Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

GENERAL NOTICE: Other entity and product names used in this publication are for identification purposes only and may be trademarks of their respective holders.

Lattice Semiconductor Corporation, Lattice Semiconductor (& design), and specific product designations are either registered trademarks or trademarks of Lattice Semiconductor Corporation or its subsidiaries in the United States and/or other countries.

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

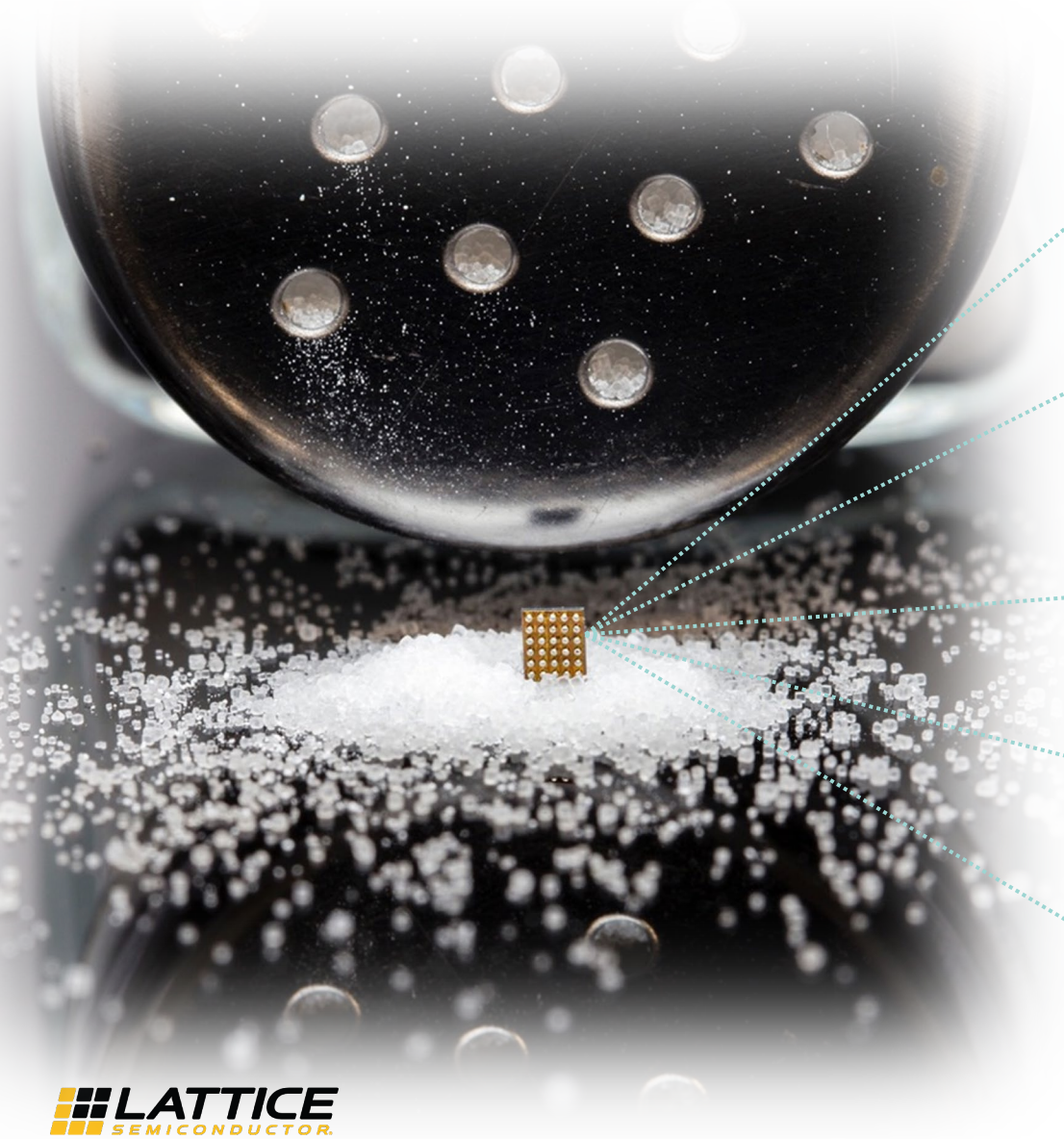
SESSION ID: PDSC-R06

Cyber Resiliency Through Firmware Protections & Supply Chain Security

Eric Sivertson

Vice President of Security Business
Lattice Semiconductor
@latticesemi

Critical Firmware Applications to Protect

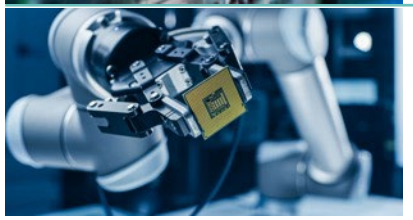


AI Inference at the Edge

Embedded Vision

Hardware Platform Security

Control & Management



Industrial Automation

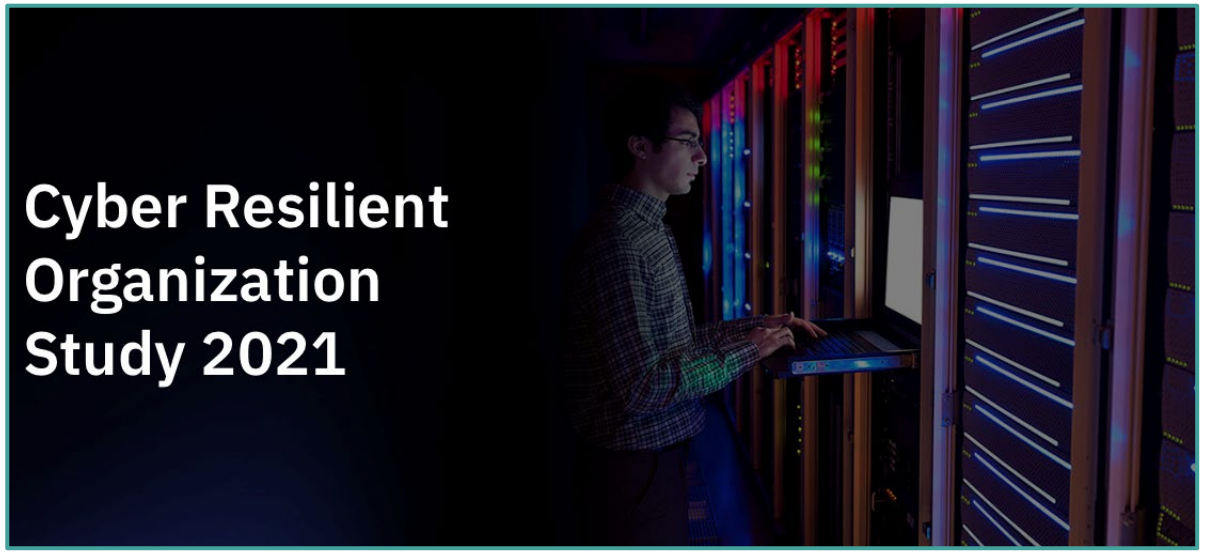
Cyber Resilience

Ability to ***continuously deliver an intended outcome***, despite adverse cyber events (i.e. attacks). This concept brings together areas of information security, business continuity and overall organizational resilience.

- Requires Strong ***Hardware Root of Trust (HRoT)*** Foundations
- Real-time ***Reactive***
- Automated ***Detect-Protect-Recover***

Cyber Resiliency Gap

- **51%** reported a significant data breach
- **61%** paid a ransom on a ransomware attack
- **74%** reported inconsistently applying their CISRP*
- **58%** remain at middle or late-middle maturity for cyber resilience
- Both ***Volume & Severity*** of cybersecurity incidents increased or significantly increased, according to **67%** of respondents
- **59%** responded that delay in patching vulnerabilities was reason cyber resiliency had not improved



The sixth annual *Cyber Resilient Organization Study* from IBM Security™ is based on research from the Ponemon Institute's survey of more than 3,600 IT and security professionals around the world in July 2021.

