CYBER SUPPLY CHAIN

-THE BASICS

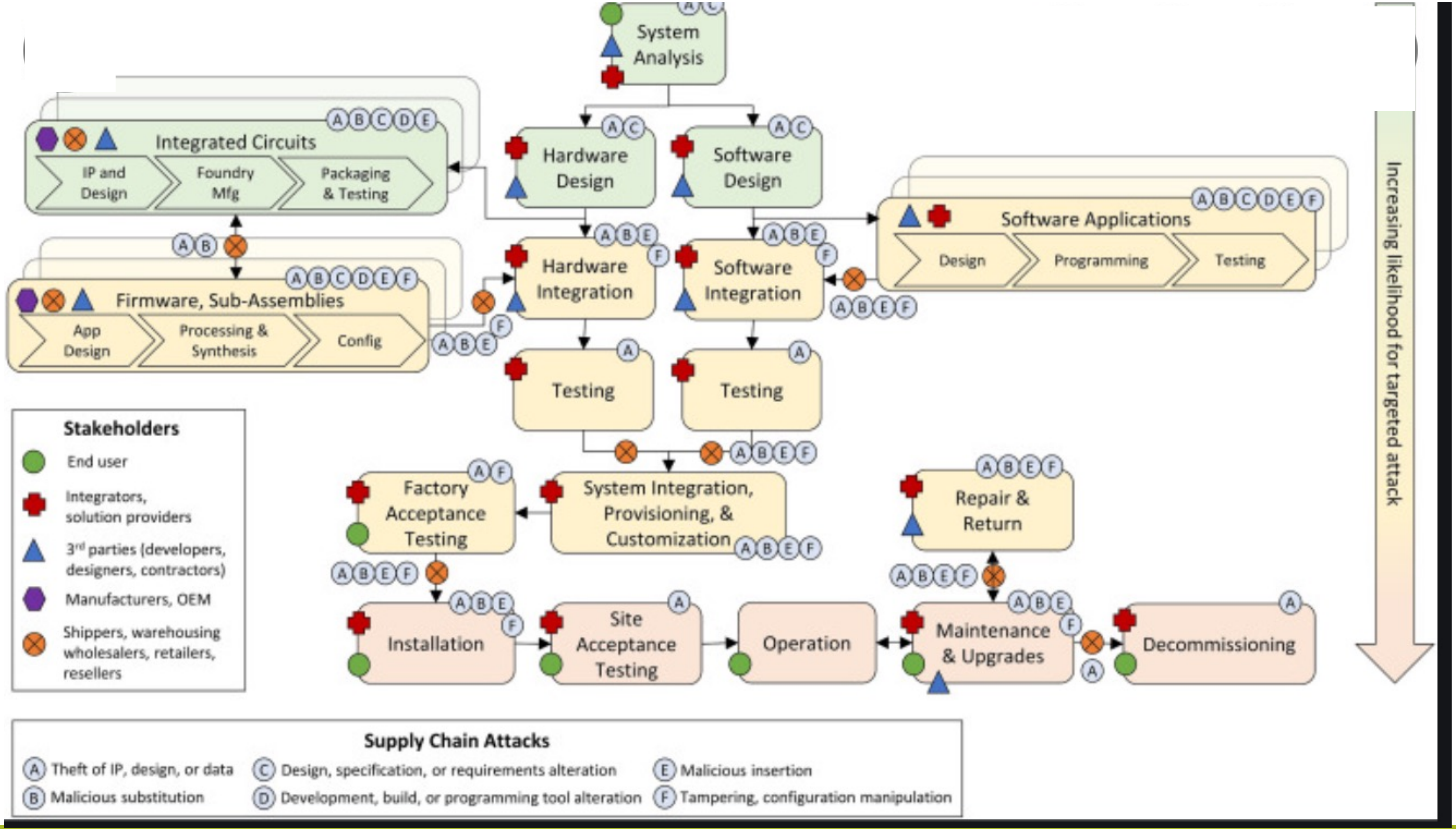
- RESEARCH AND SOFTWARE FOCUS

27 October 2021

Cyber Supply Chain Characteristics.

- Supply chains are global
- Supply chains span the entire life cycle from concept to end-of-life
- Supply chains are complex, intricate
- Multiple entities involved
  - The prime
  - Subs
    - The sub's subs
  - At each level there can be multiple interdependencies

Supply Chains are complex, global, can be many hundreds of entities involved



Stakeholders

- ● End user
- ✚ Integrators, solution providers
- ▲ 3rd parties (developers, designers, contractors)
- ⬢ Manufacturers, OEM
- ⊗ Shippers, warehousing wholesalers, retailers, resellers

Supply Chain Attacks

- Ⓐ Theft of IP, design, or data
- Ⓑ Malicious substitution
- Ⓒ Design, specification, or requirements alteration
- Ⓓ Development, build, or programming tool alteration
- Ⓔ Malicious insertion
- Ⓕ Tampering, configuration manipulation

NIST Cyber SCRM Facts*

(C-SCRM)

- - **Risk**: Cyber supply chain risk is associated with a lack of visibility into, understanding of, and control over many of the processes and decisions involved in the development and delivery of cyber products and services.
- **Product testing by the end user is problematic**.

- - **Threats** :
  - Exist throughout the supply chain
  - Effectively managing cyber supply chain risks requires a comprehensive view of threats and vulnerabilities.
  - Threats can be either "adversarial" (e.g., tampering, counterfeits) or "non-adversarial" (e.g., poor quality, natural disasters).
  - Vulnerabilities may be "internal" (e.g., organizational procedures) or "external" (e.g., part of an organization's supply chain).

- **Critical Systems**: Cost-effective supply chain risk mitigation requires organizations to identify those systems/components that are most vulnerable and will cause the largest organizational impact if compromised.

- By statute, federal agencies must use NIST's C-SCRM and other cybersecurity standards and guidelines to protect security of federal information and communications infrastructure.

*05/25/2021

Detection and Mitigation

- Detection before a problem becomes evident may be difficult.
- Mitigation and resilience are essential

.

