NDIA Systems & Mission Engineering Conference
November 1-3, 2022
Orlando, FL

Cyber Supply Chain Risk Management a System Security Role in the Future of Systems Engineering

Holly Dunlap
Hdunlap@MITRE.org
850-796-6510

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Holly Dunlap Cyber Supply Chain Risk Management SME

MITRE LABS
Cyber Solutions Innovation Center Division
Cyber SCRM, Principal System Security Engineer
Supply Chain Security System of Trust (SoT)

Raytheon Missiles & Defense (+15 years)

- NDIA System Engineering Division Elected Chair (+13 Committees, +500 members; government, industry, academia, FFRDC)
- NDIA System Security Engineering Committee Chair, +9 years
- Systems Engineering Council – Cyber Resiliency & System Security Project Lead
- Cyber Enterprise Campaign
- CODE Center
- PI Security & Trustworthy Foundations for Electronics Resurgence (STryFER) IDIQ CRAD Proposal
- Defense & Intelligence Programs

Ktech Later Acquired by RTN RMS

- USD(I) Contract Supply Chain & Logistics Layered Analysis; Data & Information Exploitation. 18 month effort.

OSD DDR&E Technical Intelligence, Pentagon +3 years

- Emerging & Disruptive Technology. Investment strategy to ensure US technical capability advantage. Work intimately with Anti-tamper Executive Agent, National & Defense Intelligence Community, and Defense System Developers. Strategic 15 – 20 Year Planning.

10 years Nuclear Weapons, National Nuclear Security Administration (NNSA) Kansas City Plant, M&O Honeywell

- 3 Year Rotational Leadership Development Program (10 years experience in 3 years)
- Certified 6 Sigma Black Belt – Microelectronics

BS Electrical Engineering & MBA

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Introduction

- Microelectronics hardware, software, and firmware are the keys to technological superiority, but also house extensive opportunities for cyber attack.
- Lurking in the interconnected value-added global microelectronics supply chain networks are new challenges relating to the lack of control, transparency, visibility, integrity, availability, and confidentiality.
- As the logic bearing component supplier base increases, high assurance systems becomes more reliant on each contributing participant to ensure that these challenges are addressed.
- Managing the cyber risks to these new technology and capability supply chains' forms the basis and need for new academic disciplines and skillsets.
- The associated global supply chain security challenges and risks are not currently addressed and integrated holistically into System Security Engineering education, training, or roles and responsibilities.
- Therefore, this article proposes the development and formalization of Cyber Supply Chain Risk Management (C-SCRM) Engineering as new role and responsibility.

Cyber Supply Chain Risk Management Engineering in the Security Future of Systems Engineering

Introduction

Microelectronics

- Logic-bearing components include Application Specific Integrated Circuits (ASICs), Field-programmable gate arrays (FPGAs), Single Board Computers (SBCs), Complex programmable logic devices (CPLDs), microcontrollers, and other programmable devices.
- According to GlobalFoundries, a specialized component in an Apple iPhone is made up of 8.5 billion transistors and each transistor 10,000 times smaller than a human hair. These transistors control the electrons through a circuit and provide today's computing power.
- ASICs provide the greatest opportunity for efficiency in size, weight, and power to achieve optimal performance.
- Field Programmable Gate Arrays (FPGAs), provide a compromise of both worlds COTS & Custom but does not achieve the premier performance of ASICs.
- Both ASICS and FPGA ICs often include billions of transistors.
- Producing a single microelectronics component may include 5 to 50 different suppliers with multiple entities contributing to each stage of design, manufacturing, test, and packaging. And every entity or suppler has risks for adversarial cyber attack.

BACKGROUND

Traditional Supply Chain Risk Management vs Cyber Supply Chain Risk Management

TRADITIONAL SUPPLY CHAIN RISK MANAGEMENT

Supply chain risk management is traditionally focused on component quality, supplier stability, affordability, and the ability of these suppliers to reliably deliver components to meet just-in-time production schedules.