From: https://www.ibm.com/resources/guides/cyber-resilient-organization-study/

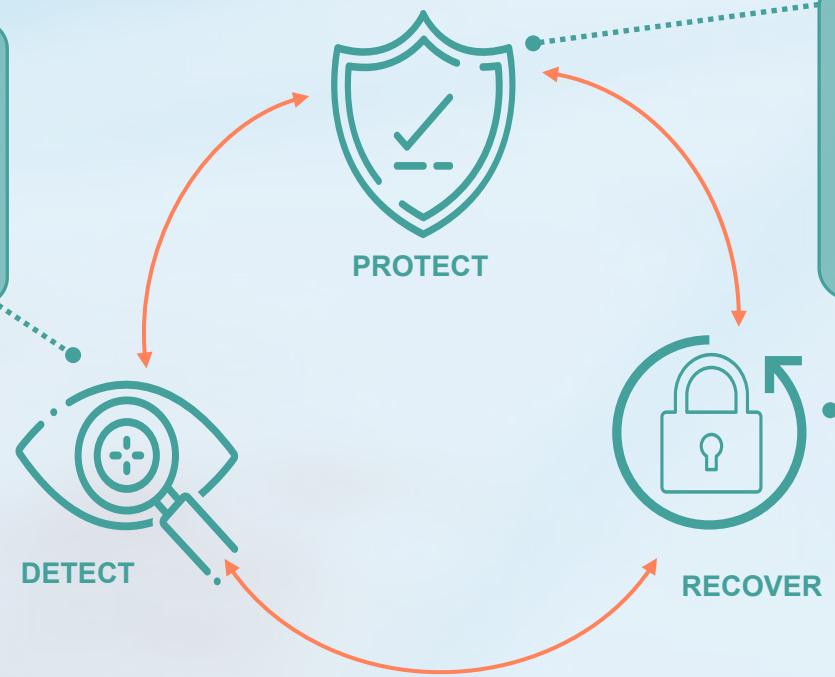
**Cybersecurity Incident Response Plan (CISPR)*

Resiliency Cycle

Platform Firmware Resiliency (PFR) Specifies Using a Hardware Root-of-Trust Device to Perform Protect, Detect & Recover Functions

DETECTION

- Cryptographically detect corrupted platform firmware & critical data
  - At Power-on
  - After In-System Updates