Lack of adequate testing protocols makes it difficult to prove that a hardware or software product is or is not vulnerable or compromised.

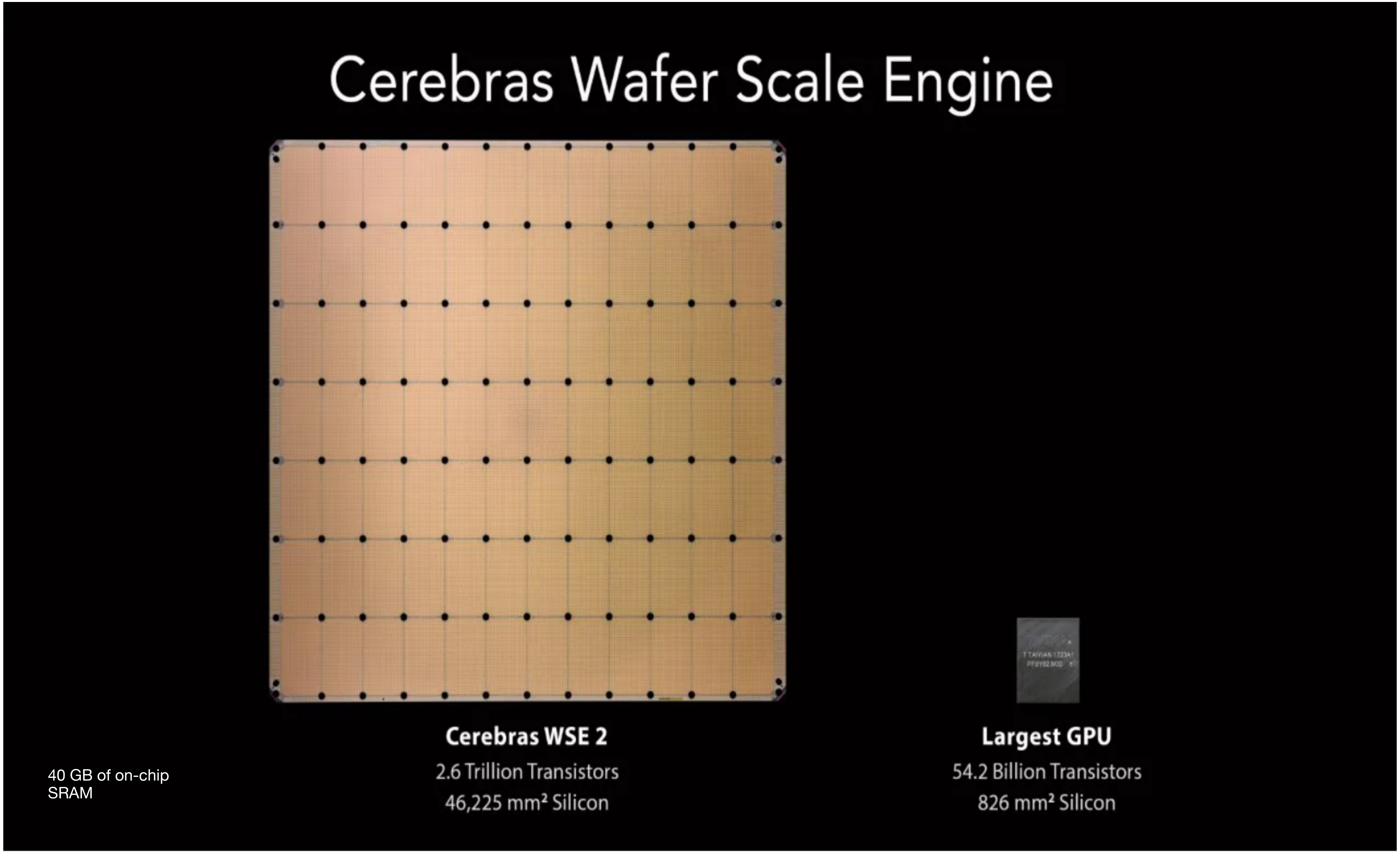
Mitigation

- Rules, Directives, Policy, Manuals, FAR (**52.204-21**) and DFAR **(DFARS 252.204-7012),** National Strategies
  - The problem is oversight and enforcement
  - Who’s in charge?
  - Good news and bad news.
  - Good: lots of interest in cybersecurity, lots of participants
  - Bad: Lots of overlapping responsibilities. No one’s in charge. No real oversight
  - Is there a need for a central national authority or clearing house with enforceable standards?
    - NIST comes closest
  - **<u>TESTING</u>**
  - <u>Research and Technology required</u>.
    - **Development of AI for full examination of all hardware and software included in the box/hardware/System, based on a standardized gold model for the product.**
  - Malicious access can be pre-engineered via components or designs and may be close to impossible or unlikely to be identified or found.

The Chip Problem

- Lack of secure U.S. capabilities, facilities
- Fabless. E.g., Apple M1 chip at 5nm (TSMC)
- Chip production and feature size – on the path to 2nm
    - How big is a nanometer?
        - A billionth of a meter.
        - Width of a piece of typing paper: 100,000 nanometers*
- Production at 5nm and 7nm now common
    - TSMC and Samsung
    - Intel trying to catch up
- More than just silicon
    - Advances in material sciences, e.g., CNT, graphene, packaging (multi-layer, split manufacturing, wafer scale)
- Chip examination, analysis
    - Past: 45nm or higher, SEM and image analysis
    - Now: Virtually impossible because of number of transistors per chip (billions to trillions, mega chips).
- **Problem: how to test and detect? More research required**

