Mixed-Granular Architectural Diversity for Device Security in the Internet of Things

AsianHOST Symposium
October 19, 2017

Robert Karam[1], Tamzidul Hoque[2], Kevin Butler[2], and Swarup Bhunia[2]

[1] Dept. of CSE, University of South Florida (Tampa, FL, USA)
[2] Dept. of ECE, University of Florida (Gainesville, FL, USA)

Email: rkaram@usf.edu

USF
UNIVERSITY OF SOUTH FLORIDA
COLLEGE OF ENGINEERING

UF
UNIVERSITY of FLORIDA

Outline

- Introduction
- Background
  - Existing vulnerabilities / break one, break all
  - Software-based “security through diversity”
- Our Contribution
  - Security through Architectural Diversity
  - uC Diversification Techniques
- Security Analysis
- Conclusion

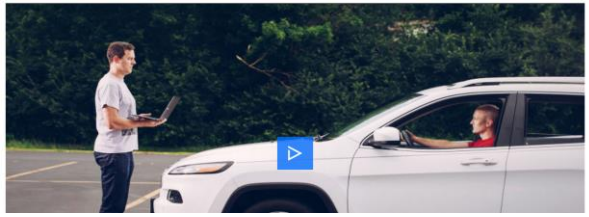
Introduction

- Security can be more challenging for IoT devices
  - Remote/in-field reconfiguration/firmware updates
  - Long in-field lifetimes
- Device size, weight, performance, battery life…
- Increasing importance of lightweight & robust security for IoT
- Encryption is strong, but not a silver bullet solution
  - Susceptible to various physical/side channel attacks
  - Attacking implementation rather than algorithm
  - Attacking protocol (WPA!?)

Introduction

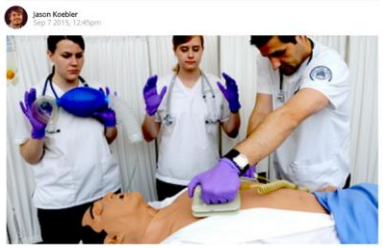
- Recent attacks highlight deficiencies in existing approaches

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



July 2015

Hackers Killed a Simulated Human By Turning Off Its Pacemaker



Some humans are already hackable, and, yes, you can do some serious damage by compromising medical implants.

September 2015

TECHNOLOGY NEWS | Tue Oct 4, 2016 | 3:58pm EDT

J&J warns diabetic patients: Insulin pump vulnerable to hacking

October 2016

21 Hacked Cameras, DVRs Powered Today's Massive Internet Outage

OCT 16

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked "Internet of Things" (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet's top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.

October 2016

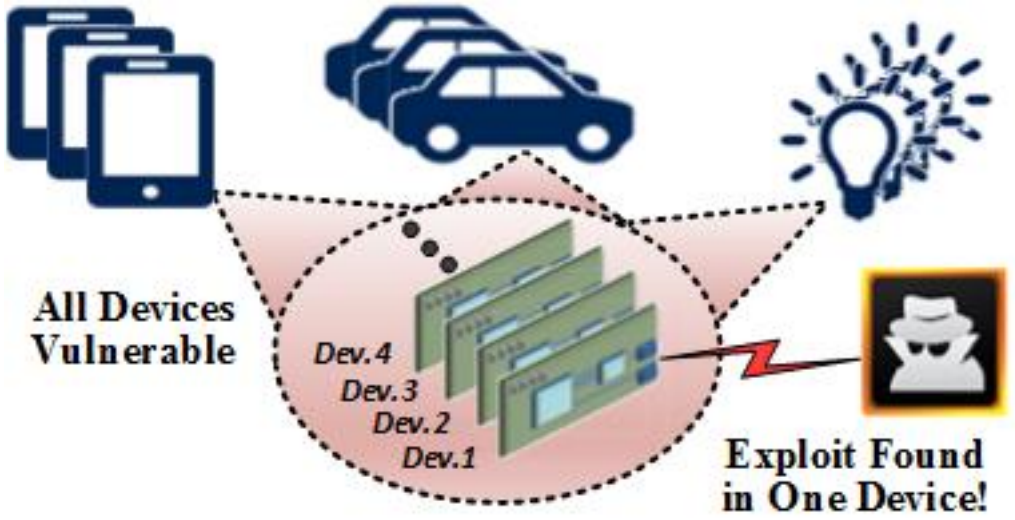
January 2017

May 2017

Hardware Homogeneity

- Identified as a root enabler of many attacks
- $$$ Economic motivation $$$
  - Expend effort on breaking one device
  - All devices with the same
    - IP
    - Chip
    - Board
    - Algorithm
    - Protocol
    - …

