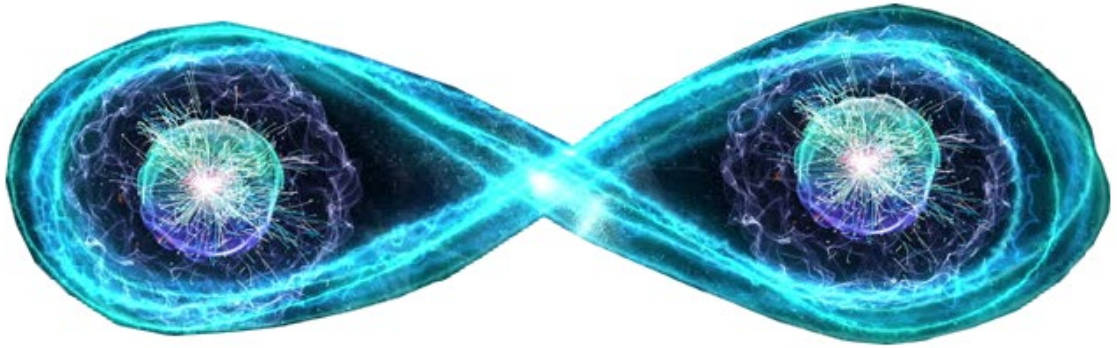
Memory and Storage Security in a



Post Quantum World

Bill Gervasi, Principal Memory Solutions Architect

Monolithic Power Systems

bill.gervasi@monolithicpower.com

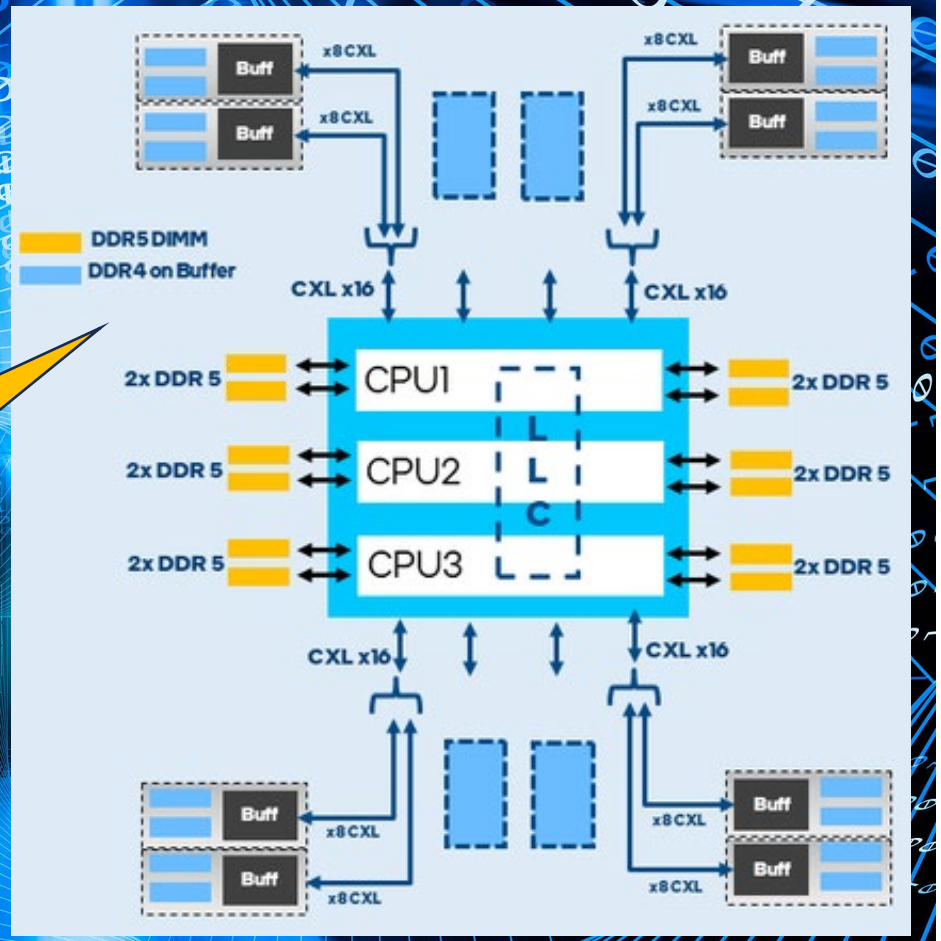
the Future of Memory and Storage

Security Concerns in the next generation

So many attack points in fabric architectures

…and the sophistication of the attackers is increasing…

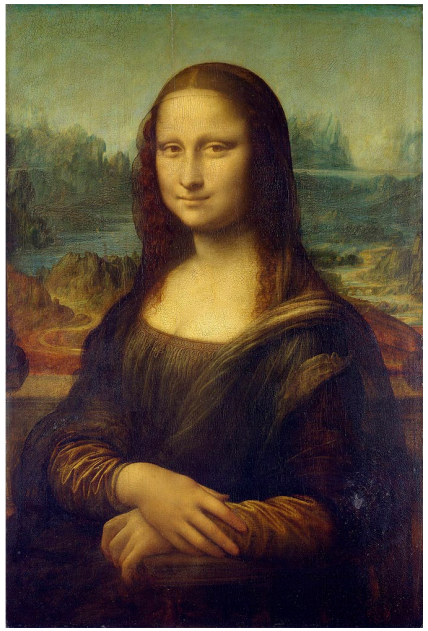