* www.nano.gov



Cerebras Wafer Scale Engine

Cerebras WSE 2

2.6 Trillion Transistors

46,225 mm² Silicon

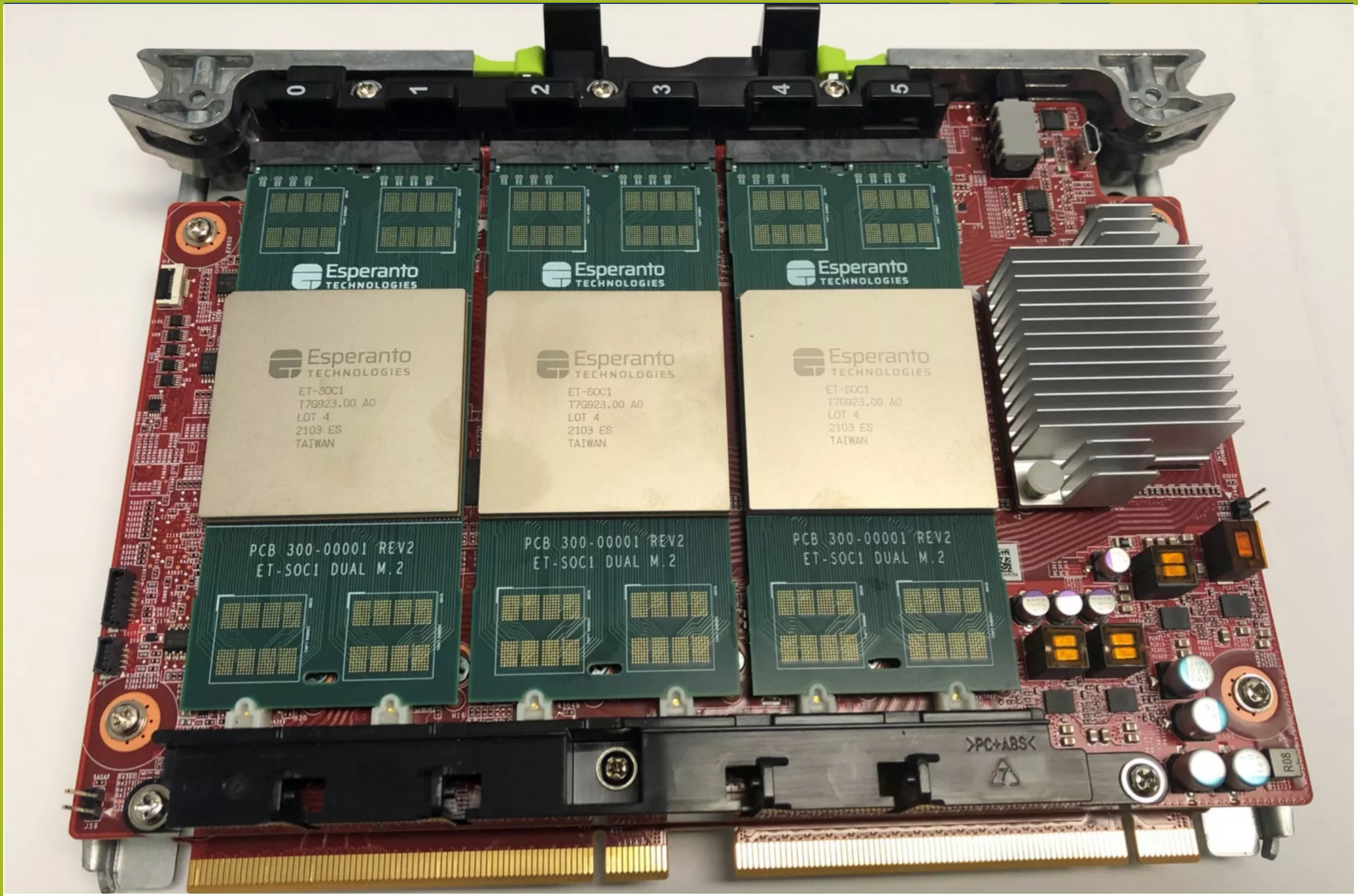
Largest GPU

54.2 Billion Transistors

826 mm² Silicon

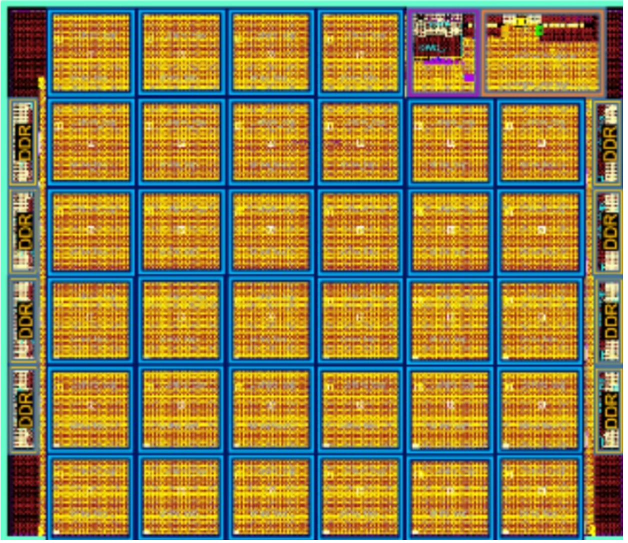
40 GB of on-chip
SRAM

COURTESY OF CEREBRAS

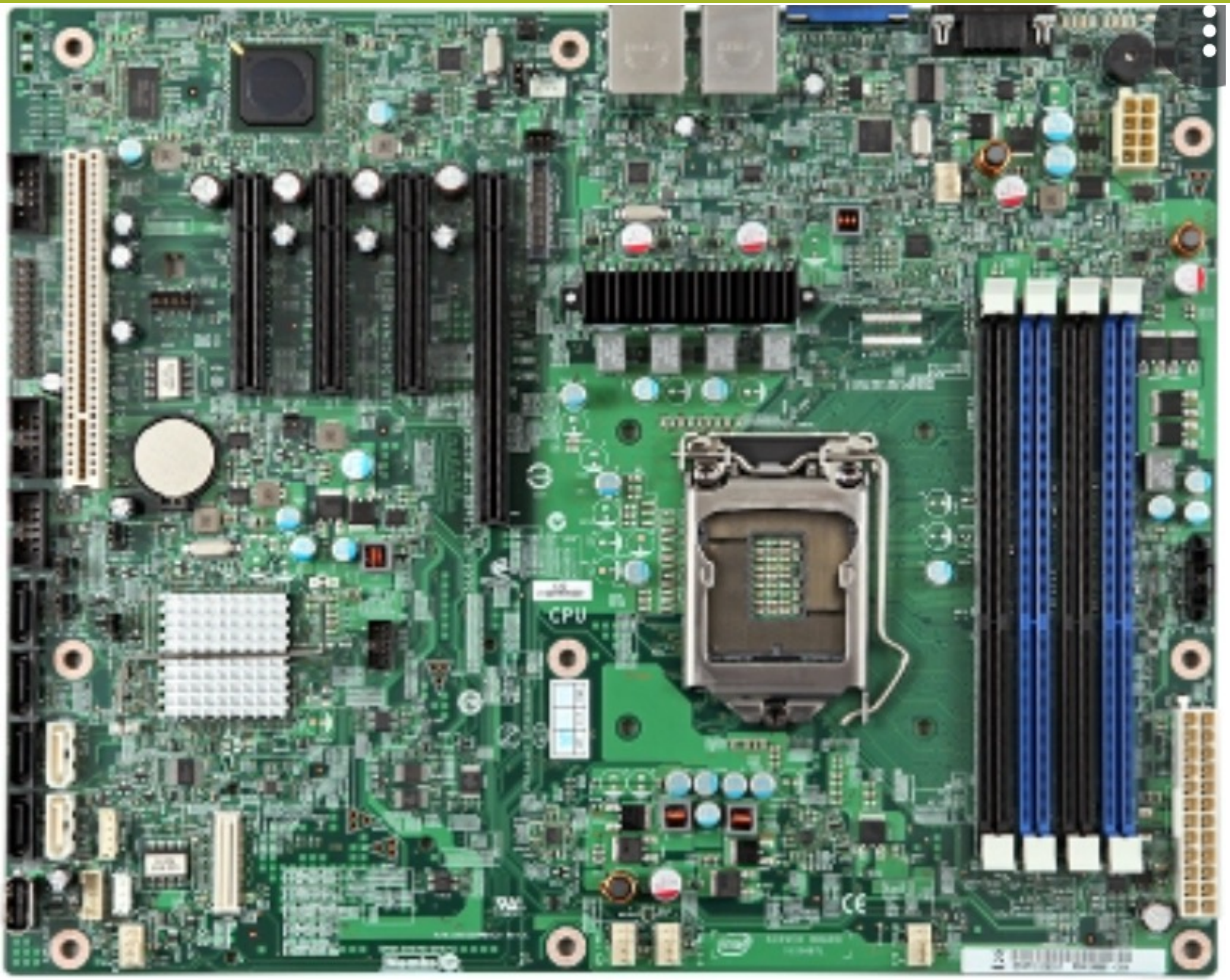


1000, RISC-V* processors on a single 7nm chip.

160+ million bytes of on-chip SRAM



* Reduced Instruction Set Computer, mostly used in embedded devices


CPU
CE

“Trusted”

- Trusted Foundry.
  - There is one so-labeled.
  - For sensitive DoD, Infrastructure activities, and the IC there are no US-controlled and manned fabs. i.e., operating at a classified level with cleared personnel
  - Why? Unrealistic.
    - **Research question: what to do?**

  - Trusted Vendors
    - For government entities it’s often likely that if the vendor is on a list of trusted vendors, the vendor and their product(s) will be deemed acceptable.
    - Without full testing and product verification for each product, there’s insufficient trust.
    - A problem at the heart of acquisition processes
    - **Same research question: What to do?**

A FEW RESEARCH EXAMPLES

IARPA

- TIC Program - Trusted Integrated Chips*

- Hardware Assurance; phenomenology of penetration
- **RAVEN** - prototype analysis tool for acquiring images of small areas at the 14nm range;
- **FUSE** - network analysis and machine learning
- **VirTUE** - vulnerability analysis, anomalous event detection, secure environment in the cloud**

DARPA

IRIS – the ability for developers to derive the function of ICs non-destructively***

TRUST – trust in integrated circuits****

