Global Supply Chain Security for Microelectronics

Supply Chain Traceability Session Report Out – October 28, 2022

26 – 28 October 2022 workshop

Supply Chain Traceability Session

FACILITATOR

Kirsten Koepsel JD LLM
Aerocyonics, Inc.

Supported by the following organizations:

Aerocyonics Inc	Intel Corporation
Battelle Memorial Institute	Johns Hopkins University Applied Physics Laboratory
Booz Allen Hamilton	Micron Technology
Boston Consulting Group	Microsoft
Bowhead Cybersecurity Solutions and Services	NASA
CALCE - UMD	National Institute of Standards and Technology (NIST)
CFD Research	Office of Naval Research
Defense Logistics Agency(DLA)	OUSD(RE), S&TPP
Defined Business Solutions	Performance Review Institute
Draper	SAIC
DUST Identity	Sandia National Laboritories
Global Semiconductor Alliance	Siemens DISW
Golden Altos Corp.	Telecommunications Industry Association
Hewlett Packard Enterprise	The Open Group
Honeywell FM&T	US Army
IBM	US Air Force
Institute for Defense Analyses (IDA)	

Q4a Key Takeaways:

What candidate considerations were discussed and what were the key takeaways?

1. Went through all of them (next slides)

CANDIDATE CONSIDERATIONS

- Traceability
- Supply Chain Illumination
- Provenance
- Pedigree
- Non-Repudiation
- Authentication
- Digital Thread / Physical Thread
- Data Requirements
- Need to add supply chain analysis

TRACEABILITY
CANDIDATE CONSIDERATION

Considerations

- Definition: the ability to verify a relationship between two or more ~~procurement~~ points in the supply chain to determine the provenance of an item
- Definition (traceability analysis): The analysis of the relationships between two or more products of the development process conducted to determine that objectives have been met or that the effort represented by the products is completed. Note: A requirements traceability analysis demonstrates that all system security requirements have been traced to and are justified by at least one stakeholder security requirement, and that each stakeholder security requirement is satisfied by at least one system security requirement. (NIST SP 800-160 Vol 1)
- What about NIST SP 800-161r1 (or NASA SEWP, DHS CISA)?
  - Does it meet the needs of Sec 224 in this area?
  - If not, what needs to happen to leverage it? Or, are there viable alternatives?

Criteria

- What should be the minimal criteria for secure microelectronics used in DoD/NCI systems?

SUPPLY CHAIN ILLUMINATION
CANDIDATE CONSIDERATION

Considerations

- Definition: ~~Continual~~ visibility throughout the supply chain that provides an understanding of the tiers of a supply chain and its internal operations (material transfer and transformation, information transfer and transformation), a supply chain map, and ~~vetting of suppliers against a defined set of supply chain criteria to identify and defend against threats~~
  Note Initial illumination information may include but is not limited to the following any of the following: supplier vulnerability, quality assurance, vetting of suppliers

- *Supply chain illumination provides a measure of visibility into the supply chain*
- *Supply chain visibility is the more common term*
- *Vetting of the suppliers is part of the trusted supply chain but not part of supply chain illumination*

What about NIST SP 800-161r1 (or NASA SEWP, DHS CISA)?

- Does it meet the needs of Sec 224 in this area?
- If not, what needs to happen to leverage it? Or, are there viable alternatives?

Criteria

- What should be the minimal criteria for secure microelectronics used in DoD/NCI systems?

PROVENANCE, PEDIGREE
CANDIDATE CONSIDERATION

Considerations

- Provenance: the chronology of the origin, development, ownership, location, and changes to a system or system component, and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data. Note: Associated data may include validation, verification and/or documentation. (NIST SP 800-161r1)
- Pedigree: The validation of the composition and provenance of technologies, products, and services is referred to as the pedigree. For microelectronics, this includes material composition of components. For software, this includes the composition of open source and proprietary code, including the version of the component at a given point in time. Pedigrees increase the assurance that the claims suppliers assert about the internal composition and provenance of the products, services, and technologies they provide are valid. (NIST SP 800-161r1) Note: for microelectronics, this may include the manufacturing processes associated with the product.
- Comments: provenance and pedigree will be very difficult to trace. See recording for Dan's explanation of pedigree. Take a look at the SAE G-32 diagram of provenance, pedigree, traceability, and non-repudiation. Provenance, traceability, pedigree, and non-repudiation are interlinked as per the diagram.
- What about NIST SP 800-161r1 (or NASA SEWP, DHS CISA)?
  - Provenance Controls: SR-4 (provenance, levels 2,3) (needs tailoring to ME)
  - Does it meet the needs of Sec 224 in this area?
  - If not, what needs to happen to leverage it? Or, are there viable alternatives?

Criteria

- What should be the minimal criteria for secure microelectronics used in DoD/NCI systems?

NON-REPUDIATION, AUTHENTICATION
CANDIDATE CONSIDERATION

Considerations

- Non-Repudiation: Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. (NIST SP 800-60)
- Recommend G-32 definition: the assurance that someone cannot deny the validity of a claim or refute responsibility; For example: tying provenance data into an immutable ledger or adding contractual obligations in a signed contract; electronic or digital signatures
- Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system. (NIST SP 800-171)
- Question as to how authentication is being used in non-repudiation after discussion by attendees of the session
- What about NIST SP 800-161r1 (or NASA SEWP, DHS CISA)?
  - Non-Repudiation Controls: AU-10 (non-repudiation, level 3), IA-4 (Identifier management, levels 2,3), IA-5 (authentication management, level 3)
  - Authentication Controls: Family: Identification and Authentication, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9
  - Does it meet the needs of Sec 224 in this area?
  - If not, what needs to happen to leverage it? Or, are there viable alternatives?

