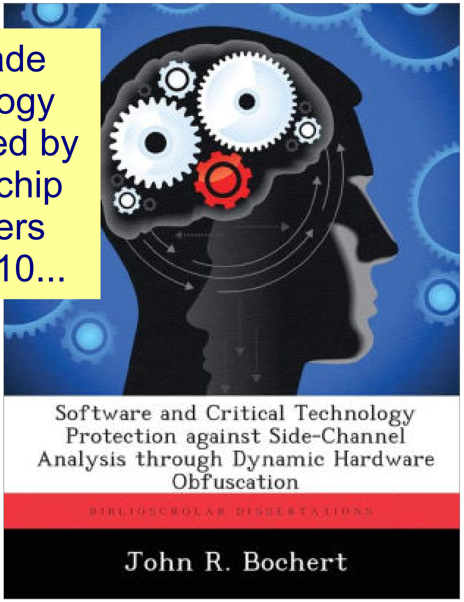
PRACTICAL REVERSE ENGINEERING

X86, X64, ARM, WINDOWS® KERNEL, REVERSING TOOLS, AND OBFUSCATION

WILEY

2014

Sawblade technology was vetted by military chip designers circa 2010...



Software and Critical Technology Protection against Side-Channel Analysis through Dynamic Hardware Obfuscation

