ConFirm: Detecting Firmware Modifications In Embedded Systems Using Hardware Performance Counters

Xueyang Wang[1], **Charalambos Konstantinou**[2], Michail Maniatakos[3], and Ramesh Karri[4]

[1]Offensive Security Researcher, Intel

[2]Assistant Professor, FSU

[3]Associate Professor, NYUAD

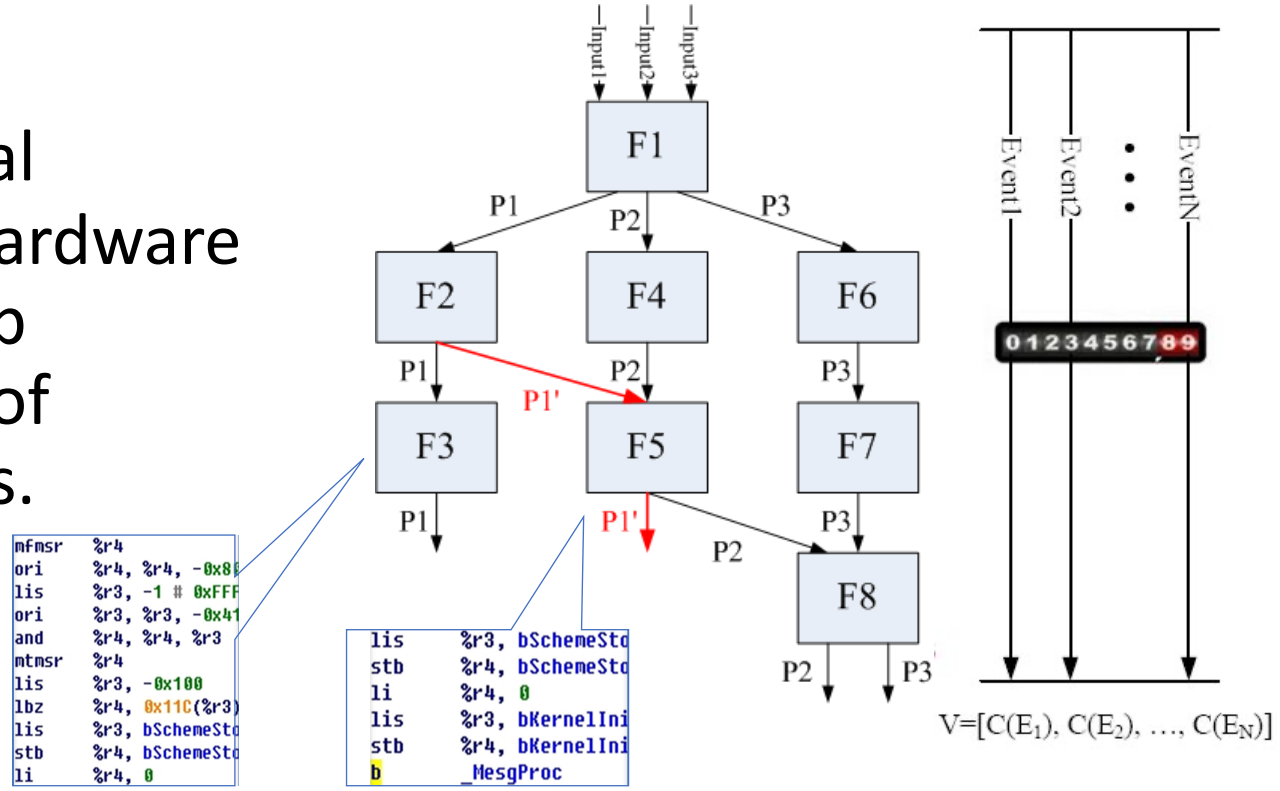
[4]Professor, NYU

*Work done while X. Wang & C. Konstantinou were PhD students at NYU.

**Paper appeared in ICCAD 2015.

ConFirm Concept

- The execution of code in embedded systems can be characterized with the total occurrences of specified hardware events and the relationship between the occurrences of different monitored events.



