STORAGE DEVELOPER CONFERENCE

SDC22 | Fremont, CA
September 12-15, 2022

BY Developers FOR Developers

A SNIA. Event

Storage Security Update for Developers

Eric Hibbard, CISSP, CIPP/US, CISA

Samsung Semiconductor

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion, please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Current Threat Landscape

- Social Engineering
- Advanced Persistent Threat (APT)
- Ransomware/Malware
- Unpatched/Updated Systems
- Security Misconfiguration
- Denial of Service
- Sensitive Data Exposure
- Injection Flaws
- Cryptojacking
- Cyber Physical Attacks
- Broken Authentication
- Broken Access Control
- Third Party (Supplier)
- Insider Theft
- Mobile Malware
- Physical Loss of Devices
- Cross-site Scripting (XSS)
- Man-in-the-Middle Attacks
- IoT Weaponization

Common Threat Actors

- Cyber Terrorists
- Government-sponsored/State-sponsored Actors
- Organized Crime/Cybercriminals
- Hacktivists
- Insiders
- Script Kiddies
- Internal User Errors

Common Motivations

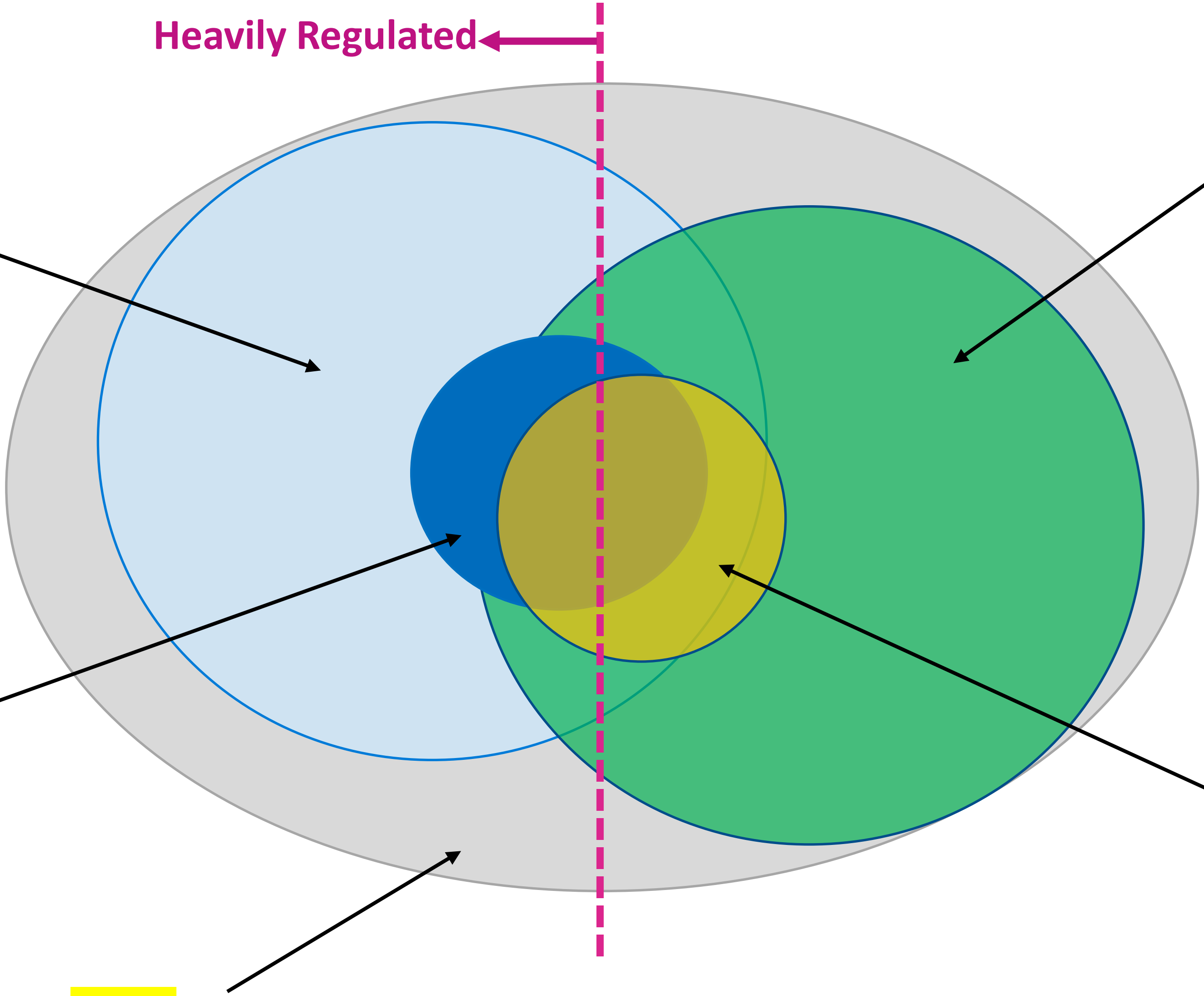
- Political, Economic, Technical, and Military Agendas
- Profit/Financial Gain
- Notoriety
- Revenge
- Multiple/Overlapping

Security is a People Problem!