The ultimate risk in the traditional supply chain is that the systems integrator will not be able to procure and receive quality components needed to build a system.

CYBER SUPPLY CHAIN RISK MANAGEMENT

The cyber risk in the supply chain faces the risk "*that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.*"

The ultimate cyber risk in the supply chain is not that a systems integrator will procure or receive a counterfeit or maliciously modified component; the risk is that such a component will go undetected and be integrated into a critical system that requires high assurance with national security implications.

DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

Vision:

- C-SCRM Engineering as a role within System Security Engineering, with official recognition and ample resources, will provide a stable foundation for an integrated defense against cyber exploited weaknesses and vulnerabilities resident in the supply chain of logic bearing components.

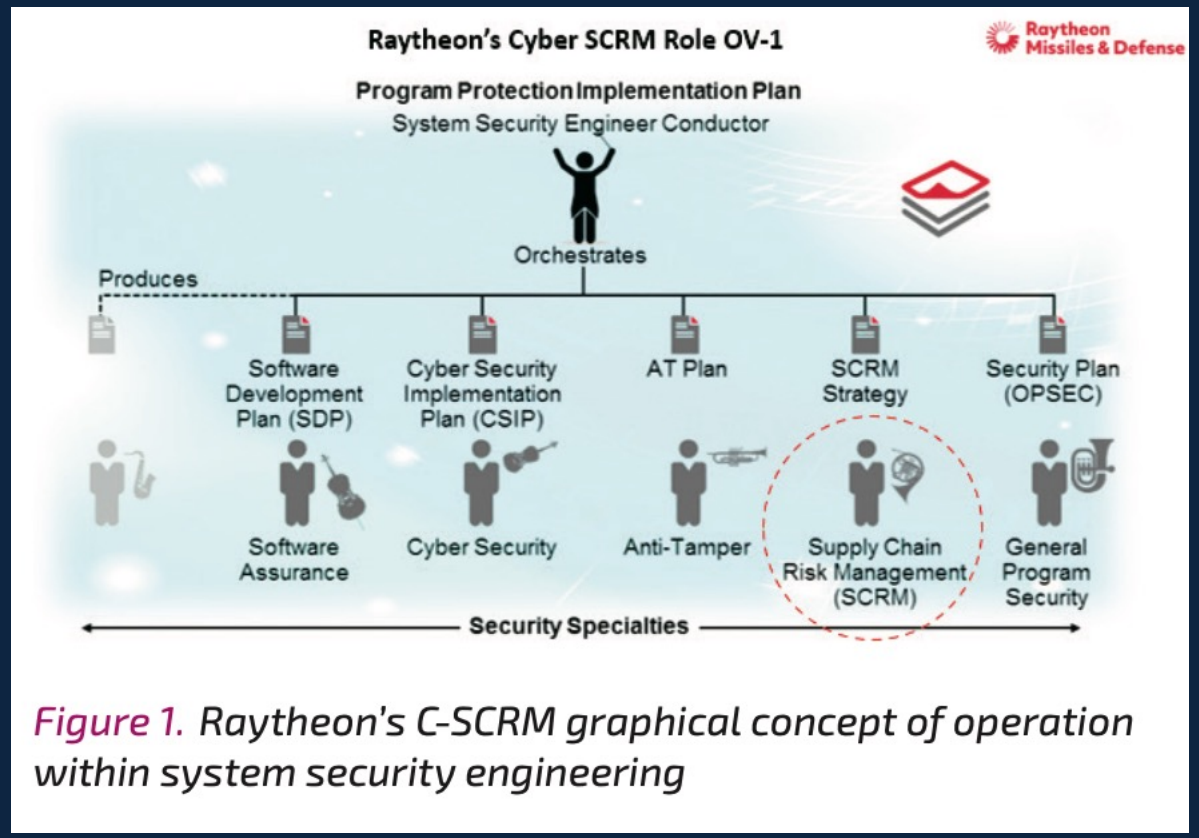

Figure 1. Raytheon's C-SCRM graphical concept of operation within system security engineering