Outline

1. Technical overview
2. Key contributions
3. Long-term impact

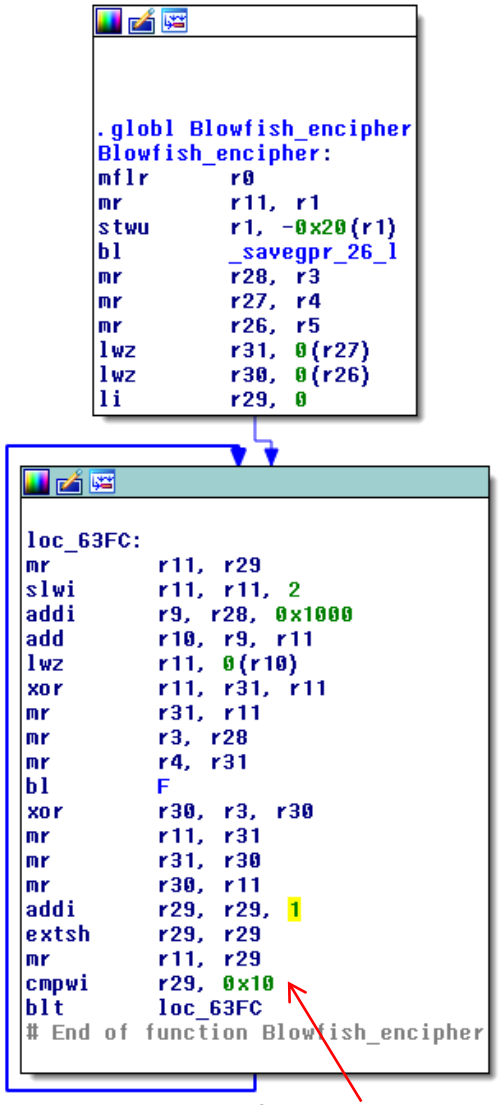
Problem Statement & Other Techniques

- Embedded systems: mobile devices, smart meters, power grid controllers, etc.
- Attacks on embedded system firmware (<=2015)
  - Reversing and exploiting an Apple firmware update *[Chen/Blackhat'09]*
  - Reprogram a smart battery by modifying the firmware *[Miller/DEFCON'11]*
  - Vulnerabilities in printer firmware update scheme can lead to malware execution *[Cui/NDSS'13]*
- Existing techniques (<=2015)
  - Requiring extra hardware components
    - E.g. Trusted Platform Module
  - Introducing high performance overhead
    - E.g. Binary instrumentation
- ConFirm
  - No extra hardware component (repurposing existing hardware for security)
  - Low performance overhead

[Chen/Blackhat'09] "Reversing and Exploiting an Apple Firmware Update," Black Hat, 2009.
[Miller/DEFCON'11] "Battery Firmware Hacking," DEFCON, 2011.
[Cui/NDSS'13] "When Firmware Modifications Attack: A Case Study of Embedded Exploitation," NDSS, 2013.

Introduction

- Hardware Performance Counters: special-purpose registers
- Low-level hardware events
  - E.g., clock cycles, instruction retirements, cache misses, load/stores, branches
- Built into almost every microprocessor
  - Intel Pentium IV: 18 counters, 130+ events
  - ARM A9: 6 counters, 70+ events
  - PowerPC e300c3: 4 counters, 30+ events
- **Key concept: program characterization**
  - ***Blowfish encryption***
  - Symmetric-key block cipher
  - The valid execution flow runs 16 iterations