Criteria

- What should be the minimal criteria for secure microelectronics used in DoD/NCI systems?

DIGITAL THREAD / PHYSICAL THREAD
CANDIDATE CONSIDERATION

Considerations

- Identified as a clear gap at ANSI Workshop #1
- Definition: a communication framework that connects traditionally siloed elements in manufacturing processes and provides an integrated view of an asset throughout the manufacturing lifecycle. *(strawman, techtarget.com)*
- *Standards being developed at the circuit board level that should be looked at (IPC Standards- several listed) and JEDEC std also at the component level JEP30*
- *Recommended definitions: Technique to compile product assurance data; method to connect all of the side threads that contain all of the data of which assurance is a sub-set*
- *A closed loop between digital and physical worlds to optimize products, people, processes and places. Note: the digital thread may not be continuous and may be maintained within separate enterprises and data sources. The data set is enabled with synchronization so upstream and downstream information is available to authorized users.*
  - What should be included in the digital thread of assurance data? Notional thought at this time – different answers from manufacturers. Should this be a more pointed question towards assurance requests. Digital thread should have some claim to what is being asked in the assurance claim. What is the assurance claim someone wants?

Criteria

- What should be the minimal criteria for secure microelectronics used in DoD/NCI systems?

DATA REQUIREMENTS
CANDIDATE CONSIDERATION

Consideration

- What data is required? Relates to assurance case and risk tolerance
- Is the data available?
  - Data exists and can be delivered
  - Data does not exist but can be generated
  - Data cannot be made available
  - Data can be available but hard to gather
- When is the data available?
- Can the data delivery be standardized?
- Should this data be requested? Just because you can request it, should you have access to it.
- This question really can't be answered at this point – what is the purpose of the data, what is the efficacy of the data,; are they going to share or not monumental request needing funding; data rights that could require NDAs, contractual requirements; data can come at a cost; need to start identifying what we need and does it exist; needs to be a partnership; manufacturers may be more willing to share processes rather than data

Criteria

- What should be the minimal criteria for secure microelectronics used in DoD/NCI systems?

Q4b Key Takeaways:

What candidate categorization criteria were discussed and what were the key takeaways?

1. Broader understanding of why the terms matter but not a clear understanding of what the threats, weaknesses, vulnerabilities, the risk assessment necessary to evaluate what is acceptable and what is not acceptable and the countermeasures needed
2. To enable this, we are going to need to understand traceability-where the parts come from and where they are going
3. Don’t know what security risk and criticality of the parts. What do we need to use the parts? Customer may need additional mitigations to reduce risk when data is missing
4. Flesh out the traceability matrix for the table using the IPC standard 1782A
5. Define gradation within the terms
6. Currently-use what is practical but also with an eye to the future

Q4c Key Takeaways:

What areas demonstrated the greatest need in terms of relevant regulations, policy, standards, best practices?

1. Discussion of listed references as well as added G-32 JA7496, IPC 1782
2. The existing policy today for DoD is 5200.44
3. Digital thread and JEDEC Part Model to reduce human entry errors into software tools

REGULATION, POLICY, OTHER
REFERENCES

Regulation

-

Policy

- DoDD O-5240.24, *Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)*
- DoD is 5200.44

Other

-

STANDARDS & BEST PRACTICES

REFERENCES (HIGHLIGHTED WERE MENTIONED)

- NIST SP 800-160 v1: Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
- IPC-1782A, Standard for Manufacturing and Supply Chain Traceability of Electronic Products (2021)
- IPC-1782, Standard for Manufacturing and Supply Chain Traceability of Electronic Products (2016)
- IPC 1791A, Trusted Electronic Designer, Fabricator and Assembler Requirements
- ISO/IEC 20243-1:2018: Information technology — Open Trusted Technology Provider Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products — Part 1: Requirements and recommendations
- ISO/IEC 20243-2:2018: Information technology — Open Trusted Technology Provider Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products — Part 2: Assessment procedures for O-TTPS and ISO/IEC 20243-1:218
- SAE AS 5553A Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition
- SAE AS 6081Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition - Distributors

STANDARDS & BEST PRACTICES

REFERENCES

- NIST 800-161r1
- NIST 800-171
- IPC 1783, 1792, 2551, 2581, 2591 and IPC/HERMES 9852
- JEDEC JEP30
- SAE JA7496

Q4d Key Takeaways:

What recommendations does the group have for DoD on next steps?

1. Needs to engage in some of the standards activities to understand what is being written as well as understand feedback in terms of what they need to do
2. Flesh out candidate criteria for each of the considerations
3. Will take work to flesh LoA matrixes but not until after understanding the security risks and the device criticality. Could be done in a smaller group. Candidate criteria would go into the matrix
4. Deep dive of the threats, risks, vulnerabilities and the countermeasures and efficacy.

Questions / Discussion?