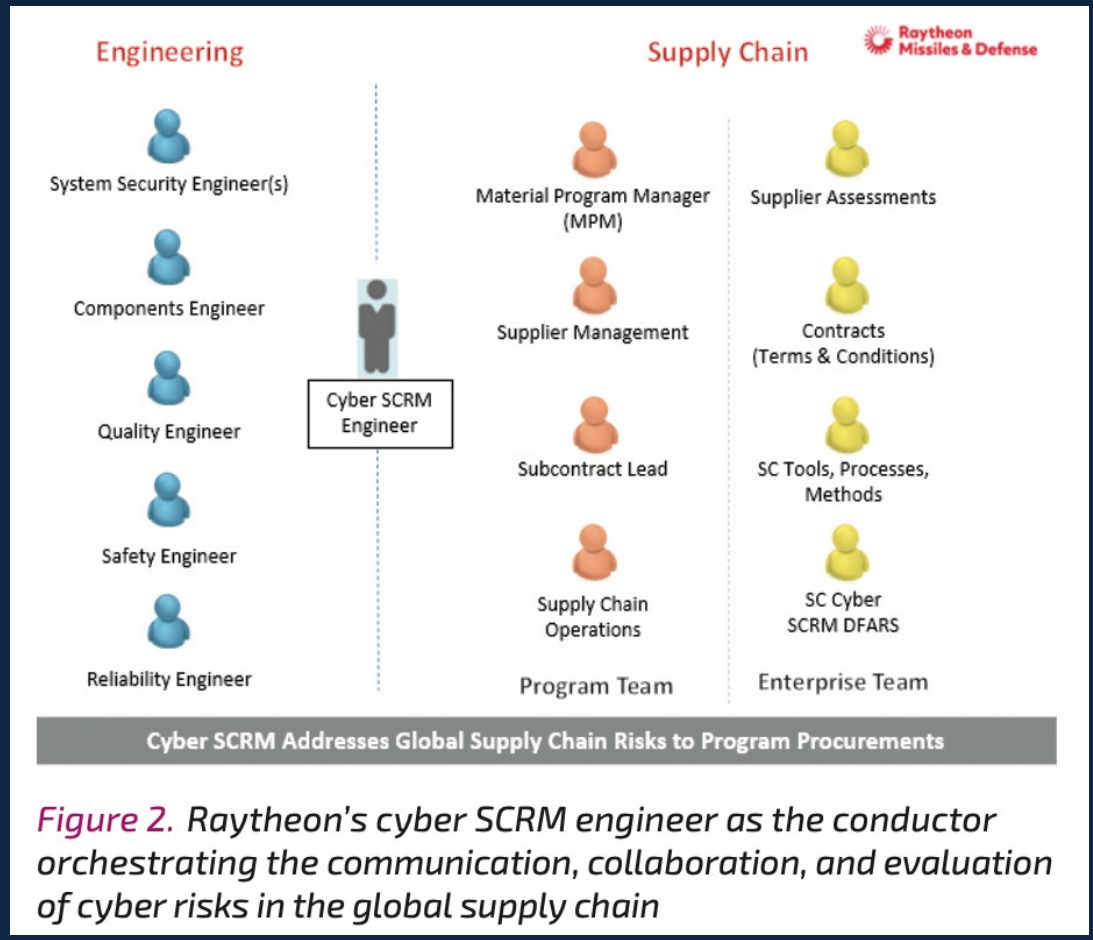

Figure 2. Raytheon's cyber SCRM engineer as the conductor orchestrating the communication, collaboration, and evaluation of cyber risks in the global supply chain

Current State:

- C-SCRM for product security lacks dedicated and recognized leadership roles, a common security framework, and coordination of effective strategies. Without leadership, there is no empowered advocate to bring together the disparate and diverse community of stakeholders and range of countermeasures essential to effectively manage the cyber risks within the global supply chain.
- The creation of a C-SCRM role in engineering provides a stable locus for an integrated and coordinated response to cyber threats in the supply chain. With official recognition, this role can serve as the connective tissue for disparate efforts and unique needs of the diverse range of stakeholders who are essential to C-SCRM. If provided adequate resources, this role can provide guidance along with a common security framework for C-SCRM strategies that have been proven successful, as well as promising new countermeasures, which require expertise and holistic systems awareness to effectively implement.
- Without this role, C-SCRM efforts will remain dangerously isolated, lacking a unified threat matrix mapping to coordinated and characterized countermeasures. Each supplier will continue to represent a potential vector for malicious actors to launch deliberate and targeted attacks. The logic bearing component supply chain will continue to feature layered vulnerabilities, rather than layered security.

Cyber-SCRM Engineering Overlay

11 foundation concepts included in the Security FuSE Roadmap

Concept 1	C-SCRM Engineering Proficiency in the SSE Team
Concept 2	C-SCRM Education and Competency Development
Concept 3	C-SCRM Stakeholder Alignment
Concept 4	Extending Safety and Mission Assurance Failure Modes Effects and Criticality Analysis (FMECA) to derive C-SCRM requirements for procurements and subcontractor build to specifications
Concept 5	C-SCRM Architecture Framework to provide program layered defense solution diversity and agility
Concept 6	Operational Agility through C-SCRM Forensics
Concept 7	Capability-Based C-SCRM Engineering
Concept 8	Security as a functional requirement in the procurement of products, subcontracts, and services.
Concept 9	Assurance modeling for Cyber SCRM to increase confidence in component authenticity and integrity.
Concept 10	C-SCRM Orchestration
Concept 11	Concept 11: Techno-Social Contracts

11 foundation concepts included in the Security FuSE Roadmap

Concept 1: C-SCRM Engineering Proficiency in the SSE Team	
Problem to Address	Insufficient knowledge of holistic approaches to managing risks posed by the distributed global supply chain.
Need to Fill	A formally recognized new role for C-SCRM Engineering as a responsibility within System Security Engineering.
Barriers to Overcome	Formal recognition and ownership by Engineering. Partnership with Supply Chain, Quality, Mission Assurance, and Whole Life is essential but Engineering and specifically SSE must own to address the technical security requirements and manage the global supply chain cyber threats and vulnerabilities.
Concept 2: C-SCRM Education and Competency Development	
Problem to Address	Cyber-attack vectors in the microelectronics hardware, software, firmware, and their interconnected value-added global supply chain networks lack holistic integration into SSE education, creating a skills gap.
Need to fill	Education and proficiency development to manage distributed global supply chain risks that accompany procuring components and skills to create program material security strategy with subcontractors.
Barriers to Overcome	Perception that the existence of mitigations and countermeasures in the form of processes, technologies, tools, and testing are evaluated, selected, and integrated with intent during the procurement process. Just because mitigations exist, does not mean they are used in a layered defense approached today.
Concept 3: C-SCRM Stakeholder Alignment	
Problem to Address	No formally recognized holistic set of requirements or guidance to drive stakeholder needs to an integrated tailored set of system solutions that manage cyber risks in the supply chain.
Need to fill	C-SCRM trade space-based risk mitigations or countermeasures catalog. (For cost, risk, and performance.)
Barriers to Overcome	Common framework and set of metrics and measures for evaluating mitigation effectiveness in context of a system and its intended operational environment.