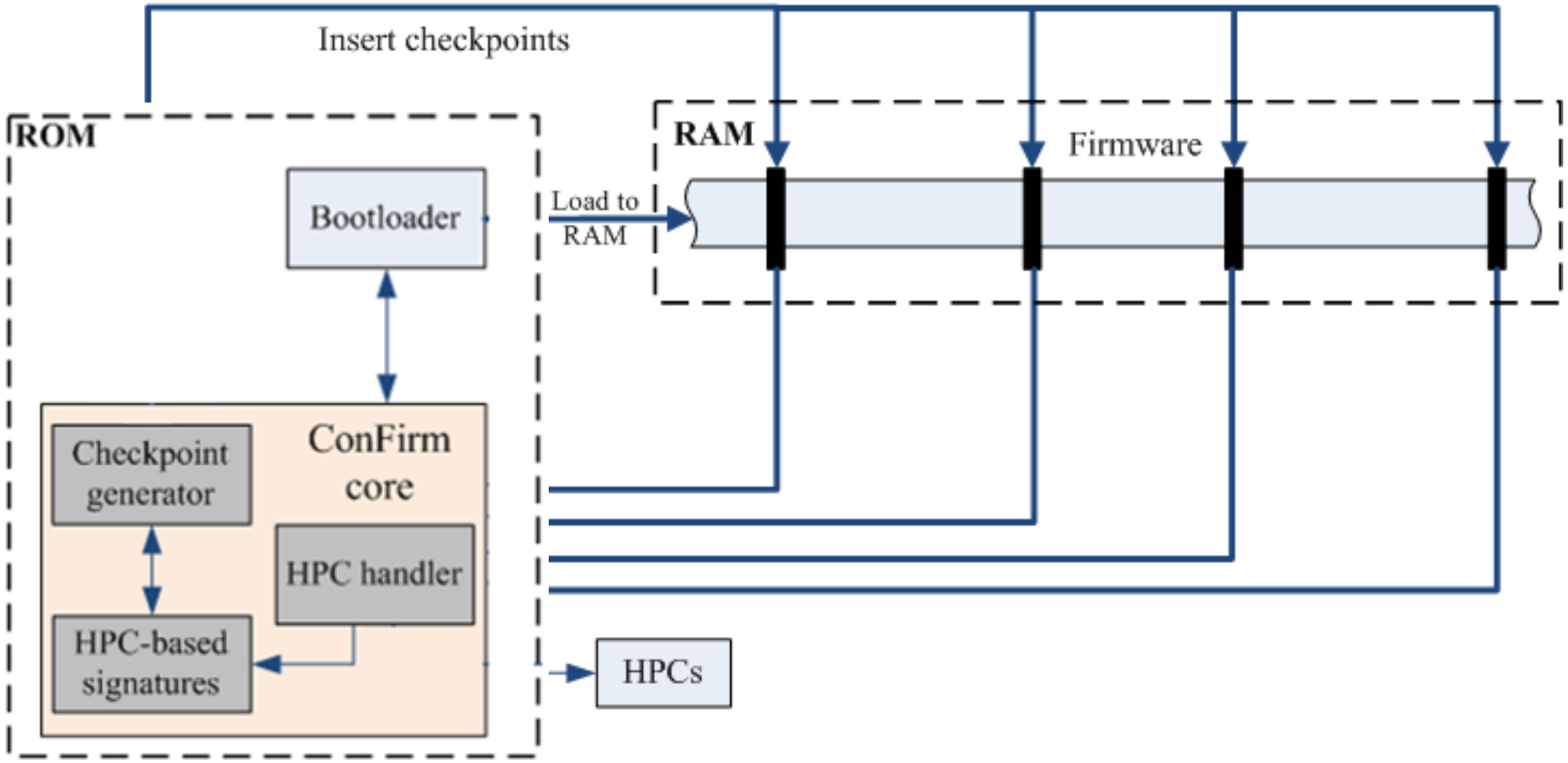


cmpwi r29, 0x10

cmpwi r29, 0x0A

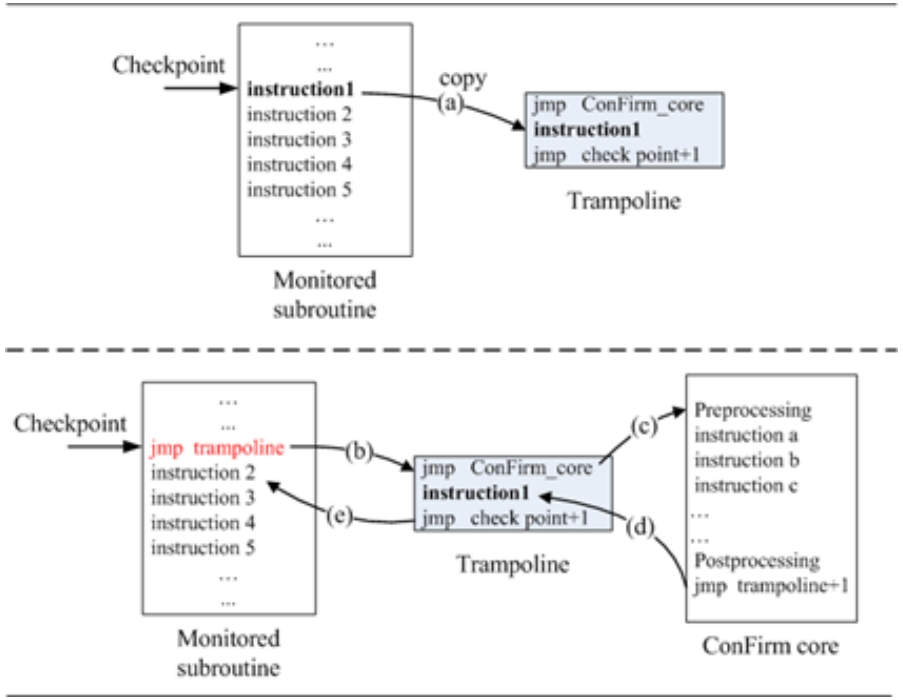
ConFirm

- High level structure

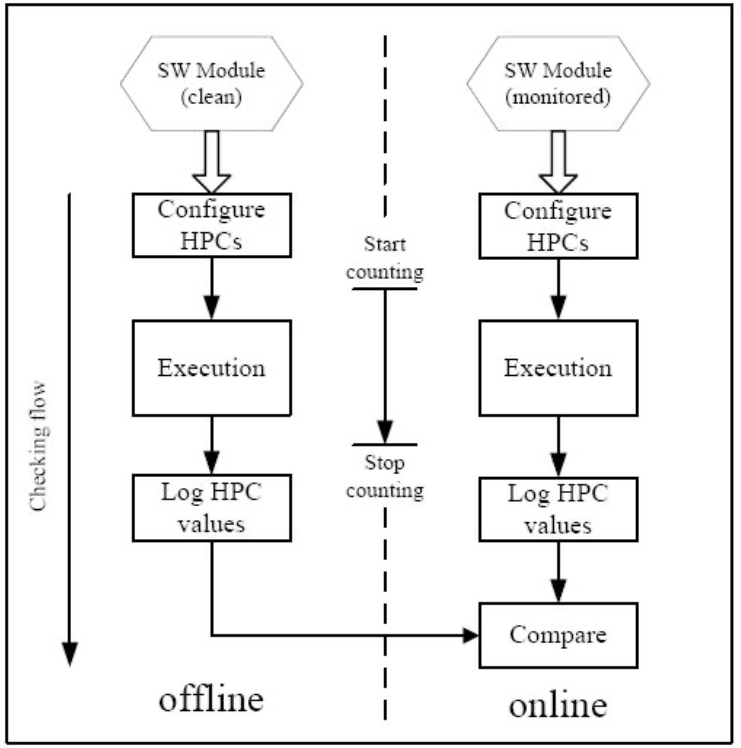


Checkpoints & Detection

- Checkpoint insertion: Inline hooking & randomization



- Two-phase detection:
  - Deviation of P_{test} from P_{ref_y} on event E_x



Devices & Events Selection

- Platform 1:
  Wireless Access Point
  ARM Cortex A15
  - 6 HPCs
  - 70 hardware events
- Platform 2: Recloser Controller
  PowerPC e300c3
  - 4 HPCs
  - 40 hardware events

Hardware event	C.V (%)
BRANCH instruction executed	0.72
INSTRUCTION architecturally executed	0.93
RETURN instruction speculatively executed	1.07
STORE instruction speculatively executed	1.27
LOAD instruction speculatively executed	1.27
Average over all tested events (∼70)	**18.9**