Growing variety of memory and storage options creates new challenges

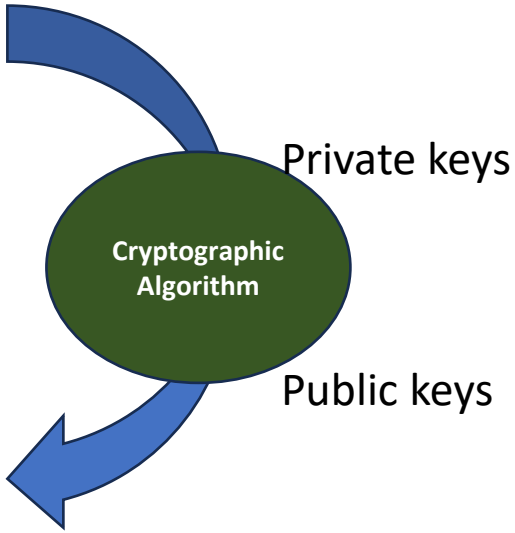


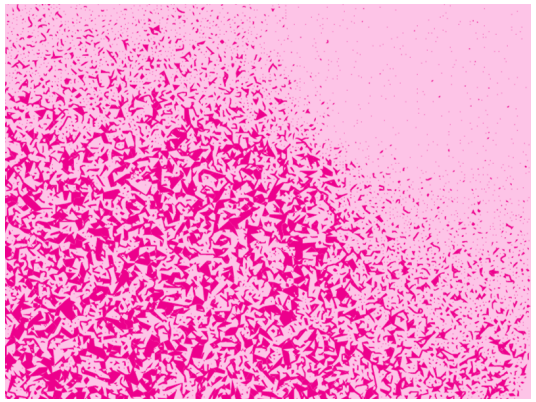
Detection & mitigation need support

Hardware		Software
Malware	Virus-style programs, Denial of Service attacks	Insecure Agency
Man-in-the-middle	Mimic trusted device, Intercept data in flight	Insecure Plugin Design
Spy chips	Devices planted in system Malicious data corruption	Insecure Output Handling

Not even close to a comprehensive list… illustrative only!







