

RSA®Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: SPO2-W03

What Happens to Your Threat Model When Hardware Isn't Really Hardware?

Lorie Wigle

VP, Software and Services Group
Intel Corporation

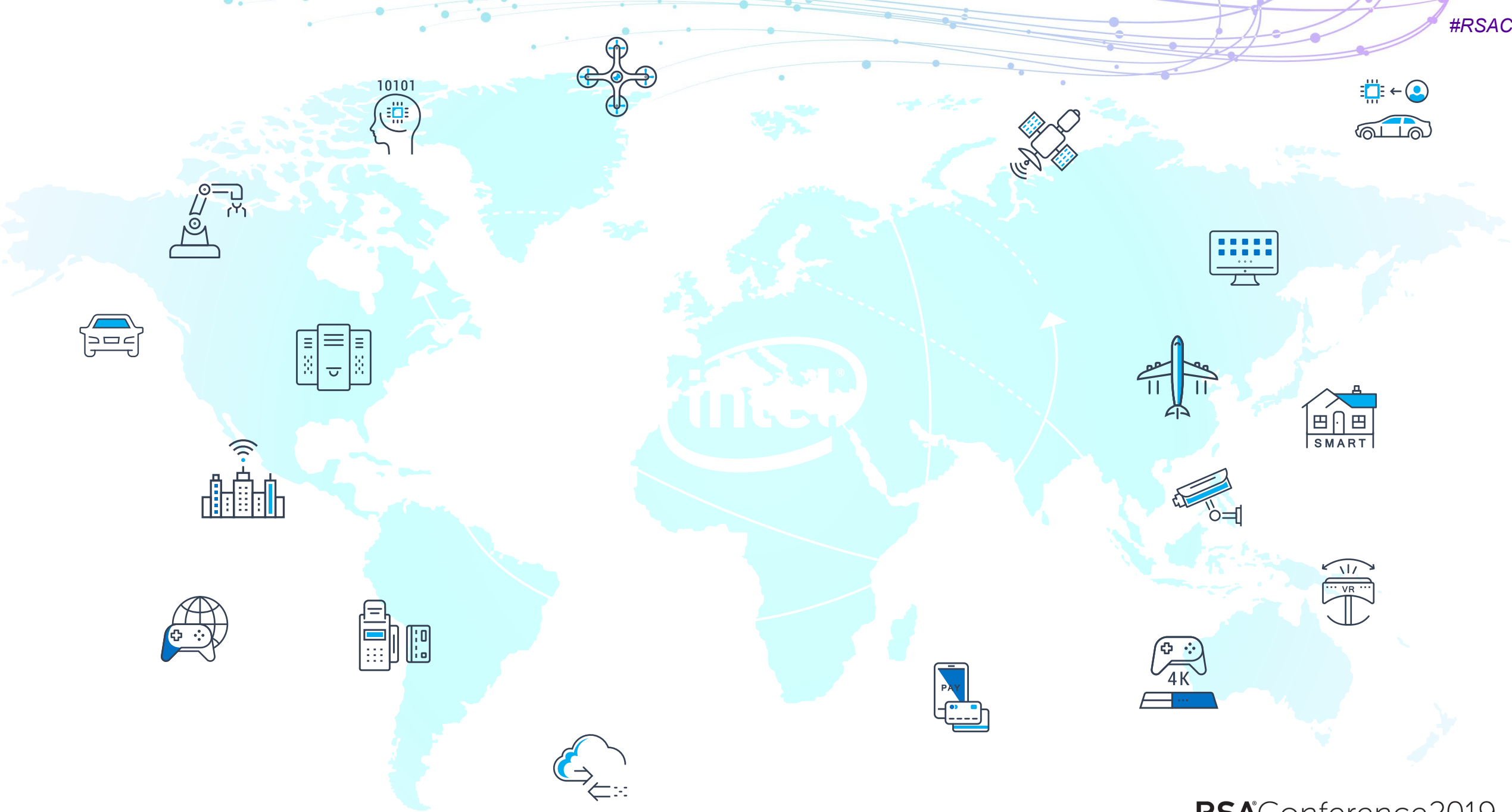
Twitter: @LWigle



#RSAC

Agenda

- Security-sensitive organizations have a solid grasp software security update tradeoffs
- Hardware security isn't evaluated with same mindset
- Hardware refresh plans should be considered as part of the initial purchasing criteria and TCO