Foundation concepts 4-6 included in the Security FuSE Roadmap

Concept 4: Extending Safety and Mission Assurance Failure Modes Effects and Criticality Analysis (FMECA) to derive C-SCRM requirements for procurements and subcontractor build to specifications	
Problem to Address	Suppliers and subcontractors are often selected early in a program proposal or system development lifecycle before system security risks are considered.
Need to fill	Extending FMECA to a program's bill of materials analysis to influence supplier selection and procurement and subcontractor technical security requirements.
Barriers to Overcome	Tools to analyze and visualize system bill of materials (BOM), BOM decomposition, logic bearing component (hardware, software, and firmware) identification, and FMECA results. Ensure the term "Program Critical Suppliers" includes C-SCRM criteria. "Program Critical Suppliers" definition may currently include criteria beyond security considerations (cost, single source, financial stability, geographical relocation, etc.)
Concept 5: C-SCRM Architecture Framework to provide program layered defense solution diversity and agility	
Problem to Address	No composable OpenSystems architecture to design blocks with security attributes.
Need to fill	Hierarchical architectural contracts using modeling languages such as SysML, AADL, DSL, RUST connecting to design blocks with security profiles.
Barriers to Overcome	Interoperability of modeling languages. Development and adoption of domain security profiles.
Concept 6: Operational Agility through C-SCRM Forensics	
Problem to Address	No ability to characterize and determine intentional verses unintentional failures.
Need to fill	Analysis of failures to differentiate the root cause to include quality, counterfeit, and malicious modification. Ability to identify, analyze, isolate, and respond to component failures.
Barriers to Overcome	Access to component provenance and pedigree data to forensically analyze root cause of failures, develop trends, and indicators to predict failures from unintentional and intentional based effects.

Foundation concepts 7-9 included in the Security FuSE Roadmap

Concept 7: Capability-Based C-SCRM Engineering	
Problem to Address	Security strategies are based on known available (limited view) solutions or pre-determined (selected) supplier security offerings.
Need to fill	Establish C-SCRM risk-based framework with technical requirements to drive desired results.
Barriers to Overcome	The risks are not simply addressed by flowing down policy or federal acquisition requirements in contracts. Effective technical C-SCRM demands critical thinking to develop the tailored derived requirements and ensure those requirements are implemented and executed to deliver components that meet an acceptable program risk tolerance.
Concept 8: Security as a functional requirement in the procurement of products, subcontracts, and services.	
Problem to Address	As a non-functional requirement, system security does not get prime SE attention. Product security requirements are often absent in contracts for suppliers and subcontractors.
Need to fill	Establishment of a C-SCRM Engineering role responsible for the overall Supply Chain product security architecture to include procurements, subcontracts, and services.
Barriers to Overcome	The assumption that product technical security requirements and criteria are magically integrated into supplier selection, data and information management, transportation and logistics, and testing requirements. DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting contributes but does not directly address product security. DFARS 7012 addresses information protection related to products on business system IT networks.
Concept 9: Assurance modeling for Cyber SCRM to increase confidence in component authenticity and integrity.	
Problem to Address	NIST Risk Management Framework controls and checklist approaches for compliance without expertise and critical thinking are ill-equipped to increase customer confidence in the system's assurance level.
Need to fill	Reinvigorate formal methods of data driven evidence to support claims of assurance while embracing digital engineering analysis and automation tools.
Barriers to Overcome	Lack of skilled and experienced system security and C-SCRM engineers with elevated critical thinking and system domain experience.

Foundation concepts 10-11 included in the Security FuSE Roadmap

Concept 10: C-SCRM Orchestration	
Problem to Address	No identified role responsible for translating technical product security requirements to the supply chain and contracting community. The supply chain and contracts team are the mechanism in which technical requirements authored are communicated from the engineering teams to suppliers and subcontractors. Disparate cyber global supply chain risk mitigations range from emerging technology to proven solutions with little to no ability to latch them together for a holistic approach. No ability to easily compare mitigations to assess their effectiveness and value.
Need to fill	A formal C-SCRM role within SSE responsible for orchestrating collaboration and communication across the engineering community and translate technical product security requirements to supply chain suppliers and subcontracts statements of work requirements in contracts. A visible and accessible C-SCRM semantic ontology risk mitigation catalog for technical capability cyber supply chain risk mitigation selection and orchestration.
Barriers to Overcome	No obvious advocate, champion, or leader with influence and resources to bring the disparate and diverse community together.
Concept 11: Techno-Social Contracts	
Fulfilling the C-SCRM overlay of the FuSE foundational concepts 1-10 provides procured components and subsystems at an acceptable level of risk. Successful execution of C-SCRM enables agile, resilient, and secure system capability options composed of an integrated set of high assurance critical components to support the Techno-Social Contract concept in fielded operations.	