BIBLIOSCHOLAR DISSERTATIONS

John R. Bochert

2016

Domenic Forte · Swarup Bhunia
Mark M. Tehranipoor *Editors*

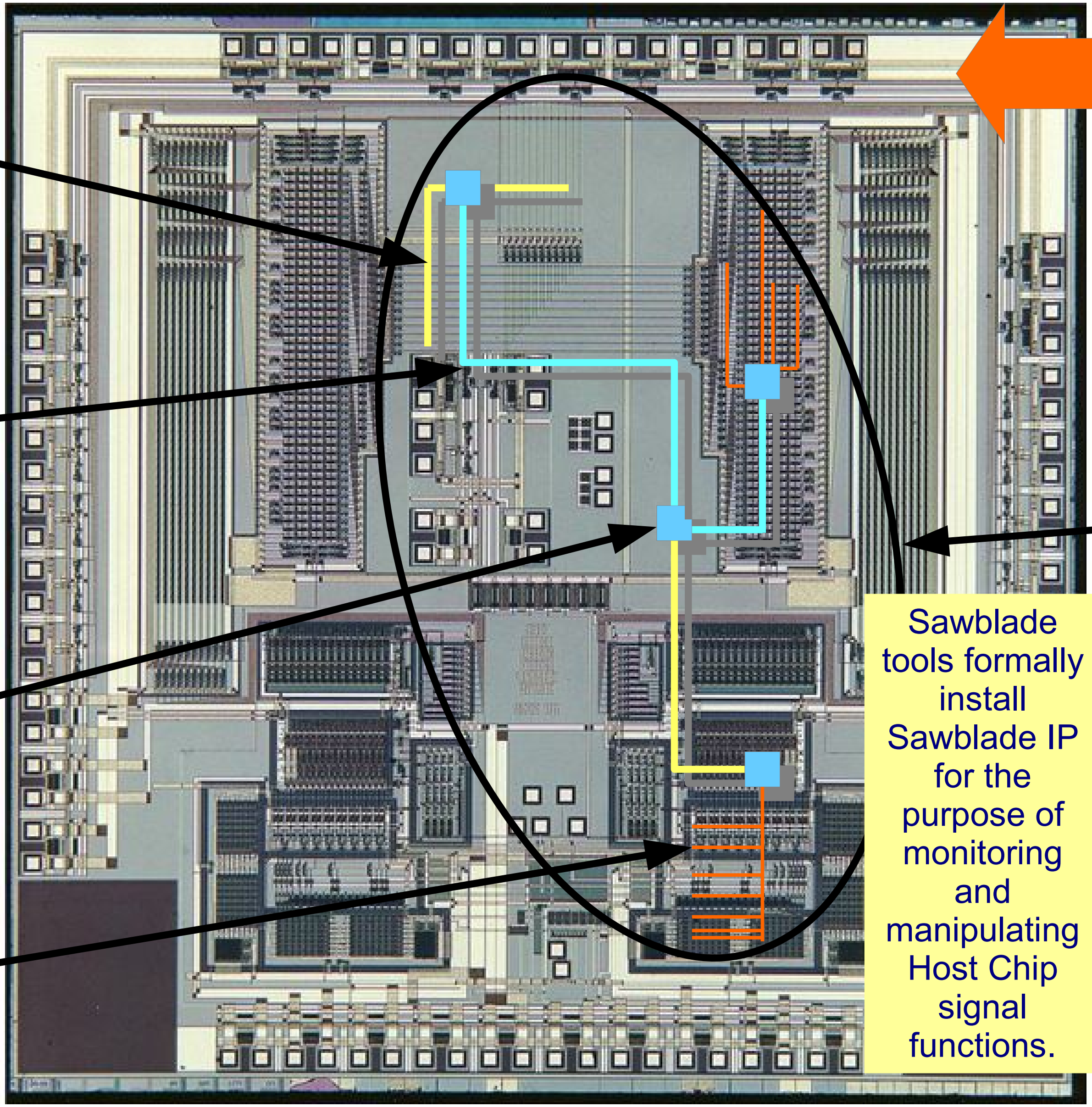
Hardware Protection through Obfuscation

Springer

2017

… to accomplish what is only now being widely discussed in 2017.

Solution: Chip Signals Management by Instrumentation and Automation



1 - Signals monitor structured groups

2 - Monitored signals inform state machines

3 - State machines determine response

4 - Response asserted via dynamic signals

Chip Design

Existing or New

Host circuit fitted with a separately formalized layer of networked instrumentation and automation

Sawblade tools formally install Sawblade IP for the purpose of monitoring and manipulating Host Chip signal functions.

Is It Validation or Security?

How SAFE is your “VALID”?

- Validation

1. to make valid; substantiate; confirm: aka “**assurance**”
2. to give legal force to; legalize. aka “**imperative**”
3. to give official sanction. aka “**safety**”

The security gap between Software and Hardware must be closed.

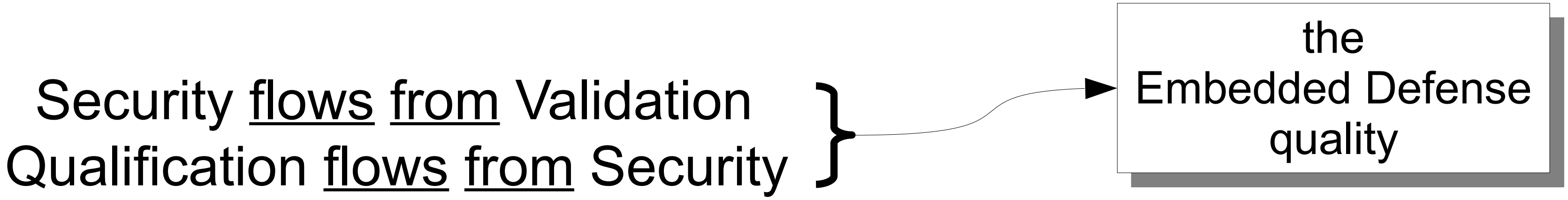
How VALID is your “SAFE”?

Validation = Security

- Security

1. freedom from risk. aka “**safety**”
2. protection; defense. aka “**imperative**”
3. well-founded confidence. aka “**assurance**”

Real-time Security requires operational 365/24/7 overwatch for the life of the chip.



Security flows from Validation
Qualification flows from Security

the
Embedded Defense
quality

Current Encryption is Doomed

NSA: (National Security Agency)
“A sufficiently large quantum computer, if built, would be capable of undermining all widely-deployed public key algorithms used for key establishment and digital signatures.”

NSA:
“It is generally accepted that quantum computing techniques are much less effective against symmetric algorithms than against current widely used public key algorithms. While public key cryptography requires changes in the fundamental design to protect against a potential future quantum computer, symmetric key algorithms are believed to be secure provided a sufficiently large key size is used.”

NSA's backdoor revealed in 2015.

So what do we do now while we wait?

NSA:
“Choosing the right time to champion the development of quantum resistant standards is based on 3 points: forecasts on the future development of a large quantum computer, maturity of quantum resistant algorithms, and an analysis of costs and benefits to NSS owners and stakeholders. NSA believes the time is now right—consistent advances in quantum computing are being made, there are many more proposals for potentially useful quantum resistant algorithms than were available 5 years ago, and **the mandatory change to elliptic curves that would have been required in October 2015** presented an opportune time to make an announcement. NSA published the advisory memorandum to move to quantum resistant symmetric key options and to allow additional continued use of older public key options as away to reduce modernization costs in the near term. In the longer term, NSA is looking to all NSS vendors and operators to implement standards-based, quantum resistant cryptography to protect their data and communications.”

https://en.wikipedia.org/wiki/Dual_EC_DRBG

End

Sawblade intellectual property and tools offer a way to formally confront a wide range of security and safety hardware issues today.

Sawblade Ventures, LLC
Austin, Texas