PROTECTION

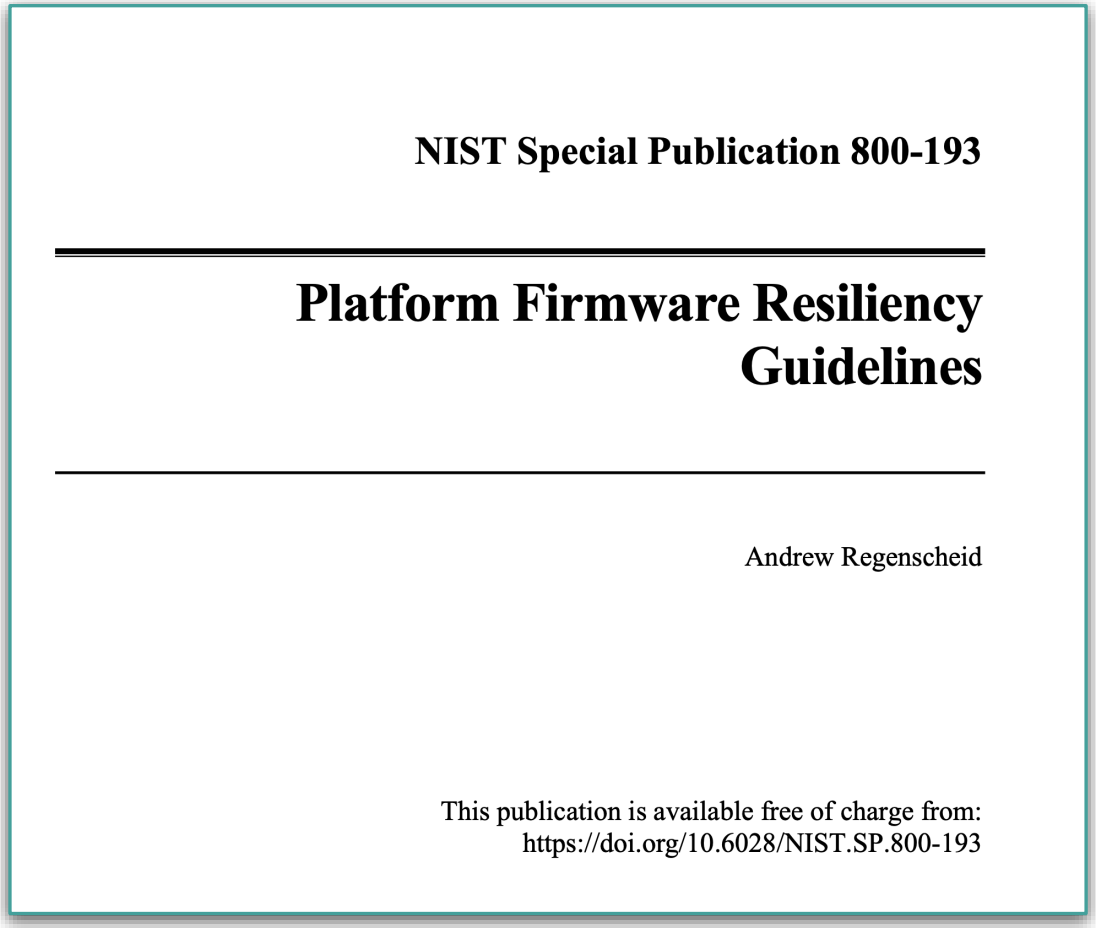
- Protect platform firmware & critical data from corruption
- Ensure authenticity & integrity of firmware updates

RECOVERY

- Restore corrupted firmware & critical data to its previous value Initiate trusted recovery process

Real-Time Resistance while being attacked

Resiliency Standards



NIST Special Publication 800-193

Platform Firmware Resiliency Guidelines

Andrew Regenscheid

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-193

TRUSTED® COMPUTING GROUP

Resources Work

Cyber Resilient Technologies

Formed in June 2018, the TCG Cyber Resilient Technology (CyRes) workgroup focuses on supporting three primary principles for resilience:

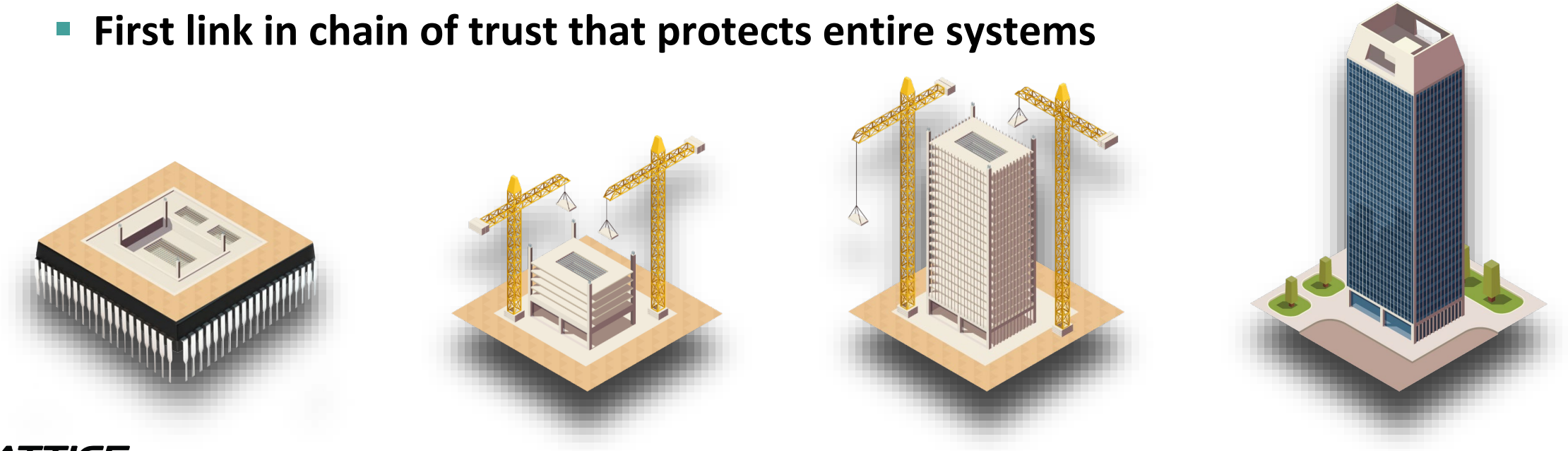
- **Protecting** updatable persistent code and configuration data
- **Detecting** when vulnerabilities are not patched or when corruption has occurred
- **Recovering** reliably to a known good state even if the platform is compromised.