Security regimes include verifying a root of trust

Combination of keys and hashing algorithms allow data security

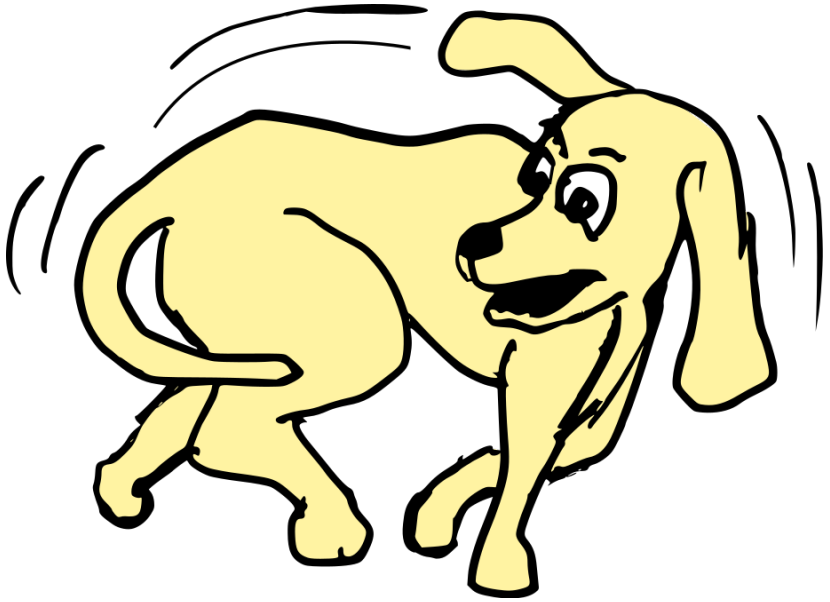
Algorithms assume thousands of years are needed to decode the information

The larger the data set, the more difficult to decode

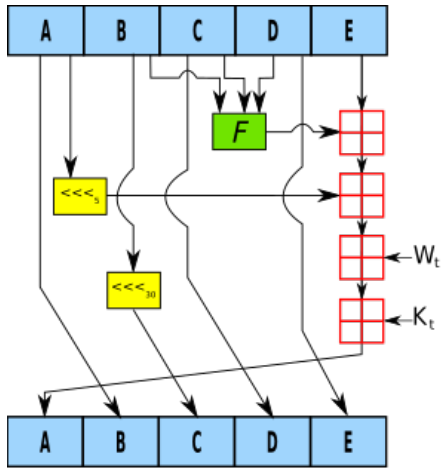
Security is a treadmill

Algorithm complexity increases as computers get better

1993: SHA-0 160-bit hash
1995: SHA-1 improved algorithm
2001: SHA-2 256 & 512-bit hashes
2015: SHA-3 improved algorithm



e.g., During Auto SSD standard development, NIST deprecated 256-bit in favor of 384-bit… so we changed the proposal



Security requirements will undoubtably change during the life of the next generation memory and storage

We need to be flexible in how we keep up

Hardware + firmware likely necessary… but where?