- DisaggregatetheCircuit_Summary.pdf (darpa.mil)
- ** IARPA launches VirTUE program - Intelligence Community News
- *** March 2015 report
- **** 2007 Report

CHEST

CENTER FOR
HARDWARE AND
EMBEDDED SYSTEMS
SECURITY AND TRUST

CHEST Program – Center for Hardware and Embedded Systems Security and Trust

Supported by NSF Directorate for Computer and Information Science and engineering (CISE)*

Joint Efforts – Industry – University Cooperative Research Program (IUCRC)

<u>Universities</u>

- University of Cincinnati
- Northeastern
- UC Davis
- UV
- UCONN
- UT Dallas

*https://www.nsf.gov/cise/about.jsp

CHEST

CENTER FOR
HARDWARE AND
EMBEDDED SYSTEMS
SECURITY AND TRUST

Research Areas

- Hardware assurance
- Counterfeit detection
- Integrated circuit authentication
- Anti-reverse engineering
- Anti tampering
- Secure communication protocols
- Formal verification
- Secure processor architectures
- Vulnerability analysis/analyses
- Infrastructure safety and resilience
- Secure systems engineering including security of nanoscale computer devices

CHEST
CENTER FOR
HARDWARE AND
EMBEDDED SYSTEMS
SECURITY AND TRUST

*

- UCONN Examples
- **Physically Unclonable Functions (PUFs)** (*A set of unique features that can be built into a chip but not cloned.)*
    - **E.g., a novel way to authenticate untrusted integrated circuits**
  - **Hardware Security Primitives**
    - **E.g., phase change memory and its applications in Hardware security**
  - **Counterfeit Detection and Prevention**
    - **E.g., automated detection of counterfeit ICs using machine learning**
  - **Side – channel attacks**
    - **E.g., Error tolerance on FPGAs**
  - **Hardware Trojans**
    - **E.g., Hardware trojan detection**