Hardware event	C.V (%)
BRANCH instruction completed	1.05
Completed INSTRUCTION	1.13
LOAD micro-ops completed	1.59
STORE micro-ops completed	1.78
BRANCH instruction MISPREDICTED	2.35
Average over all tested events (∼40)	**16.7**

Devices & Events Selection & Attacks

- Platform 1:
  Wireless Access Point
  ARM Cortex A15
  - 6 HPCs
  - 70 hardware events
- Platform 2: Recloser Controller
  PowerPC e300c3
  - 4 HPCs
  - 40 hardware events

- Platform 1:
  - Denial of Service (DoS)
    Adding a function hook to the subroutine: checkTaskSwitch()
- Platform 2:
  - Man-in-the-Middle
    Targeting the Ethernet packet receiving subroutine: tfEtherRecv()

Technical contributions

I. The design of a host-based validation tool that leveraged existing hardware features (HPCs) to detect malicious modifications in embedded systems firmware.

II. The implementation of a prototype on ARM- and PowerPC-based embedded platforms.

III. The feasibility of the technique was demonstrated with two real-world firmwares and attacks.

IV. The performance and storage overhead on the monitored system were also evaluated.

Historical contributions

1. One of the early works of HPCs for system security (most HPC security work is after 2015*)
2. The first work to introduce HPCs for securing the firmware of embedded systems
3. The first contribution of evaluating HPC-based security on real-world firmwares used in embedded devices of critical infrastructure

Hardware-based security solutions were not applied to embedded systems before this work
(due to the overlooked security risk in embedded systems and high deployment costs for hardware modifications)

***[Das et al.'19]** "SoK: The challenges, pitfalls, and perils of using hardware performance counters for security" IEEE Symposium on Security and Privacy (SP) 2019.

Historical contributions

< 2015

>=2015

TABLE III: Analysis of security papers using HPCs

Application		Authors	Non-determinism acknowledged	Non-determinism challenges addressed	Measurement error addressed	Recommend using HPCs
Exploit	2012	Xia *et al.* [80]	○	×	×	●
	2011	Yuan *et al.* [81]	○	×	×	●
	2016	Aweke *et al.* [82]	○	×	×	●
	2014	Zhou *et al.* [77]	○	×	×	●
	2015	Pfaff *et al.* [32]	○	×	×	●
	2016	Torres & Liu [83]	○	×	×	●
	2016	Wang & Backer [78]	○	×	×	●
	2018	Das *et al.* [79] ∗	○	×	×	●
	2015	Herath & Fogh [84]	○	×	×	●
Malware	2013	Demme *et al.* [5] †	○	×	×	●
	2014	Tang *et al.* [6] ∗	○	×	×	●
	2013	Wang & Karri [4]	○	×	×	●
	2014	Bahador *et al.* [85]	○	◑	◑	●
	2016	Wang & Karri [86]	○	×	×	●
	2014	Kazdagli *et al.* [87] †	○	◑	◑	●
	2016	Wang *et al.* [88]	○	×	×	●
	2015	Garcia-Serrano [89]	○	×	×	●
	2017	Zhang *et al.* [90]	○	×	×	●
	2017	Singh *et al.* [76] ∗	○	×	×	●
	2016	Jyothi *et al.* [91]	○	×	×	●
	2017	Patel *et al.* [92]	○	×	×	●
	2016	Peng *et al.* [93] ∗	○	×	×	●
Side-channel Attack	2012	Martin *et al.* [94]	○	×	×	●
	2008	Uhsadel *et al.* [95]	○	×	×	●
	2015	Bhattacharya & Mukhopadhyay [96]	○	×	×	●
	2016	Chiappetta *et al.* [97]	○	×	×	●
	2018	Maurice *et al.* [98]	○	×	×	●
	2015	Hunger *et al.* [99]	○	×	×	●
	2016	Gruss *et al.* [100]	○	×	×	●
	2016	Payer [101]	○	×	×	●
	2016	Zhang *et al.* [102]	○	×	×	●
	2015	Nomani & Szefer [30]	●	●	○	●
	2017	Gulmezoglu *et al.* [103]	○	◑	◑	●
	2017	Irazoqui [29]	●	●	○	●
	2017	Allaf *et al.* [104]	○	×	×	●
Firmware Verification	2015	Wang *et al.* [105]	○	×	×	●
	2016	Wang *et al.* [106]	○	×	×	●
Integrity Checking	2011	Malone *et al.* [28]	●	●	○	●
	2017	Bruska *et al.* [107]	○	×	×	●
Virtual Machine Introspection	2012	Vogl & Eckert [108]	○	×	×	●
Vulnerability Analysis	2015	Copos & Murthy [31]	●	●	◑	●