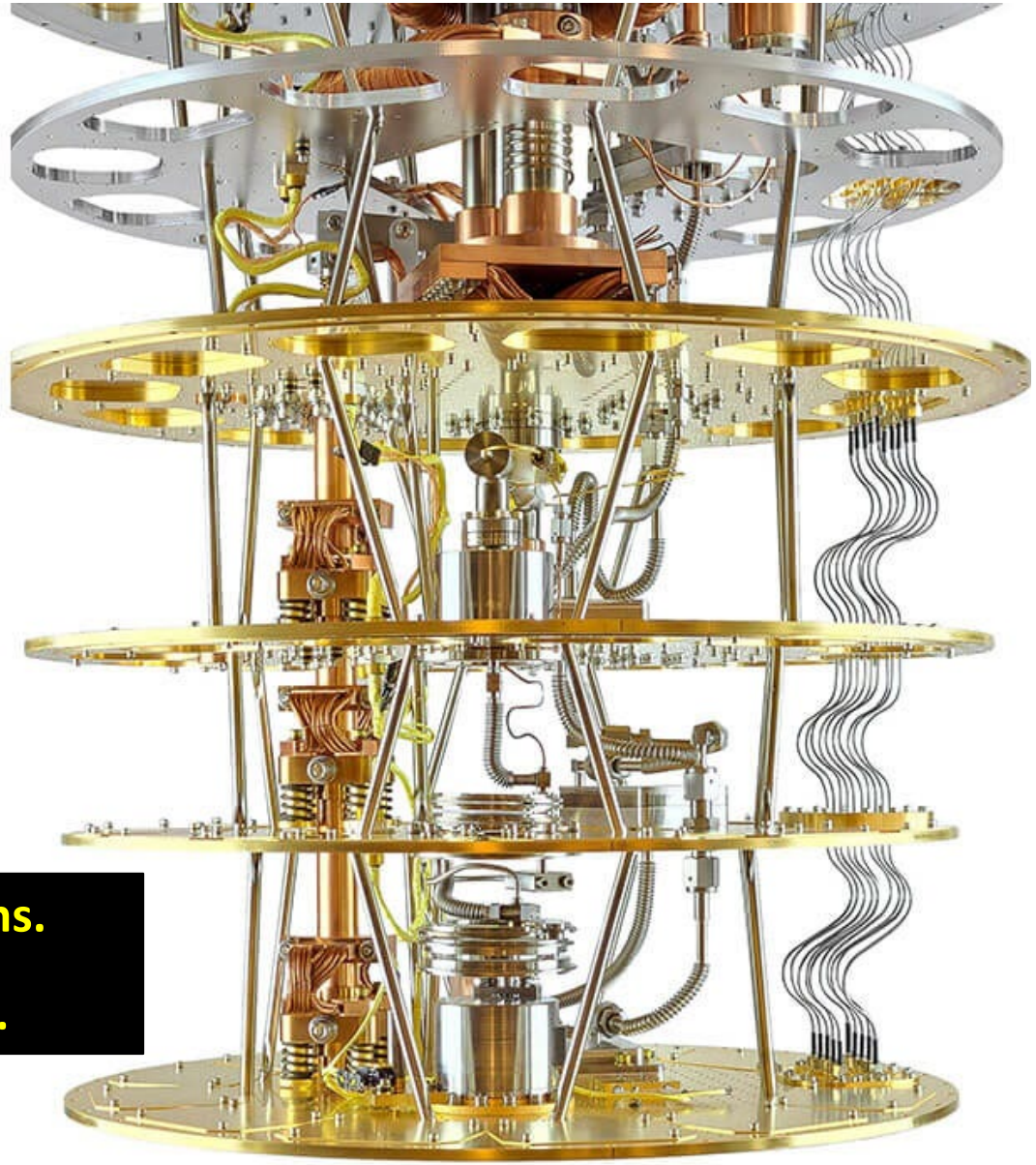
Enter Quantum Computers

Quantum computers process data exponentially faster than traditional computers

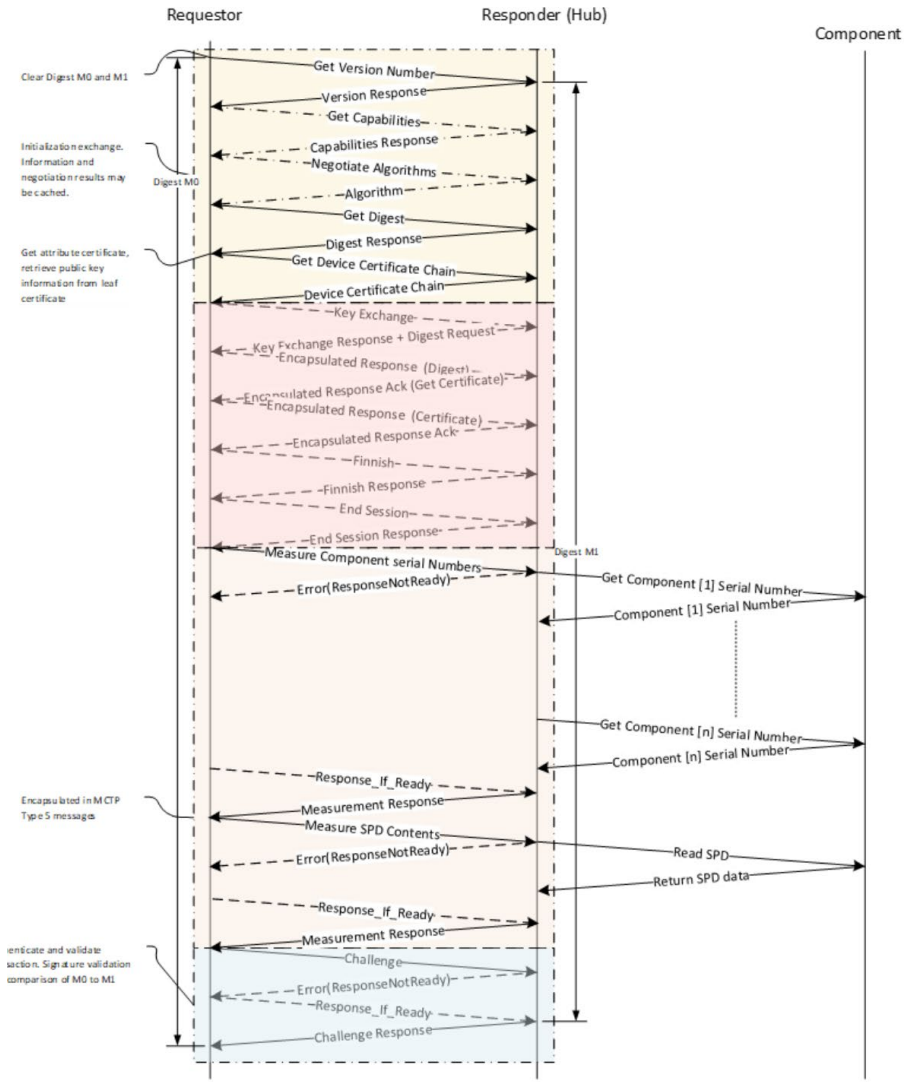
Need for newer security algorithms emerge