- **Oblivious RAM**
  - **E.g., Privacy leakage via write-access patterns to the main memory**
- **Supply chain security**
  - **E.g., Clone detection of RFID-based supply chains**
- **Embedded systems Security**
  - **E.g., Hardware security and its adversaries**
- **Reverse Engineering**
  - **E.g., non-destructive testing**
- **Secure Processor Architectures**
  - **E.g., Generalized external interaction with tamper-resistant hardware**

* https://chest.engr.uconn.edu/research/#pufs

A Research Compendium Suggestion

- **There are hundreds if not thousands of cybersecurity research efforts. We need to consider the creation of a centralized research database.**
    - First step: catalog research to the extent possible. A need for a dedicated funded effort to create a living, breathing database to include
        - Government unclassified
        - Government classified
        - Academia
        - Industry
        - Proprietary where possible
        - Commercial, e.g., McAfee, Norton, etc.
        - Documented effectiveness
        - Industry C-SCRM best practices (NIST)

- Research Catalog
    - Sorted by type, approach, status
    - Detection of indicators
    - Cyber Risk Predictive Analytics (NIST and GSA)
    - Standards and best practices, standards efficacy

RESEARCH

Developing Technologies

- Examine the applications and utility of current and developing technologies
- A need for concerted focused efforts and a supporting budget
  - Big data analytics. Collection and analysis of data based on histories of cyber attacks, etc.
  - AI and ML, enhanced analysis of the cyber supply chain
    - Not aware of any existing complete databases of cybersecurity research in general and cyber supply chain in particular.
  - Material sciences, e.g., graphene, CNT, Blockchain (as an aid to provenance), superconductivity. Impact on vulnerability?
  - Anonymized case studies on cyber supply chain incidents (NIST)
  - Research on continuously evolving technological changes and threats that continue making C-SCRM a challenge (NIST)
  - Quantum – Feynman
    - Intelligence collection, cryptography, solution optimization, computer processing , communications.

RESEARCH

Developing Technologies

(Some specific ideas)

- Testing. AI for full examination of H/W and S/W based on a standardized product gold model.
  - How to improve on current, useable, verifiable testing technologies
  - Are current hardware end product testing methodologies effective?
- Detection of malicious content on a chip.
- Evaluation of "trusted" vendors
- How to overcome the lack of a truly trusted foundry?
- What are the enhanced analytics (AI and ML) that might lead to discovery of new threats and techniques
- How to create and maintain a centralized cybersecurity research database?*

* A possible model? DDR&E JFAC (Joint Federated Assurance Center) does something similar with cyber testing DB across the services.

Hardware Attack Elements

What detection techniques are plausible, extant?

- Detection of built-in backdoors is difficult without intensive investigation of components or other testing
- Eavesdropping, the possibility to gain access to protected memory without opening the hardware component**.**
- Fault induction, causing the interruption of normal system behavior
- Hardware modification, tampering with the product with invasive operations. The modification could be hardware but can also be software with a jailbreak maneuver.
- Fabrication backdoors, the presence of hidden methods for bypassing normal computer authentication systems.
- Counterfeit and clone components

Firmware*

- Lots of attention to software; also important to consider firmware
- Hardware and firmware are generally stealthier than software attacks, and they are often misidentified as design flaws or bugs.
- Firmware is the bridge between hardware and software; it runs higher level operations and controls basic functionality of the device, including communication, program execution, and device initialization.
- By reverse engineering firmware, adversaries can learn the system, identify vulnerabilities, and corrupt code by alteration or insertion. Firmware can be reprogrammable, and is, therefore, vulnerable to supply chain attacks during routine updates or [remote] maintenance
- Malicious firmware can hijack root access, steal data, affect device operation, and even disable the device

*https://www.sciencedirect.com/science/article/pii/S1738573320308573

Hack Examples

- Chinese company **SuperMicro**
  - Surveillance microchips placed inside hardware within data centers used by Apple, Amazon and others *
- **Realtek chip**
  - A botnet using a variant of the IOT malware "Mirai" found in the SDK
  - Affected over 200 Wi-Fi and router products from 65 vendors
  - A successful attack would provide full control of the WiFi module and root access to the device's operating system
- **SolarWinds Attack** **.
  - Company's Orion product provides system management tools for network and infrastructure monitoring
  - >30,000 public and private organizations affected
  - Malicious code created a backdoor for hackers to access and impersonate users and accounts..
  - Spread was undetected. Attackers had 14 months of unfettered access.
  - Gov't systems effected included DHS, State, Commerce and Treasury
  - Detected by FireEye.
- **UEFI - Researchers Discover UEFI Bootkit Targeting Windows Computers Since 2012 (Unified Extensible Firmware Interface)**
  - Circumvents Microsoft Windows Driver Signature Enforcement to load its own unsigned driver.
  - Facilitates espionage activities such as document theft, keylogging, and screen monitoring by periodically capturing screenshots.
  - The intrusion route of the malware remains unknown as yet.
- **Surface Pro 3**
  - Security flaw introduces malicious devices in enterprise networks and may defeat TPM

An excellent site for hardware attack information: Hardware attacks, backdoors and electronic component qualification - Infosec Resources (infosecinstitute.com)

Also see Flaw In AMD Platform Security Processor Affects Millions Of Computers | Hackaday