Conclusion

The geographically distributed globally connected supply chain provides unprecedented access to legacy, state of play, and leading-edge advanced technology but with it comes layers of complex threats and vulnerabilities presenting potential cyber risks to the supply chain and therefore our products and services. The breadth and depth of the opportunities and rising challenges establishes the need to develop a new Cyber SCRM Engineering role as a System Security Specialty within Systems Engineering to focus investments, coordinate and collaborate with disparate communities, and develop repeatable and reliable methods for evaluating and reducing global supply chain risks.

Cited Works:

NIST. (2018). Risk Management Framework for Information Systems and Organizations.
NIST Special Publication 800-37, Revision 2. Gaithersburg, MD: National Institute of Standards and Technology.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

NIST. (2020). Security and Privacy Controls for Information Systems and Organizations.
NIST Special Publication 800-53, Revision 5. Gaithersburg, MD: National Institute of Standards and Technology.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

NIST. (2018). Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
NIST Special Publication 800-160 Vol. 1, Gaithersburg, MD: National Institute of Standards and Technology.
https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final

NIST. (2021). Cyber Supply Chain Risk Management Practices for Systems and Organizations
NIST Special Publication 800-161 Rev. 1 (Draft). Gaithersburg, MD: National Institute of Standards and Technology.
https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/archive/2021-04-29

Rick Dove, Tom McDermott, Delia Pembrey MacNamara, Keith Willett, Holly Dunlap, Cory Ocker
"Security in the Future of Systems Engineering (FuSE), a Roadmap of Foundation Concepts", 31st Annual INCOSE International Symposium, 2021
http://www.parshift.com/s/210717IS21-FuseSecurityRoadmap.pdf

Joel Heebink, “Zero Trust for Hardware Supply Chains: Moving from Absolute Trust to a Quantifiable Assurance Model”, NDIA 2021 Virtual Systems and Mission Engineering Conference.
https://ndia-se21.visiond.com/en/NDIA-1596229109/SE21/tab-embed.php?eventTabID=1659094

References

Daniel DiMase, Zachary A. Collier, John Chandy, Brian S. Cohen, Gloria D'Anna, Holly Dunlap, John Hallman, Jay Mandelbaum, Judith Richie,
"A Holistic Approach to Cyber Physical Systems Security and Resilience," 2020 IEEE Systems Security Symposium (SSS), 2020, pp. 1-8, doi: 10.1109/SSS47320.2020.9197723.
https://ieeexplore.ieee.org/document/9197723/authors#authors

Rick Dove, Tom McDermott, Delia Pembrey MacNamara, Keith Willett, Holly Dunlap, Cory Ocker
"Security in the Future of Systems Engineering (FuSE), a Roadmap of Foundation Concepts", 31st Annual INCOSE International Symposium, 2021
http://www.parshift.com/s/210717IS21-FuseSecurityRoadmap.pdf

Report of the Defense Critical Supply Chain Task Force, House Armed Services Committee, July 22, 2021
https://armedservices.house.gov/_cache/files/e/5/e5b9a98f-9923-47f6-a5b5-ccf77ebbb441/7E26814EA08F7F701B16D4C5FA37F043.defense-critical-supply-chain-task-force-report.pdf

Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War
Author: Chris Nissen, John Gronager, Robert Metzger, Harvey Rishikof
https://www.mitre.org/sites/default/files/publications/pr18-2417-deliver-uncompromised-MITRE-study-26AUG2019.pdf

Koon, J 2021, ' Complex Chips Make Security More Difficult', Semiconductor Engineering Deep, Insights for the Tech Industry
4 November, viewed 15 November 2021,
<https://semiengineering.com/complex-chips-make-security-more-difficult/>.