The NIST treadmill is alive and well

2024: First three PQCs: FIPS 203, FIPS 204, FIPS 205
2025: HQC joins the list



- **2030: NIST plans to deprecate RSA-2048 and ECC-256 algorithms.**
- **2035: NIST plans to disallow RSA-2048 and ECC-256 algorithms.**



Security handshake to establish root of trust is fairly complex

Requires certificates that are multiple KB in size

Taking this complexity all the way to every active component would be

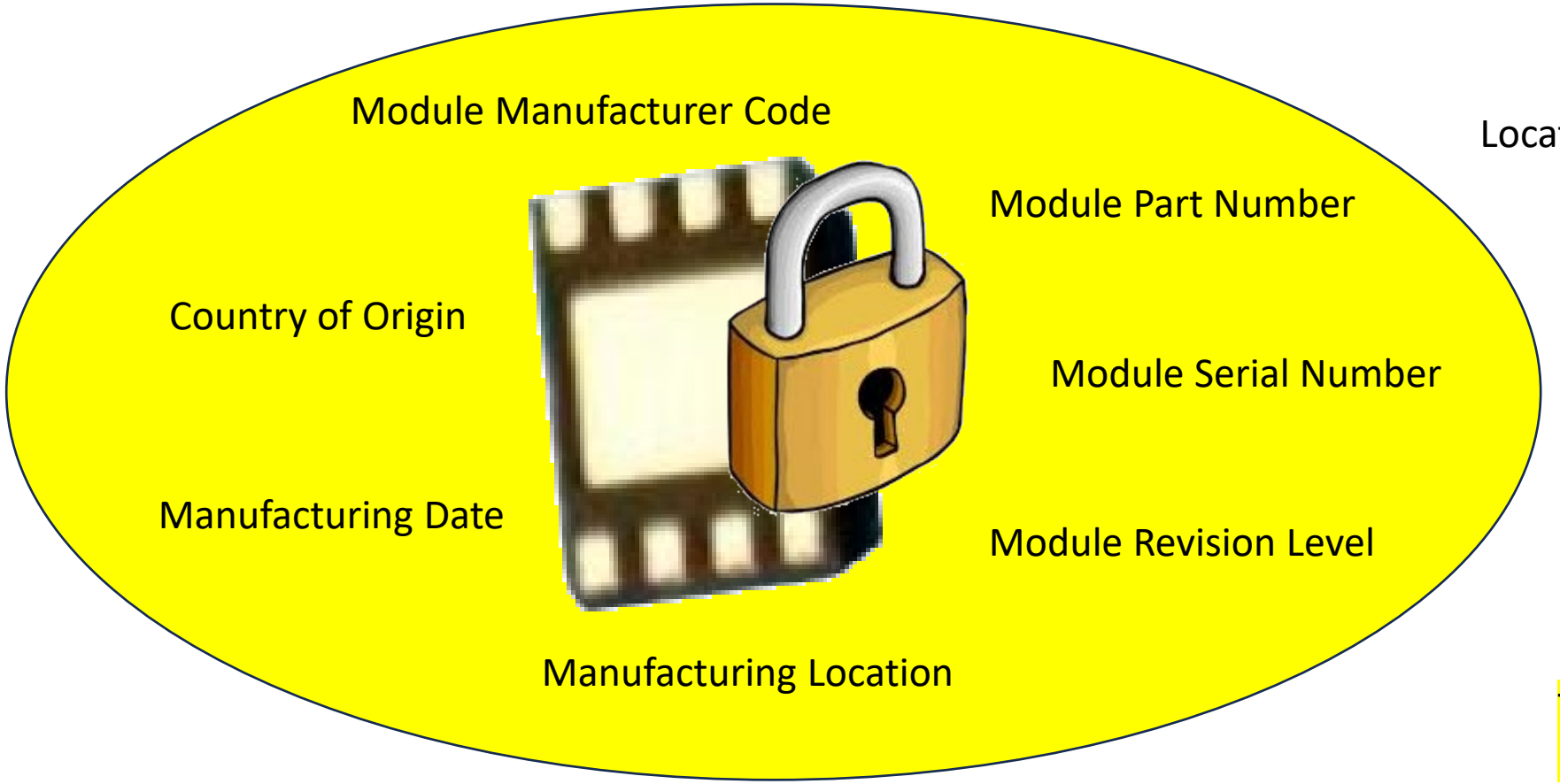
- Too costly
- Introduce new security risks and attack points