Protection techniques lessen the likelihood that malware is able to persist itself and provide techniques for better protecting code and data. ***Detection*** techniques identify whether a platform is healthy and work when the device is disconnected, using standalone techniques (like secure boot), or connected, by using technologies like remote attestation. Detection involves the creation of evidence about the kind of platform and where a verifier could obtain health information. If detection identifies a problem, ***recovery*** is triggered to remedy the platform and try to return it to a functional state. Remediation could involve updating code or changing security settings.

For connected cyber resilient platforms, the protection, detection and recovery capabilities help identify misconfigured or unpatched code and reliably deploy updates. For consumer scenarios this may be done directly by the manufacturer, service provider or end user. In organizational settings, management may be done by the IT department or its delegates. Policies may be defined for recovery actions that are device and domain specific.

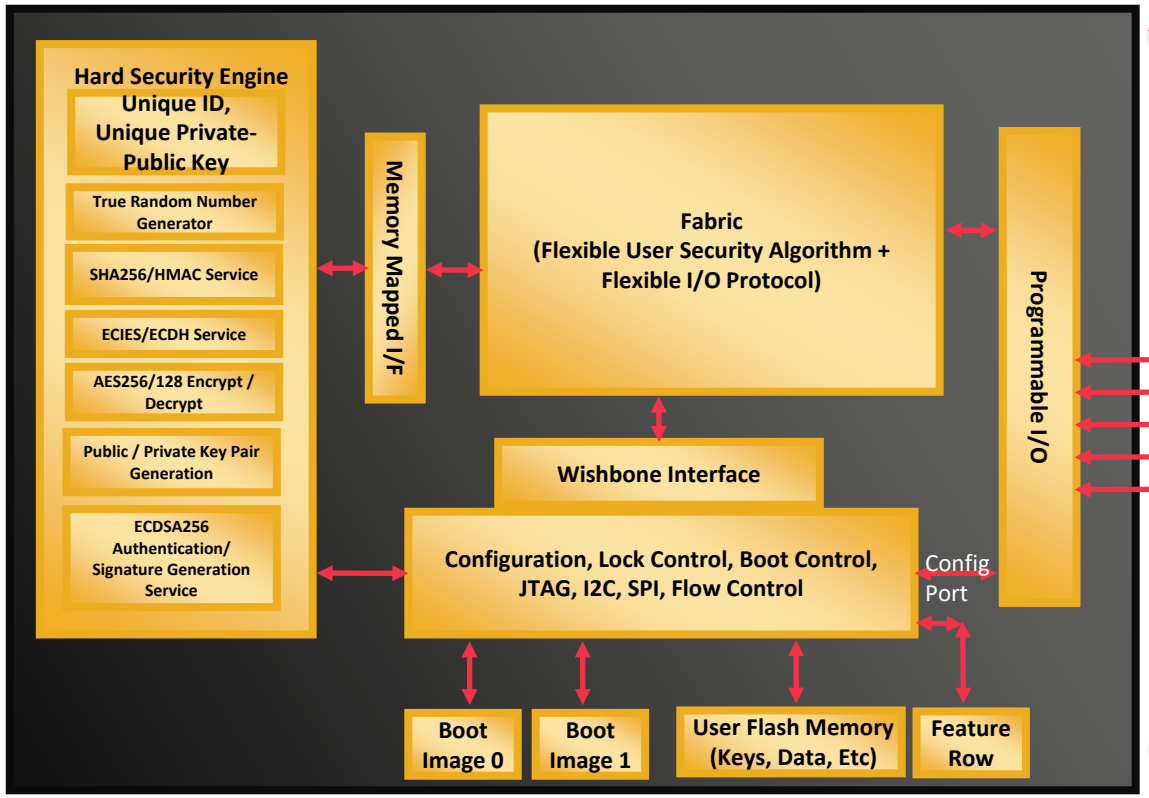
Root of Trust Foundations for Cyber Resilience