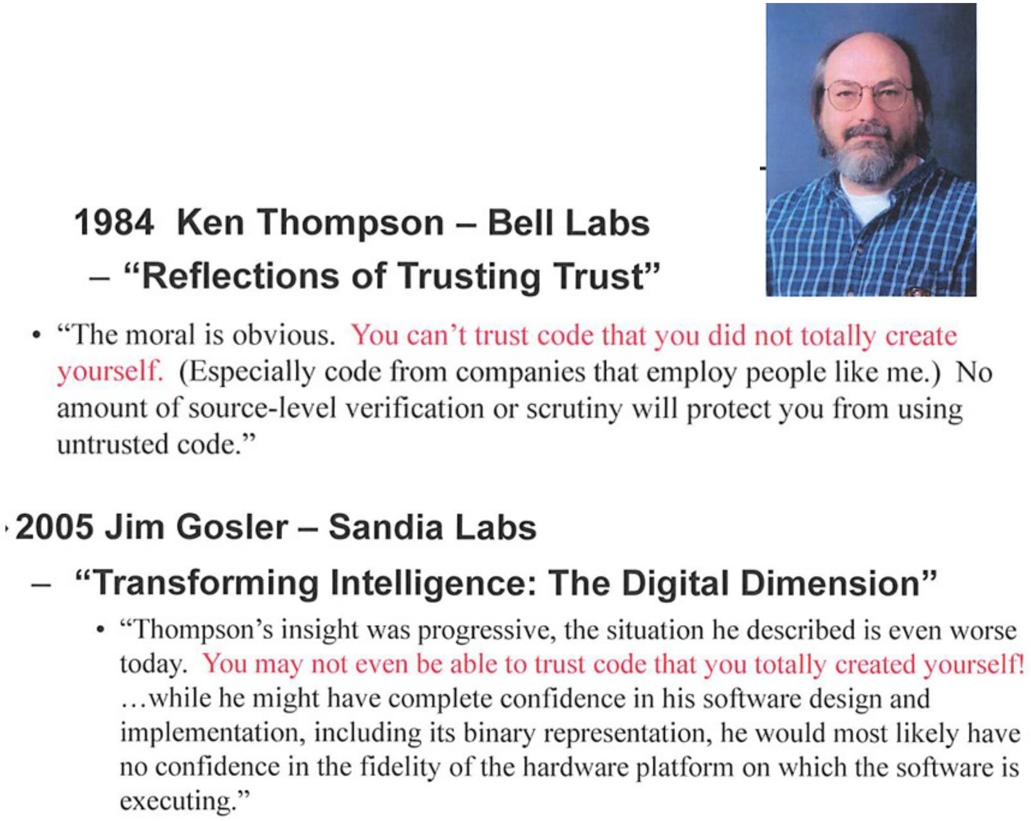
*Report: China Used Tiny Chips to Infiltrate the U.S. Supply Chain – Nextgov

** https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know

Good News

- More involvement and sensitivity about cybersecurity needs including supply chain.
- **NDAA 2021**.
  - Considered to be the most significant effort ever undertaken by Congress to improve national cybersecurity and protect US critical infrastructure from nation-state and noon-state and criminal behavior.
- **EO 10428 Executive Order on Improving the Nation's Cybersecurity**, 12 May 2021
- **NDAA 2022**. In draft. Passed by the HASC with "an eye on improving the cyber workforce."
- 6 October 2021-Civil Cyber-Fraud Initiative (DOJ)
  - Contractor accountability to safeguard public sector information and infrastructure to meet required cybersecurity requirements in order to safeguard public sector information and infrastructure
- **WH National Cyber Security instantiation**
  - National Cyber Director Chris Inglis
  - Cyber and Infrastructure Agency (CISA) – Jen Easterly
  - Deputy National Security Advisor for Cyber and Emerging Technology- Anne Neuberger
  - FBI, DNI, DHS, NSA, Cyber Command,

- **DoD Forms New Task Force to Shore Up Supply Chain** 8 September 2021
  - Address ongoing challenges with its supply chain visibility and resiliency, including ways to mitigate risk.
  - Understand vulnerabilities and the necessary responses
  - Build on existing efforts
- **DOJ Civil Cyber-Fraud Initiative (DOJ)** 6 October 2021-Civil
  - Contractor accountability to safeguard public sector information and infrastructure to meet required cybersecurity requirements in order to safeguard public sector information and infrastructure
  - Holding companies to task for deliberately providing deficient cybersecurity products or services, misrepresenting their cybersecurity practices or protocols, or violating their obligations to monitor and report cybersecurity incidents and breaches.
  - Use the False Claims Act (FCA) to go after contractors and grant recipients for cybersecurity-related fraud by failing to secure their networks and notify about security breaches adequately



1984 Ken Thompson – Bell Labs

– "Reflections of Trusting Trust"

- "The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code."

2005 Jim Gosler – Sandia Labs

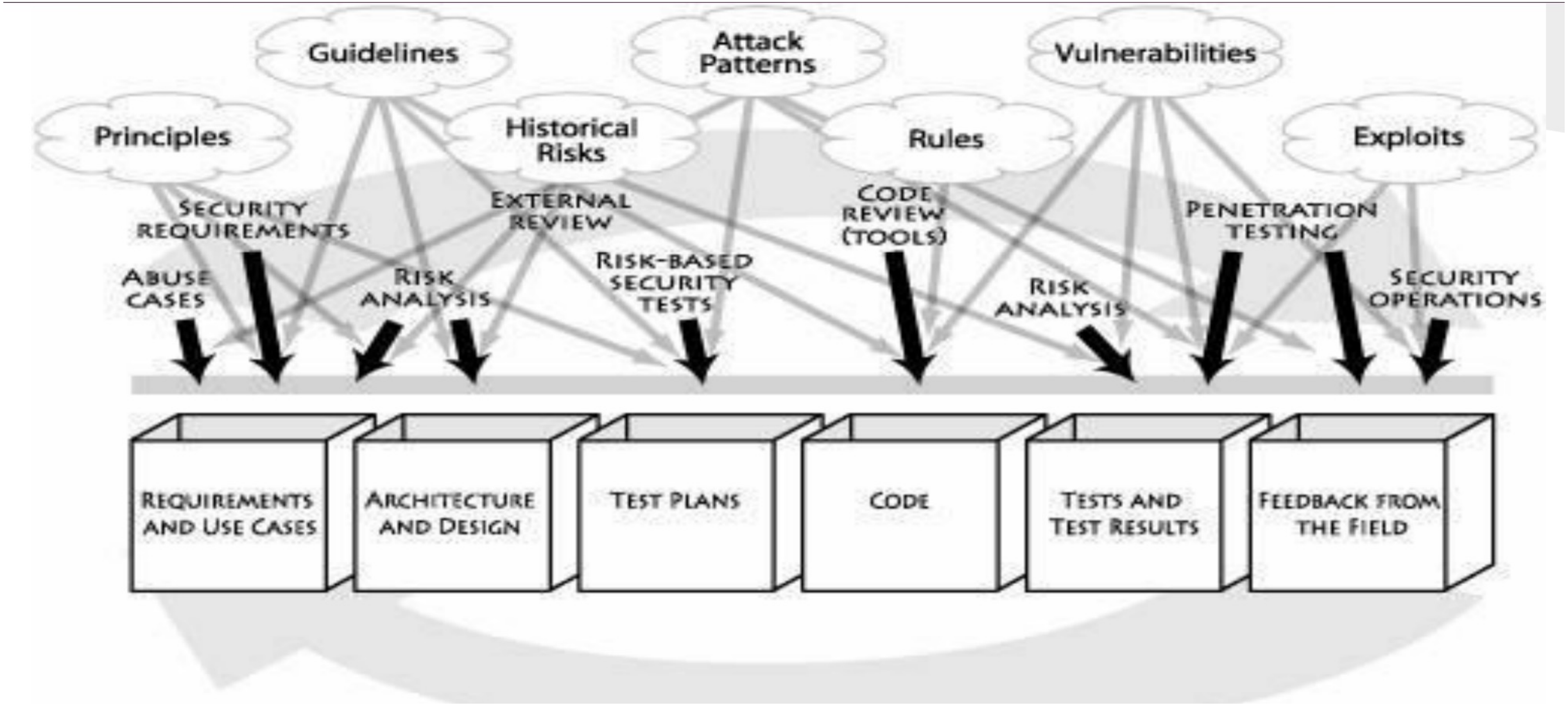
– "Transforming Intelligence: The Digital Dimension"