Balancing service vs security needs



Security sensitive organizations spend a lot of time evaluating risk tolerance when considering **software security update** time-to-deploy.

When it comes to hardware, the analysis on refresh is generally based on total cost of ownership, availability of features, mechanical failure or anticipated life span.

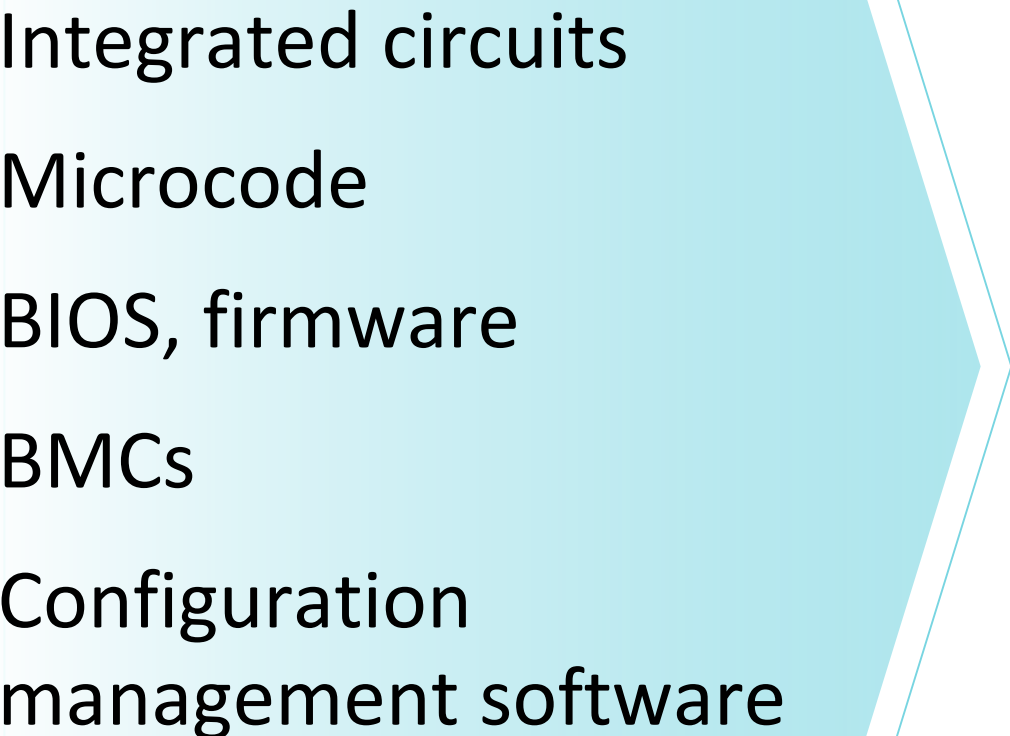
Major security incidents are now pushing security considerations to the front-burner

Today's hardware upgrade calculations

- Equipment failure
- Higher quality video feeds, storage upgrades, improved connectivity.
- Evolutions in functionality



Hardware doesn't exist in a vacuum

- 
- Integrated circuits
 - Microcode
 - BIOS, firmware
 - BMCs
 - Configuration management software
- Software vulnerabilities need to be managed
 - Does it have a mature patching mechanism?
 - Does it contain anti-tampering mitigations?