●Yes ○ No × Not Applicable based on column 3 ◑ Respondent's answer inconsistent with description provided in the paper ∗ Windows † Android
Others: Linux

1) Early works of HPCs for system security

2) First work of HPCs for firmware verification/security

3) First work of repurposing existing hardware in embedded systems for security

[Das et al.'19] "SoK: The challenges, pitfalls, and perils of using hardware performance counters for security" IEEE Symposium on Security and Privacy (SP) 2019.

Potential for Long-Term Impact (1/5)

Enabling HPC-based monitoring for safety and security of cyber-physical systems (CPS) in multiple sectors

- Following our work, there has been a line of research on using HPCs for detecting security compromise and safety- related system failures in CPS
    - [Krishnamurthy *et* al.'19] proposed using HPC measurement to perform real-time monitoring of software running on embedded processors in CPS
    - [Carelli *et* al.'19] studied how HPCs can be reused to enhance the safety of a CPS in automotive, aerospace, civil infrastructures, and healthcare sectors
    - [Kadiyala et al.'20] investigated the utility of multiple cores in embedded CPS from the point of view of security, where one of the cores operate as a watchdog measuring metrics of HPC values
    - [Patel et al.'20] presented how on-chip temperature sensors allows robust real-time monitoring of the processor behavior in CPS

[Krishnamurthy et al.'19] "Anomaly detection in real-time multi-threaded processes using hardware performance counters," IEEE TIFS, 2019.
[Carelli et al.'19] "Performance monitor counters: interplay between safety and security in complex cyber-physical systems," IEEE Transactions on Device and Materials Reliability, 2019.
[Kadiyala et al.'20] "LAMBDA: Lightweight Assessment of Malware for emBeddeD Architectures," ACM Transactions on Embedded Computing Systems (TECS), 2020.
[Patel et al.'20] "Towards a new thermal monitoring based framework for embedded CPS device security," *IEEE Transactions on Dependable and Secure Computing,* 2020.

Potential for Long-Term Impact (2/5)

Using HPCs to detect different types of attacks

- Our work of re-purposing HPCs for detecting firmware modifications has inspired researchers to explore the feasibility of using HPCs for detecting advanced attacks such as ROPs, ransomware, and side-channels
  - [Zhang *et* al.'16] demonstrated how HPCs can detect, and hence mitigate, cache-based side-channel attacks in multi-tenant cloud systems
  - [Alam *et* al.'17] presented a novel approach for detecting micro-architectural side-channel-attacks by profiling low-level hardware events using HPCs
  - [Das *et* al.'18] leveraged HPCs to measure the mis-predicted return events to detect ROP attacks at runtime
  - [Dinakarrao, et al.'19] showed how to predict adversarial HPC pattern for a given application to be misclassified by deployed ML classifiers
- Given that attacks are evolving, there is a potential for improving HPC-based detection/prevention of new attacks

[Zhang, et al.'16] "CloudRadar: A Real-Time Side-Channel Attack Detection System in Clouds," RAID, 2016.
[Alam, et al.'17] "Performance counters to rescue: A machine learning based safeguard against micro-architectural side-channel-attacks." IACR Cryptol. 2017.
[Das, et al.'18] "Ropsentry: Runtime defense against rop attacks using hardware performance counters," Computers & Security, 2018.
[Dinakarrao, et al.'19] "Adversarial Attack on Microarchitectural Events based Malware Detectors," DAC, 2019.