- "Thompson's insight was progressive, the situation he described is even worse today. You may not even be able to trust code that you totally created yourself! …while he might have complete confidence in his software design and implementation, including its binary representation, he would most likely have no confidence in the fidelity of the hardware platform on which the software is executing."

- **See EO10428 Section 4: "Enhancing Software Supply Chain Security"**
- ***Recommended reading***

- Older, retired technology may provide insights into the algorithms and security built into the product (s)
- This might provide an attack vector on still in use products

Iconic thoughts: With full credit to my friend Jim Gosler, 4 March 2009



Hunter Stevenson, Khalid Alharbi: Software Security (colorado.edu)

- Trust in software begins at the beginning of the software development cycle with creation of the code and continues throughout the life cycle. Rigorous source code analysis throughout development and use
- New threats emerge everyday. The risk environment changes dynamically
- Continuous identification of risks
- Address vulnerabilities from the early stages of S/W development life cycle
- Is your security posture reactive or proactive?
- Technology advances in time can overcome initial product security precautions.
- Age can make a product more vulnerable to attack.

Miscellany

National Risk Management Center – DHS CISA. “Planning, analysis, and collaboration center working to identify and address the most significant risks to our Nation’s critical infrastructure”

Windows 11 and TPM 2.0

- UEFI (Unified Extensible Firmware Interface) firmware, no legacy BIOS allowed, secure boot
- Host integrity at runtime and startup Attestation Certificate Authority (ACA)

Draft NIST SP1800-34B, **validating the integrity of computing devices**. See https//csrc.nist.gov/publications/detail/sp/1800-34/draft

- Joint NIST-Industry effort
- Risk Analysis
- Use of multiple tools developed/developing, e.g., RSA, Intel, Microsoft, others

The best general source materials are found on the NIST and MITRE Websites

CMMC (Cybersecurity Maturity Model Certification)

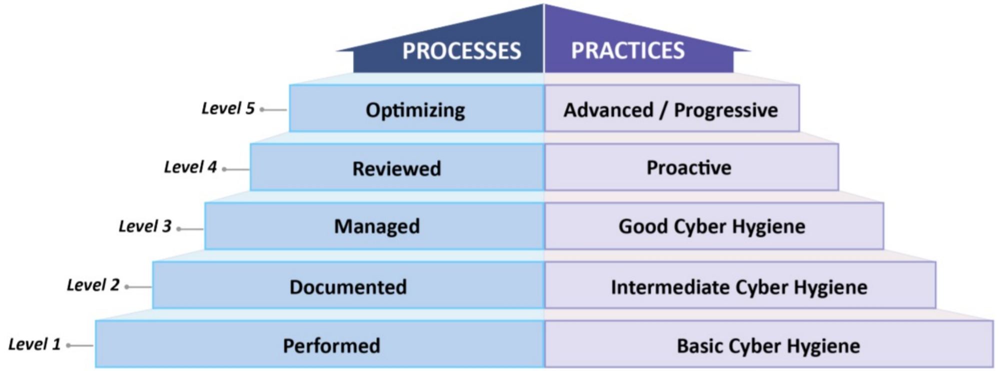
Summary

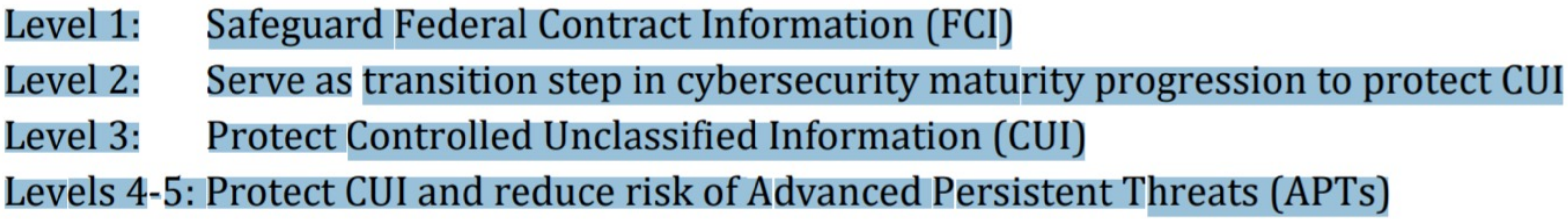
- Supply chains are complex
- Supply chains are generally global
- Vulnerability is ubiquitous
- Voluminous research
  - **Need for a centralized, shareable database**
  - Need useable, verifiable testing technologies
  - Many research challenges
- Need to address hardware end product testing
- Trusted systems. Really?
- Enforceability

" WE COULDN'T HIRE THE CYBERSECURITY CANDIDATE YOU SENT US. HE WAS SAYING TOO MANY SCARY THINGS ABOUT OUR COMPUTERS."