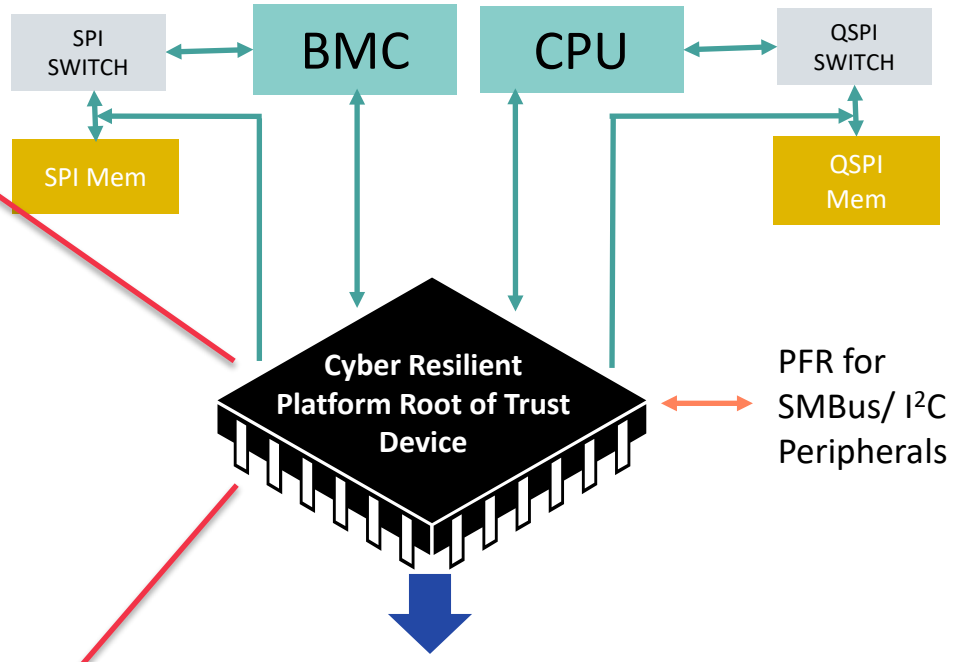
- Ability for device to verify its own code/configuration – self attestable
  - Must implement in secure hardware
    - Protected in Supply Chain
    - Immutable unique electronic ID tied to each device at silicon level
- Ideally first digital device on and last digital off
  - First link in chain of trust that protects entire systems