Having a system management hub proxy the module leaves it open to spoofing with non-secured components

However, end users do want to add bill-of-materials tracing to memory modules to increase trust levels

Bill of Materials

Hardware and software identifiers programmed into a secured (immutable) configuration ROM



Located on system management bus

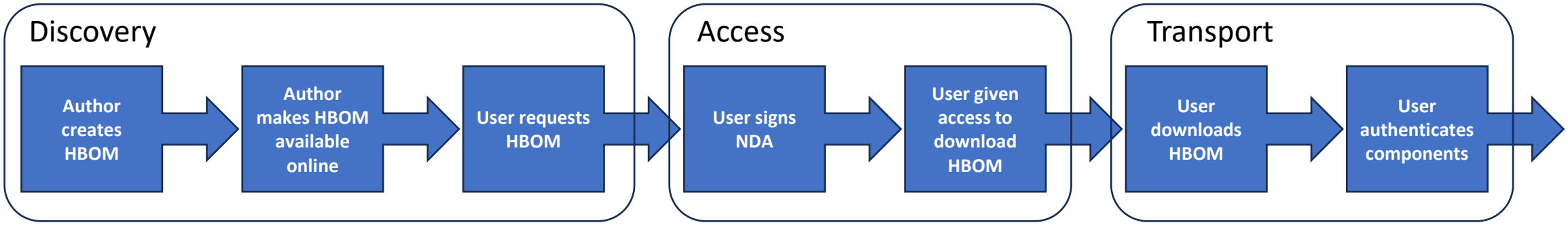
Read by baseboard manager or host CPU

This information may be spoofed!
Next level verification still needed

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

CISA.gov

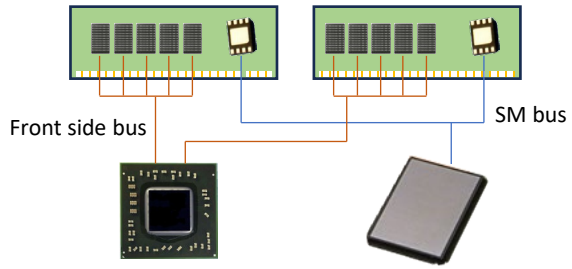


Establish a trust between end user and supplier

1. Supplier creates an HBOM (Hardware Bill of Materials) describing product
2. Customer signs an NDA with the supplier to get encrypted access to HBOM
3. EDA interface establishes secure access and rights
4. HBOM may include nested links to key (e.g., smart) components
5. SBOM equivalent for software/firmware also exists

https://www.cisa.gov/resources-tools/resources/hardware-bill-materials-hbom-framework-supply-chain-risk-management
https://www.cisa.gov/sbom

