PQC Impact on I2C

Is PQC the Death of I2C?

Paul Kaler, Jeff Wolford, Jeff Hilland, HPE

Agenda

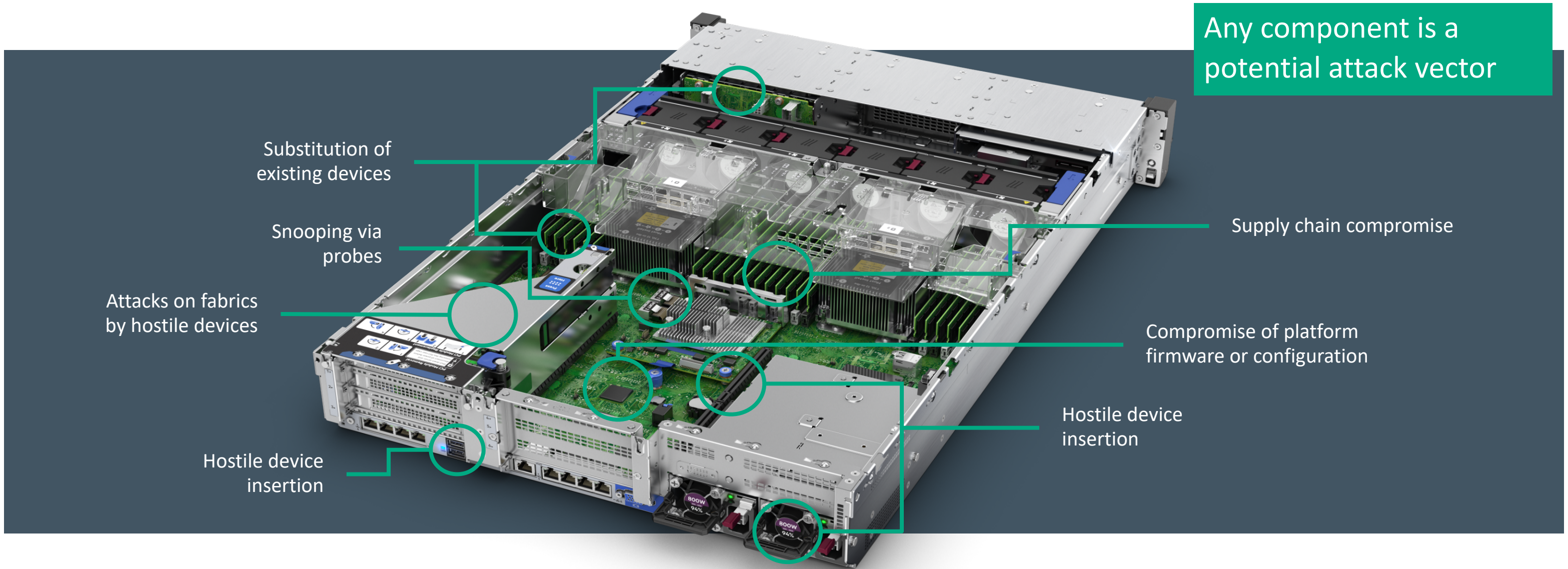
- What's the Problem with Post-Quantum Cryptography (PQC) and I2C
- Platform Implications & Customer Impact
- Potential Solutions
- Industry Call to Action

What's the Problem with PQC and I2C?

- PQC Signatures are 50-500x larger than traditional signatures
- Use Case: SPDM Signed Measurements using SPDM over MCTP over SMBus/I2C
  - With 73B MCTP (64B MCTP payloads) over I2C at a typical 100kHz rate that is 171 messages/second
  - After MCTP and SPDM headers that leaves 59 bytes for SPDM payload
  - FIPS 204 ML-DSA-87 (Dilithium) signature is 4,627B vs. ECDSA P-384 96B signature **(~50x larger)**
    - Dilithium takes ~half a second for just one signature compared to $1/100^{th}$ of a second for P-384
  - FIPS 205 SLH-DSA-SHA2-256f (SPHINCS+) signatures are 49,856 bytes **(~500x larger)**
    - SPHINCS+ takes ~5 seconds per signature
- Timeframe Challenges
  - PQC algorithms are being implemented in silicon now– no ubiquitous sideband alternative to I2C
  - LMS has smaller sig size but has issues (e.g., stateful tracking, no HSM backup and restore)
  - CNSA 2.0 prefers PQC for firmware and software signing algorithms starting 2025—that's next year!
    - Dilithium is starting to emerge as the favorite but there is some interest in SPHINCS+
  - Falcon (FN-DSA) has smaller signatures (~1,273B) but will be too late for the 1^{st} round of silicon

Platform Implications & Customer Impact

- Platforms can contain dozens of devices to attest with SPDM



Platform Implications & Customer Impact

- Increased boot times due to PQC Signed Measurements on all those devices
  - Consider a full-up 2U 2P platform with 40 E3.S NVMe drives, 32 DIMMs, 2 CPUs, 3 risers, 6 CEM cards, 10 backplanes, 2 OCP NICs, 2 power supplies, and 5 FPGA/CPLDs adds up to **102 devices**
  - Assuming SPDM gets 100% of the MCTP over I2C/SMBus bandwidth and zero response delays, latency, or retries
    - This adds almost a minute of boot time for Dilithium and over **8 minutes** for SPHINCS+
  - More real world 50% utilization Dilithium adds almost **2 minutes** and SPHINCS+ adds over **16 minutes**

Potential Solutions

- Realistic path for short-term improvements
  - Use SPDM/MCTP over PCIe VDM where available—not isolated from host
  - Management Controller parallelize across devices as much as possible—I2C makes this difficult in muxed architectures
  - Drop down to non-PQC SPDM if I2C is all that is available or wait…
- Longer term possibility
  - Falcon – smaller signatures than Dilithium but still much larger than non-PQC
- What the industry needs for an isolated control plane for PQC
  - Move to I3C/USB for device management
  - OCP needs to align on just one (preferably USB)

Industry Call to Action

- OCP Datacenter NVMe requiring I3C for PQC in v2.6
- Can we get to one sideband (USB) for DC-MHS HPMs?
  - I3C isn't enough bandwidth for all use cases and hubs are new, untested, and expensive
  - USB is gaining traction (e.g., OCP NIC, PCIe CEM) and is time tested and multi-purpose
  - Plumbing just USB on an HPM would be a simplification and cost reducer
  - EDSFF needs a path to USB (pinout challenges)
  - Devices could support via native USB or USB-I3C bridging
    - PCIe CEM
    - EDSFF
    - Microcontrollers and secure elements
  - Other problems PQC introduces
    - Resource constrained devices (e.g., memory footprint, simple devices like fans)

PQC Resources

- FIPS 204: ML-DSA-87 (Dilithium) https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf
- FIPS 205: SLH-DSA (SPHINCS+) https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf
- NIST SP 200-208: LMS https://csrc.nist.gov/publications/detail/sp/800-208/final
- Falcon (FN-DSA) Will be FIPS 206 when released https://falcon-sign.info/
- CNSA 2.0 FAQ April 2024 Ver. 2.0 https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/1/CSI_CNSA_2.0_FAQ_.PDF

Thank you!