IDA

Institute for Defense Analyses

4850 Mark Center Drive • Alexandria, Virginia 22311-1882

Cyber Physical Systems: Why Hardware Matters

Brian S. Cohen

ASQ Collaboration on Quality in the Space and Defense Industries Conference

Cape Canaveral, FL | March 11, 2019

IDA | Why Hardware Security Matters

- Current and future platforms will contain chips with billions of transistors
  - Hardware is now widely recognized as being a key source of vulnerabilities
- Hardware has challenges around resilience
- It is expensive to “replace it” and difficult to “fix it with a patch”
  - Most hardware cannot be fixed in operation
  - This is especially true for space platforms
- We need formalisms for security in specifications that are able to be a part of our quality practices, which currently, depend on “conformance”
- Vulnerabilities (in hardware and software) may be
  - Accidents in design and manufacture
  - Deliberate “features” of design and manufacture
  - Deliberately placed or exploited by an adversary
- Security and vulnerabilities often fall outside of typical quality and reliability engineering considerations

Phobos-Grunt Downed by Bad Chips?

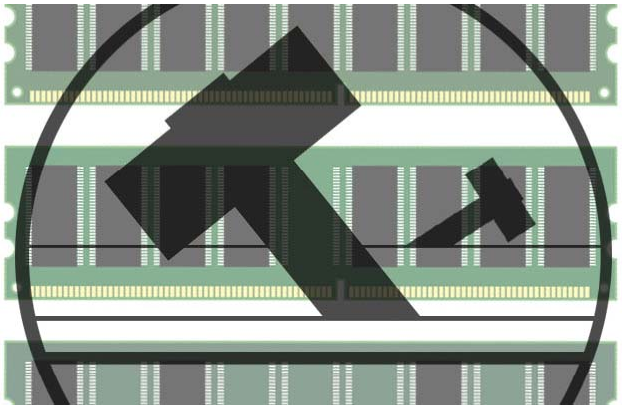
- Fell to Earth on 15 January 2012 [1]
  - "Failure mechanism attributed to the simultaneous disabling of two identical chips in the dual-computer control system, causing both to restart simultaneously."
  - "… the specific component identified in the report as the likely locus of the double-hardware failure—the WS512K32, which is a single-package assembly of SRAM totaling 512 kilobytes"
  - Press reports suggest that investigators thought the chip failures were a result of counterfeit components—lesser circuits labeled with higher performance qualities.
  - "Roskosmos has blamed supposedly counterfeit chips for a plague of on-orbit breakdowns.
    - A Proton booster carrying three GLONASS navigation satellites crashed late in 2010.
    - A year earlier, … four GLONASS satellites broke down. The newspaper Izvestiya reported on 12 August 2011 that Moscow concluded that the failure was due to shoddy chips from Taiwan that weren't radiation hardened."
- If you cannot trust your supplier to deliver products that contain quality, uncompromised, or invulnerable products, then who can you trust?
- Testing for vulnerabilities at the platform level is a losing proposition.

Photo: ROSCOSMOS/EPA/Landov
Waiting its Turn: The Phobos-Grunt probe before being loaded onto a rocket for launch on its failed trip to Mars.

[1] *Did Bad Memory Chips Down Russia's Mars Probe? Moscow blames radiation wreckage on an SRAM chip, but does it add up?*, James Oberg, IEEE Spectrum, February 2012

IDA | Rowhammer

- Rowhammer – “a method for repeatedly hammering on rows of cells of memory in DRAM devices to induce cells to flip from one state to another” [2]
  - In 2015, Google researchers used Rowhammer “to produce these bit flips in cells and gain kernel-level privileges” [2]
- A Rowhammer attack has been demonstrated on an Android phone [3]
  - The exploit, dubbed Glitch, flips bits in the dynamic memory on the phone in less than two minutes
  - Although it isn’t mature enough to be an immediate threat, it could in the future pose a broad and serious risk



[2] *Rowhammer Hardware Exploit Poses Threat to DRAM Memory in Many Laptops, PCs*, Dennis Fisher, ThreatPost, March 2015

[3] Drive-by Rowhammer attack uses GPU to compromise an Android phone, Dan Goodin, Ars Technica, May 3, 2018

What is Hardware Assurance (HwA)?

- The level of confidence that microelectronics (also known as microcircuits, semiconductors, and integrated circuits, including its embedded software and/or intellectual property) function as intended and are free of known vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system's hardware and/or its embedded software and/or intellectual property, throughout the life cycle [4]
- Hardware Assurance is like System Assurance and Software Assurance: It focuses on an engineering goal so you can “build in” security instead of trying to “test it in.”

[4] *Defense Acquisition Guidelines (DAG) Chapter 9 (Program Protection Planning), Section 3.2.4*

IDA | Summary

- Engineering assured cyber physical systems requires at least the following:
  - A system engineer
  - Software assurance
  - Hardware assurance
- We need to build security and assurance into the hardware for unmanned aerial vehicle (UAV), space, and other key applications
  - We can't just "test it in" or try to "recover" from exploitation
- In the future, we will need to harmonize and integrate the quality, safety, and cyber security disciplines
- And most of all, we need to collaborate on standards that address things in a broad manner rather than a stove piped manner

IDA

Institute for Defense Analyses

4850 Mark Center Drive • Alexandria, Virginia 22311-1882

Questions?

For a copy of this presentation contact

Brian S. Cohen

703-845-6684, bcohen@ida.org