Hardware risks are often overlooked

NEWS

IoT botnets target enterprise video conferencing systems

WootCloud researchers have discovered a trio of IoT botnets based on Mirai that exploit Polycom video conferencing systems. Polycom has issued an advisory and best practices for mitigating the risk.



By **Lucian Constantin**

Romania Correspondent, CSO | FEBRUARY 20, 2019 11:00 AM PT

ENDPOINT

3/8/2017
08:45 AM

Why Printers Still Pose a Security Threat



Kelly Sheridan
News

Connect Directly



0 COMMENTS
[COMMENT NOW](#)

Newly discovered security flaws in popular printers remind us how networked devices continue to put users at risk.

Networked printers for years have left gaping holes in home and office network security. Today, experts continue to find flaws in popular laser printers, which are putting businesses at risk.

Experts at the University Alliance Ruhr recently announced vulnerabilities in laser printers from manufacturers including Dell, HP, Lexmark, Samsung, Brother, and Konica. The flaws could permit print docs to be captured, allow buffer overflow exploits, disclose passwords, or cause printer damage.

Up to 60,000 currently deployed printers could be vulnerable, [they estimate](#).

Is security built into your purchasing criteria?

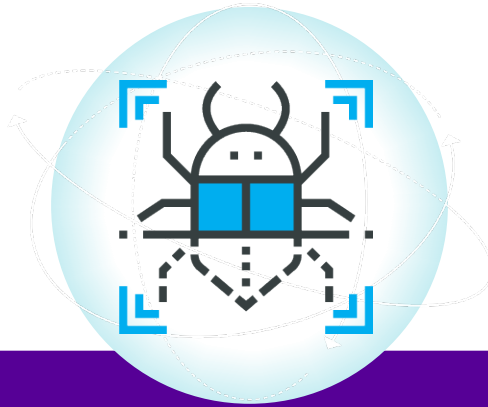
- When you buy new equipment...
 - Require a **mature update mechanism**
 - Consider **minimum hardware-based security** functionality
(e.g., secure storage, encryption support)
- Factor security measures into your **supply chain** program
- Other foundational security elements for **your threat environment**



RSA®Conference2019

Resilience and Mitigations





The technology industry is investing heavily in security. This work will provide resilience against potential future threats. The work we do today is deployed along a longer timeline than that for software.

Innovations that move the needle

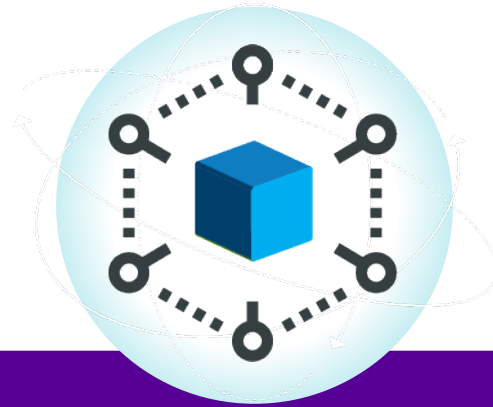
- Certified Systems by Design
- BIOS/UEFI hardening, anti-tampering technologies
- Secure Storage and Trusted Platform Modules
- Secure Elements to store secrets, keys properly on the platform and prevent leakage
- Evolutions in cryptography
- Streamlining microcode updates to ecosystem



Collaborations that move the needle

- Industry efforts
 - ARM & Intel for secure device onboarding
 - Industrial Internet Consortium
 - IETF and other SDOs
- Public/private partnerships
 - NTIA work on patching
 - NIST efforts on firmware update standards, sector-by-sector
 - TCG & NIST work on resilience





With long lifecycles in the field, this means the security work in your deployment **may not enable your organization** to take advantage of recent security investments.

Security must be a factor in hardware refresh decisions

- Security is part of TCO – including hardware
- Align advances in security to your organizations needs
 - Priority of availability may exceed confidentiality and integrity
 - Your unique business requirements and risk assessment