Example: PFR Applied to Servers

Simple, Robust, Scalable PFR



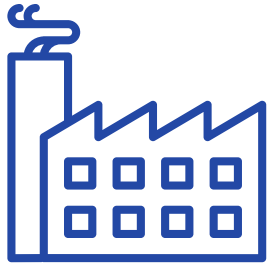


DETECT → RECOVER → BOOT → PROTECT

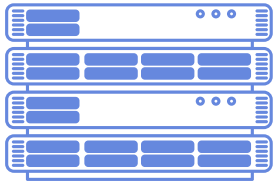
NIST SP 800 193

Supply Chain Weaknesses

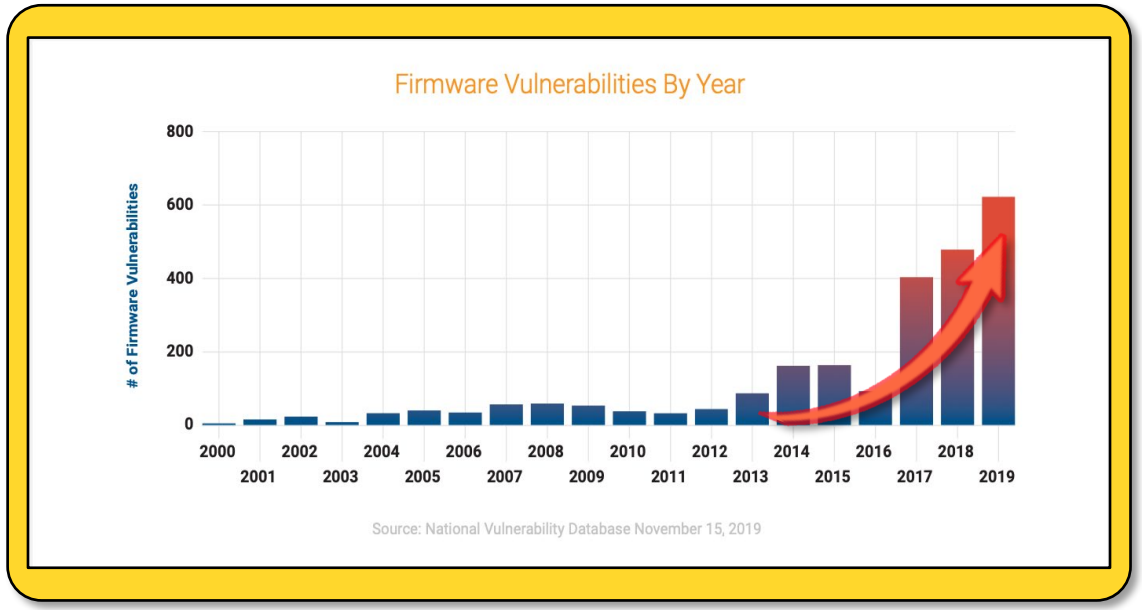
MANUFACTURING | **IN-TRANSIT** | **SYSTEM INTEGRATOR** | **IN-SYSTEM UPDATES**



Install Firmware, Program CPLD



Firmware Can be Compromised Anywhere along the Supply Chain



Example Supply Chain Attacks

High Level Sponsored Supply Chain Attack

- Hackers & CM/ODM Collaboration
- Microsoft Embedded was Target
- Enabled behind Firewall Enterprise Access

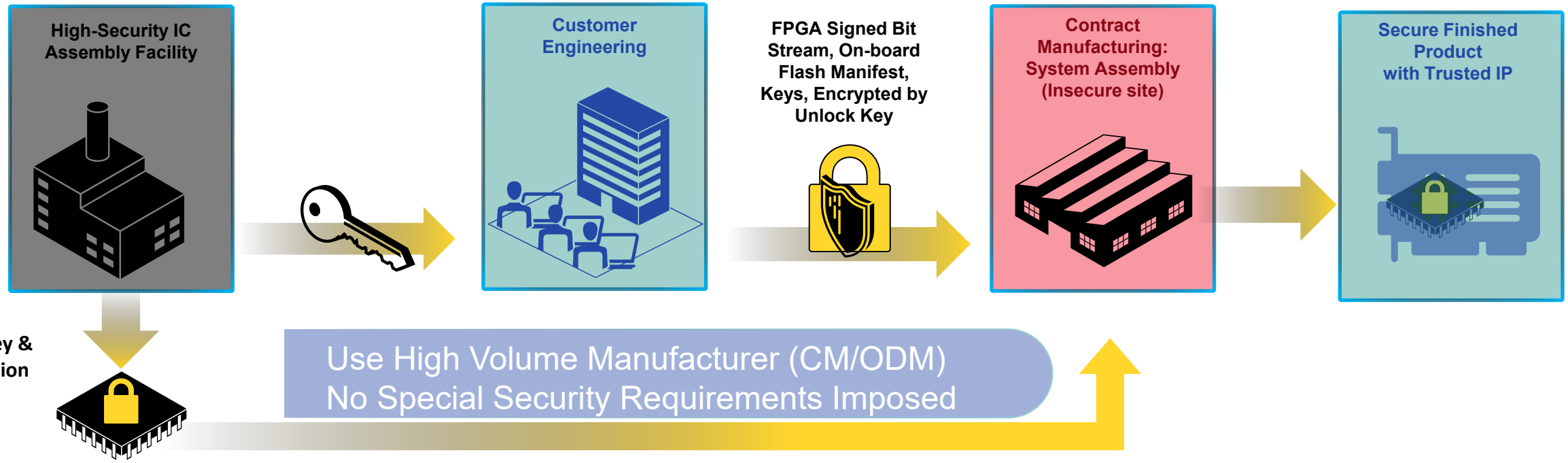
Growing Catalog of Firmware Attacks Available