BACKUP SLIDES

CMMC - Cybersecurity Maturity Model Certification

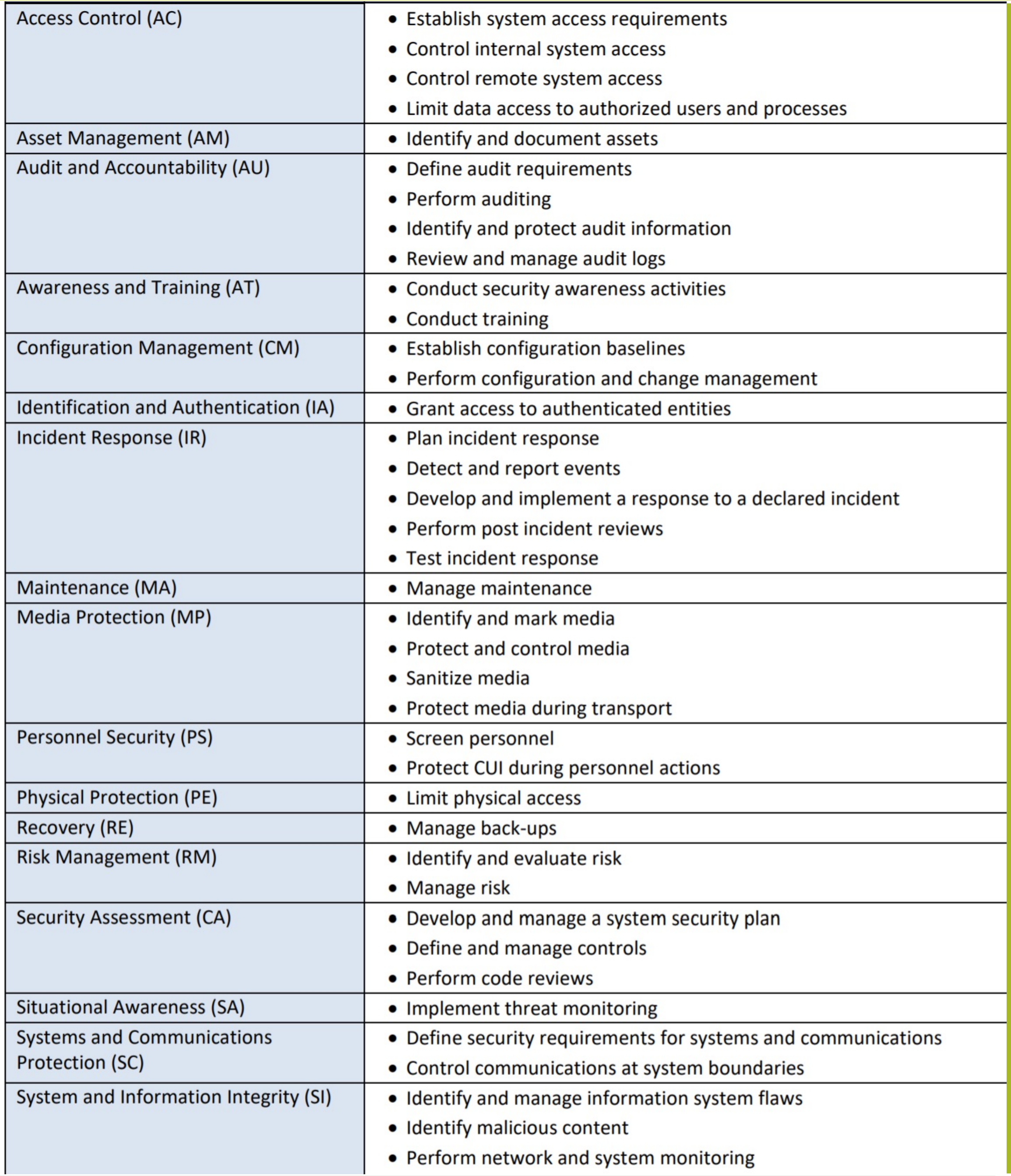



Level 1: Safeguard Federal Contract Information (FCI)
Level 2: Serve as transition step in cybersecurity maturity progression to protect CUI
Level 3: Protect Controlled Unclassified Information (CUI)
Levels 4-5: Protect CUI and reduce risk of Advanced Persistent Threats (APTs)

Introduces cyber rigor in industry performance

Oversight by DCSA

CMMC BACKUP



Access Control (AC)	• Establish system access requirements • Control internal system access • Control remote system access • Limit data access to authorized users and processes
Asset Management (AM)	• Identify and document assets
Audit and Accountability (AU)	• Define audit requirements • Perform auditing • Identify and protect audit information • Review and manage audit logs
Awareness and Training (AT)	• Conduct security awareness activities • Conduct training
Configuration Management (CM)	• Establish configuration baselines • Perform configuration and change management
Identification and Authentication (IA)	• Grant access to authenticated entities
Incident Response (IR)	• Plan incident response • Detect and report events • Develop and implement a response to a declared incident • Perform post incident reviews • Test incident response
Maintenance (MA)	• Manage maintenance
Media Protection (MP)	• Identify and mark media • Protect and control media • Sanitize media • Protect media during transport
Personnel Security (PS)	• Screen personnel • Protect CUI during personnel actions
Physical Protection (PE)	• Limit physical access
Recovery (RE)	• Manage back-ups
Risk Management (RM)	• Identify and evaluate risk • Manage risk
Security Assessment (CA)	• Develop and manage a system security plan • Define and manage controls • Perform code reviews
Situational Awareness (SA)	• Implement threat monitoring
Systems and Communications Protection (SC)	• Define security requirements for systems and communications • Control communications at system boundaries
System and Information Integrity (SI)	• Identify and manage information system flaws • Identify malicious content • Perform network and system monitoring