Noteworthy Examples of Attacks/Breaches

- Colonial Pipeline attack in the US (critical infrastructure)
- Russian/Ukraine Hacking
- Lampsus$ digital extortion gang theft of source code and data
- Costa Rica state of emergency (ransomware by cybercrime gang Conti)
- North Korea’s Lazarus Group’s theft of $540M cryptocurrency
- Data theft from health care providers (ransomware and data breaches)

Privacy: Collection Limitations, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, Accountability



Information Security: Ensures Confidentiality, Integrity, and Availability (CIA) of information

Personal Data Protection: Safeguards applying under various laws and regulations to personal data (PII, PHI, etc.) about individuals that organizations collect, store, use and disclose

Ethics: Moral principles that govern a person's behavior or the conducting of an activity

Cybersecurity: Ensures Confidentiality, Integrity, and Availability of data; Identify, Protect, Detect, Respond, Recover

Legal/Regulatory Landscape

- Cybersecurity (many)
  - US DoD Cybersecurity Maturity Model Certification (CMMC)
  - US Presidential Executive Orders (Zero Trust, Consumer IoT Labeling)
  - EU Digital Operational Resilience Act (DORA)
- Privacy (many)
  - EU General Data Protection Regulation (GDPR)
  - China Personal Information Protection Law (PIPL)
  - Multiple US state (e.g., CA CCPA/CCRA)
- Cybersecurity/privacy litigation on the rise
- Other
  - EU Directive 2009/125/EC (LOT 9)

Changes to Key Security Frameworks

- ISO/IEC 27000-series Security Standards
  - New ISO/IEC 27001 (Nov-2022) and ISO/IEC 27002 (Feb-2022)
  - New ISO/IEC 27040 Storage security (Q1 2023)
- Payment Card Industry (PCI)
  - PCI Data Security Standard 4.0 (Mar-2022)
- NIST
  - NIST SP 800-53 Rev. 5 (Sep-2020)
  - NIST Cybersecurity Framework (CSF) 2.0 initiated

- Significance: Security professional adjusting to changes (distracted)

Gazing into the Crystal Ball

Important Trends

- “Reasonable” security has a risk-based aspect
- Supply chain security
- Circular economy (reuse)
- Product security certifications (FIPS 140, Common Criteria, etc.)
- Zero Trust Architectures (primarily US Government)
- Cloud/Edge computing

Why Should Developers Care?

- Secure by design and secure by default are expected
- Vulnerability prevention and management are expected elements of the product development process
- Practicing poor cyber hygiene can have legal implications
- Source code and design specifications stolen on regular basis
- Ransomware attacks are delaying or wiping out projects
  - Paying a ransom does not guarantee a recovery
- Attackers are attempting to inject malicious code into code base
  - Open source and vendor proprietary

Storage Security Event Horizon

- Secure eradication of data on storage devices and media
  - IEEE 2883-2022 provides specific requirements and guidance
- Storage security added to security audit criteria
  - ISO/IEC 27040 (2nd Ed) includes requirements and referenced by ISO/IEC 27002
- Computational storage security considerations
- Key Per IO for NVMe storage
- Post Quantum Cryptography (PQC)

Summary

Conclusions

- Many of the security standards that are relevant to storage are new or recently updated; typically have requirements
- Exploiting some of the new storage security capabilities and practices can require significant changes
- The *trust, but verify* security mantra is practiced by many organization; vendors must earn and maintain this trust to be a supplier
- Prepare for the inevitable attacks

Additional Resources

- SNIA Storage Security Resources
  - https://www.snia.org/security
- NIST Cybersecurity
  - https://www.nist.gov/cybersecurity
- ISO/IEC Information security, cybersecurity, privacy protections
  - https://www.iso.org/committee/45306.html
- Payment Card Security Standards Council
  - https://www.pcisecuritystandards.org/
- Center for Internet Security (CIS)
  - https://www.cisecurity.org/cis-benchmarks/

Thank You!

Please take a moment to rate this session.

Your feedback is important to us.