From Eclypsium's Top 5 Firmware Attack Vectors: https://eclypsium.com/2018/12/28/the-top-5-firmware-and-hardware-attack-vectors/

From TrapX Research Labs Security Whitepaper: https://www.trapx.com/wp-content/uploads/2021/01/AOA_Report_TrapX_AnatomyOfAttack-ZombieZero.pdf

How to Reduce Supply Chain Risk Profile

"manufacturing and production experienced an average level of ransomware attacks last year with 36% of organizations hit... it is the sector that has the highest expectation of experiencing a ransomware attack in the future. " – Sophos, State of Ransomware in Manufacturing and Production 2021



- Protection against overbuilding, cloning, counterfeiting and Malware/Ransomware insertion
- Ability to track devices through the supply chain
- Locked parts with secure ownership transfer

- Lowers cost of secure manufacturing:
  - Lower OpEx/CapEx at CM/ODM
  - Reduces logistics burdens
  - Increased security with self protecting devices reduces secure handling costs

Summary: Pulling it All Together

- Security at the Device Level with Foundational HRoT
  - Immutable Device Unique Silicon Die Level Electronic Identification
  - Attestable Configuration via Asymmetric Cryptography for Trusted/Authenticated Boot
  - Confidentiality via Symmetric Cryptography for Data/IP Integrity
  - Side-Channel Attack (SCA) Resiliency & Self-Protection via Soft and Hard Lock Access control
- Security at the System Level with Cyber Resilience
  - Multiple Roots of Trust Capabilities (e.g., Storage, Reporting, Recovery, Update)
  - PFR based on NIST 800-193 to Secure Against Firmware-based Attacks
  - Nanosecond Reflexes Against Multiple Simultaneous Attacks & Un-bypass-able First-on, Last-off Platform Security
- Security Lifecycle via Secure Supply Chain Protections
  - Lockable parts with internal secure ownership transfers
  - From Initial Product Assembly, End-product Shipping, Integration, & the Product's End of Life (EOL)

Applying this for your Organization

- **Focus:** Cyber Resilience, applied at the Platform Firmware Level with new Technologies to protect your systems within high risk supply chains.
- **Targeted Goals:**
  1. Understanding Platform Firmware Risks for your platforms, particularly those that require strong resiliency
  2. Defining Cyber Resilience vs Cyber Security - where you need continuous, automated Protect-Detect-Recover paradigm applied
  3. Recognizing Emerging Platform Firmware Risk Mitigations you can use to enable PFR
  4. Applying Standards Compliance Evolution, w.r.t. PFR, such that your solutions will be recognized as within industry's best practices
  5. Resolving Supply Chain Security Vulnerabilities, particularly at the growing firmware level
  6. Using Supply Chain Security mitigations via Lockable parts & secure ownership transfers to minimize your attack surface of these vulnerabilities within the supply chain

Thank You