Potential for Long-Term Impact (3/5)

Exploring the feasibility of using other existing hardware components for security

- Our research on re-using readily built-in HPCs for security also triggers ideas of exploring other existing hardware components for security
  - Modern computer systems, including embedded systems, nowadays provide various of on-chip sensors to report real-time status of the system
    - E.g., thermal sensors, voltage/frequency interfaces
  - Similar to HPCs, these on-chip sensors' reading may also correlated to the behavior of the programs running on the platform
    - [Karabacak et al.] detected unauthorized activity by processing electromagnetic emissions on hardware
    - [Patel *et* al.] used thermal information to profile embedded processors, to detect malicious changes due to software and hardware attacks, and altered processors

[Karabacak et al.'18], "Remote detection of unauthorized activity via spectral analysis," ACM Transactions on Design Automation of Electronic Systems (TODAES), 2018.
[Patel et al.'20], "Towards a new thermal monitoring based framework for embedded cps device security," IEEE Transactions on Dependable and Secure Computing, 2020.

Potential for Long-Term Impact (4/5)

Can HPCs be abused as a security backdoor?

- While HPCs are a new channel for monitoring malicious behavior of a program, they also open an avenue for attackers: HPCs might be abused as a backdoor
- Related research efforts:
  - [Spisak'16] introduced a hardware-assisted rootkit on both the ARM and Intel x86-64 architectures. The rootkit allows an attacker to redirect control flow to malicious code by leveraging HPCs to count specific architectural events
  - [Alam *e*t al.'19] presented a micro- architectural side-channel attack by analyzing HPC counts during the execution of an encryption algorithm
  - [Dinakarrao, et al.'19] employed an adversarial sample predictor to determine the HPC count to get misclassified

[Spisak'16] "Hardware-assisted rootkits: Abusing performance counters on the {ARM} and x86 architectures," in USENIX WOOT, 2016.
[Alam et al.'19] "Ipa: an instruction profiling–based micro-architectural side-channel attack on block ciphers," Journal of Hardware and Systems Security, 2019.
[Dinakarrao, et al.'19] "Adversarial Attack on Microarchitectural Events based Malware Detectors," DAC, 2019.

Potential for Long-Term Impact (5/5)

Can HPCs for security monitoring be utilized in the next-generation of embedded systems

- We paved the utilization of such hardware-based solution in real-time industrial environments, and specifically in cyberattack scenarios to the electric grid [ConEdison, DARPA RADICS, DARPA SHEATH].
  - ConEdison: Confirm was built by funding from ConEdison (one of the largest investor-owned energy companies in the United States)
  - RADICS: funded by a $7.3M award from DARPA, ConFirm is expected to be deployed in next-generation embedded systems used in power systems (SRI, NYU, ConEdison)
  - SHEATH: ConFirm is used in the identification and demonstration of real-time detection against malicious code installed in complex COTS circuit boards

[RADICS] "Rapid Attack Detection, Isolation and Characterization Systems (RADICS)," [Online]: http://www.darpa.mil
[SHEATH] "Microsystems Exploration: Safeguards against Hidden Effects and Anomalous Trojans in Hardware (SHEATH)," [Online]: http://www.darpa.mil
[SRI] "SRI International to lead program to develop tech- nology for restoring power to a grid facing a cyberattack)," [Online]: https://americansecuritytoday.com/tigr-project-technology-restoring-power-grid-cyberattack/

Conclusions

- Overall:
  - ConFirm core resides in the boot ROM, thus is difficult to be detected or disabled by an adversary
  - The monitoring can be instrumented within any firmware regardless of its functionality
  - Directly utilizing the hardware features of the host platform, bypassing the overhead associated with the software layers

- The ConFirm team explored a new direction for hardware-based security solution in embedded systems by reusing hardware features that were designed for other purposes
- The ideas of ConFirm are expected to be used the protect critical infrastructures around the world

Thank you!

Questions?

ckonstantinou@fsu.edu