  are susceptible



Analogies from Nature

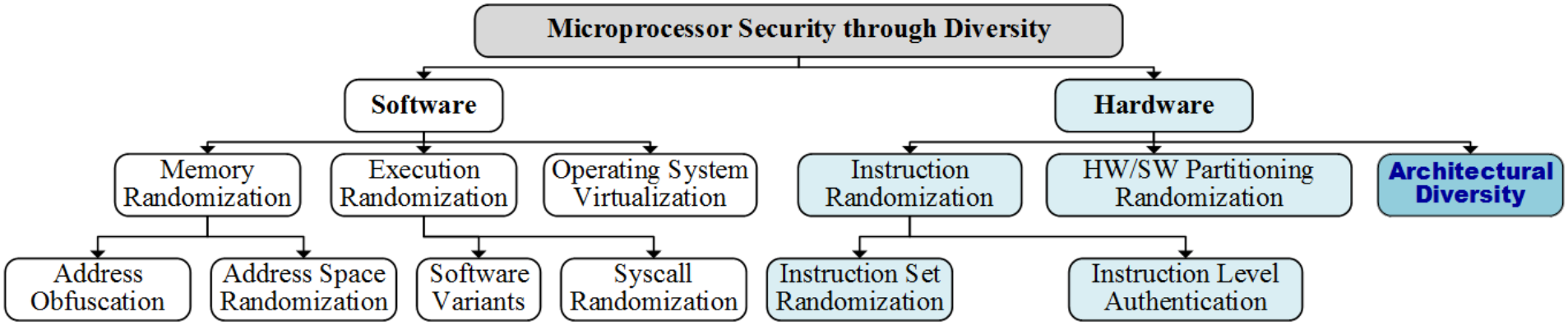
- Monocultures in nature (Wikipedia)
  - Producing or growing a single crop, plant, or livestock species, variety, or breed in a farming system at a time. [It] has allowed increased efficiency in planting and harvest.
  - Continuous monoculture…can lead to the quicker buildup of pests and diseases, and then rapid spread where a uniform crop is susceptible to a pathogen.
  - The practice has been criticized for its environmental effects and for putting the food supply chain at risk.
- Monocultures in computer science (Wikipedia)
  - A community of computers that all run identical software.
  - All systems in the community thus have the same vulnerabilities, and, like agricultural monocultures, are subject to catastrophic failure in the event of a successful attack.

Attack Vectors in IoT

- Firmware reverse engineering
  - Binutils
  - FRAK
  - DynamioRIO
- Targeted malicious modification
  - Intelligent modification of firmware
  - Bypassing digital signatures / checksums
- Malware propagation
  - Exploits in Remote Firmware Update utilities
  - Autonomous propogation of malicious firmware on network

Diversity as a Security Measure

- Diversity has been applied to computers to some degree…
  - Software: memory/execution randomization
  - Operating system virtualization
- More recently applied to hardware
  - Instruction randomization (w/ HW support)
  - HW/SW partitioning (SoC w/ FPGA) randomization
  - “Mutable” FPGA architectures