Data Center Example Using DRAM Module



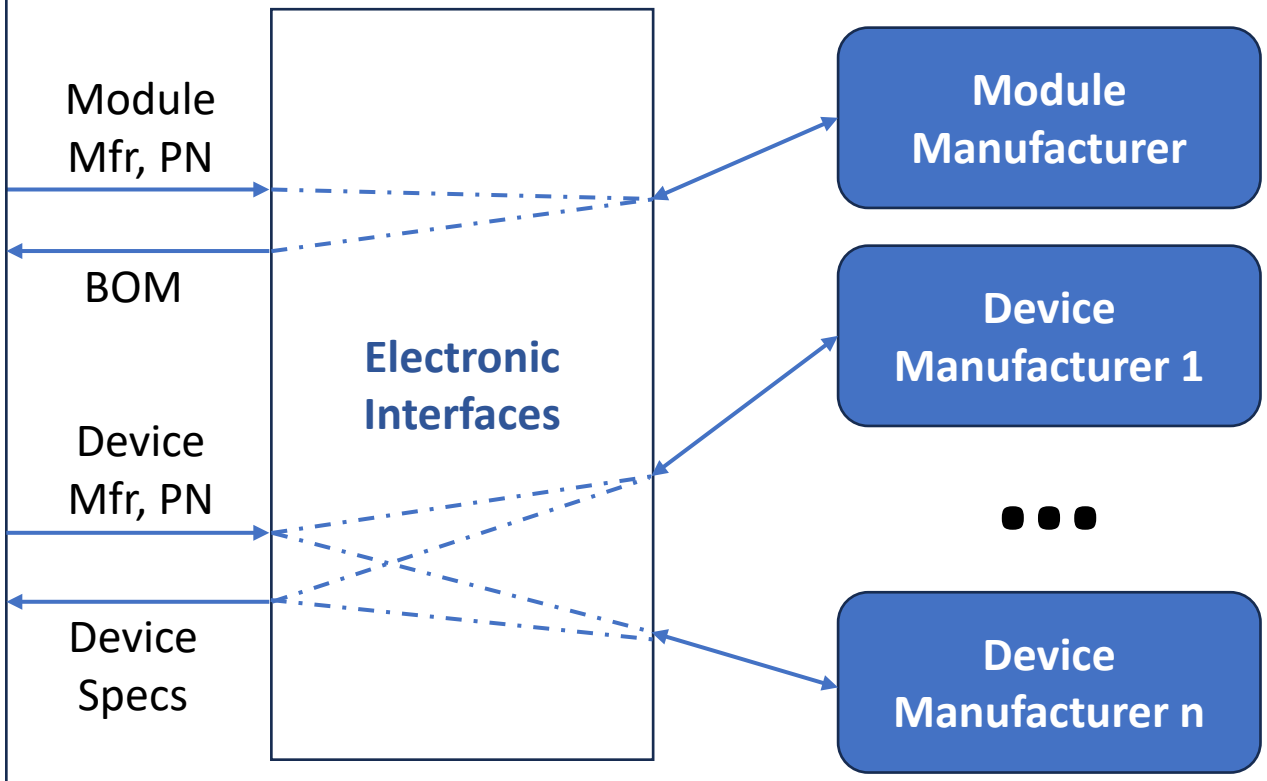
Software BOM read from configuration ROM
Manufacturer codes: Module, DRAM, etc.
Serial numbers from memory components
Serial numbers from support chips

Security check performed by host

BMC/CPU gets supplier data from ROM

Uses electronic access to module vendor to read full BOM

Any specific devices can be looked up as BOM contains supplier info as well



Spoofing resilience requires additional tracking

- Destination of module
- Known violators reported and identified
- Full SPDM* hash verification can be added using device serial numbers

* SPDM: Security Protocol and Data Model (DMTF.org)

BOM Tracking is a Start…

Data center BOM tracking builds trust in components

Requires suppliers and users cooperate with electronic links

Additional levels of security checks may be added (e.g., SPDM)

Security proxies, system authentication, encryption are beyond the scope of this talk

Security isn’t free – this takes time and adds cost…

…but detecting an attack before it happens

is cheaper than fixing the problem after it happens

Thank you for your time

Any questions?

Bill Gervasi, Principal Memory Solutions Architect

Monolithic Power Systems

bill.gervasi@monolithicpower.com