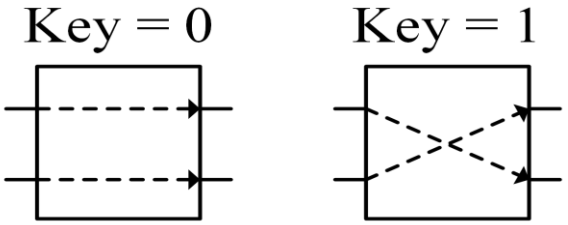


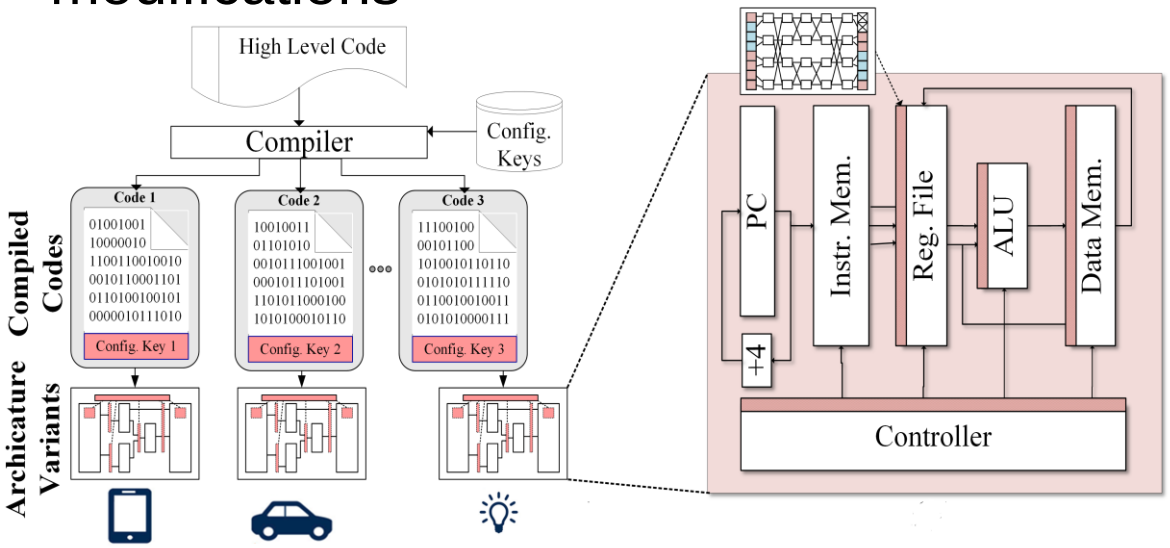
Diversity in Microcontrollers

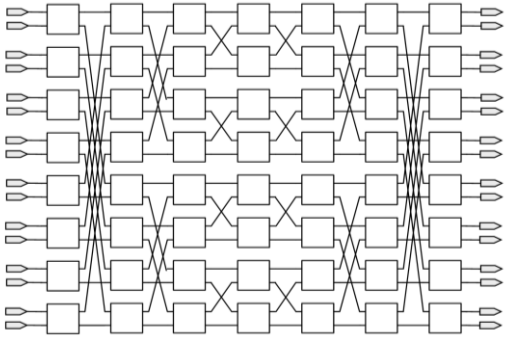
- Instruction randomization
  - Encryption/decryption in cache
  - Instruction Level Authentication (ILA)
- Shortcomings of existing techniques
  - Generally high overhead
  - Potential reliability issues
  - Same underlying ISA → Code Reuse Attacks
- We propose **mixed-granular architectural diversity**
  - Decentralized: distributed throughout functional units in uC
  - Tunable/Adjustable: meet security & design goals
  - Moving target defense: time-varying obfuscation in hardware

Mixed-Granular Diversity in Hardware

- Mixed fine/coarse-grained modifications realized with reconfigurable Benes network to obfuscate functionality
- Hardware-enabled node locking requires device-specific firmware modifications







Examples of Mixed-Granularity

- Fine-grained (decentralized)
  - Intra-instruction permutations
  - E.g. Inputs to register file (address and/or data)
  - E.g. Inputs to functional units (adder, multiplier, etc.)
- Coarse-grained (centralized)
  - Inter-instruction permutation
  - Order of instructions in cache line
  - Order of bytes in cache line
- Inter- and Intra- instruction permutations ensure firmware runs correctly only on target device
- Required modifications to the binary can be done post-compilation and are correct by construction

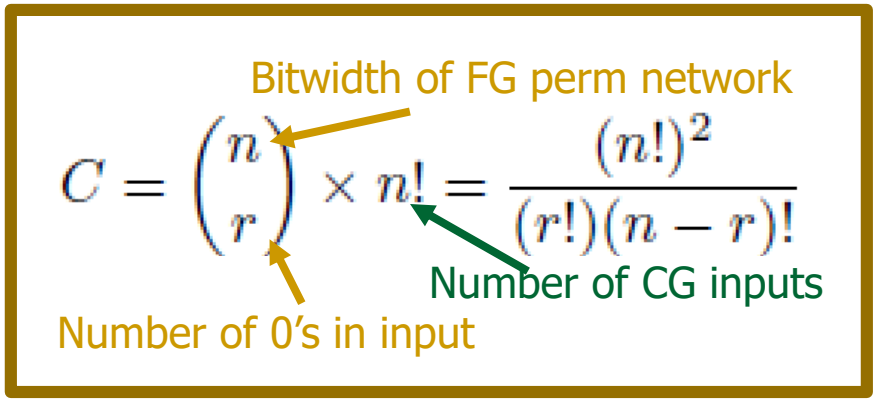
OpenRISC OR1200 CPU Prototype

- Prototype simulated with OpenRISC CPU base
- 2xFG perm networks, 1xCG perm network
  - Permuting bits from top and bottom halves of instruction word
  - Permuting 16x8-bit chunks from 4 instructions in 128-bit cache line
- Low area/power overhead (1.3%, 3.8%
- Latency overhead
  - Depends on placement (internal/decentralized, external/centralized)
  - External placement outside critical path, no latency overhead
  - Internal placement, leverage timing slack to minimize overhead

Component	Area (um^2)	Power (uW)
Fine Grained Permutation Networks	2600	19
Coarse Grained Permutation Network	10625	79
8kB I-Cache & D-Cache	820000	1529
OR1200 (Original)	1020000	2629
OR1200 (Modified)	1033214	2727
Overhead	**1.30%**	**3.80%**

Security Analysis

- Benes network permuting binary strings requires special consideration
  - Potential for many-to-one mappings depending on #(0) and #(1)
  - Binomial coefficient can enumerate all possible & average brute force complexity
- Ideal encoding has ~equal #(0) and #(1)
  - Designing ISA w/ balanced #(0) and #(1)
  - Compiler support for selecting certain registers to balance 0/1



- E.g. 2x16x1-bit FG networks w/ ~8x1's / input & 1x16x8-bit CG network, chance of compiling valid code w/o knowledge of network config < 1 in 10^{20}

Effect of Key Size & Bits per Switch

- 1 key bit per switch can realize any well-defined permutation
- 2 key bits per switch enables upper- and lower-broadcasting
  - Upper input propagates to both outputs
  - Lower input propagates to both outputs
- 2 bits per switch non-linearly transforms IN → OUT encoding (stronger against template matching) and increases brute force complexity

Thank You!

Questions?

Email: rkaram@usf.edu