SAND2014-15484C

Supply Chain Lifecycle Decision Analytics

Gio Kao, Han Lin, Brandon Eames, Jason Haas, Alexis Fisher,
John Michalski, Jon Blount, Jason Hamlet, Erik Lee, John Gauthier,
Gregory Wyss, Ryan Helinski, Dustin Franklin@
Sandia National Laboratories
Albuquerque, New Mexico
Laura McLay, lmclay@wisc.edu, University of Wisconsin-Madison

Abstract— **The globalization of today's supply chains (e.g., information and communication technologies, military systems, etc.) has created an emerging security threat that could degrade the integrity and availability of sensitive and critical government data, control systems, and infrastructures. Commercial-off-the-shelf (COTS) and even government-off-the-self (GOTS) products often are designed, developed, and manufactured overseas. Counterfeit items, from individual chips to entire systems, have been found in commercial and government sectors. Supply chain attacks can be initiated at any point during the product or system lifecycle, and can have detrimental effects to mission success. A report by the United States Government Accountability Office IT Supply Chain: National Security-Related Agencies Need to Better Address Risks, GAO-12-361, states that the Departments of Energy, Homeland Security, Justice, and Defense lack sufficient capabilities to address global supply chain risks [7].**

To date, there is a lack of analytics and decision support tools used to analyze supply chain security holistically, and to perform tradeoff analyses to determine how to invest in or deploy possible mitigation options for supply chain security such that the return on investment is optimal with respect to cost, efficiency, and security. The goal of this research and development (R&D) effort is to develop a comprehensive decision analytics framework that includes the development of a holistic end-to-end supply chain lifecycle vulnerability, mitigation assessment methodology and decision support optimization methodology to minimize overall supply chain risk.

This paper discusses the development of a supply chain decision analytics framework that will assist decision makers and stakeholders in performing risk-based cost-benefit prioritization of security investments to manage supply chain risk. Key aspects of our framework include the hierarchical supply chain representation, vulnerability and mitigation modeling, risk assessment and optimization. This work is a part of a long term research effort on supply chain decision analytics for trusted systems and communications research challenge.

***Index Terms*—Security, Integrity, Supply chain, Risk, Supply chain risk management**

I. Introduction

The USG is heavily dependent on supply chains that are highly complex with diverse geographic locations and a globalized conglomeration of internetworks at a very large scale. The complexity reduces the transparency of the supply chain at every level of involvement. This includes people, organization, processes, services, sources, products, and infrastructure. National Institute of Standards and Technology (NIST) special report 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organization reports that the complexity, diversity, and scale of the supply chains reduce the visibility and understanding of how the supply chain technology is being acquired, developed, integrated, and deployed. The government currently lacks the visibility, understanding and control over these supply chains. Although a brief synopsis of root causes is provided, the focus of this report is not to identify the root causes of these complex supply chains. Understanding the root cause may not solve the existing supply chain problems. However, it may help provide insights into better securing our supply chain for the future. The genesis of these highly complex and convoluted supply chains may be traced to several interrelated root causes such as:

- Technology advancement
- Demand competition and specialization
- Cost and profits

In recent decades, the rapid advancement in technology can be attributed to an increasingly globalized economy that has intensified competition and driven innovation and technology advancement. Consequently, making supply chain risk decisions to be more complicated than ever before. According to the director of Department of Defenses (DoD) Defense Microelectronics Activity (DMEA), "the defense community is reliant critically on a technology that becomes obsoletes every 18 months, and is made in unsecure locations over which the USG does not have market share influence" [12]. As a result, DoD is limited to utilize independent distributors and brokers that are highly susceptible to counterfeit threats.

Given today's global supply chain management, it is extremely challenging to fully comprehend the supply chain vulnerabilities due to its inherent complex corporate structures and distribution networks. Examples are: component complexity (e.g., too many unique components), supplier complexity (e.g., too many sub-suppliers), process complexity (e.g., too many steps), and service complexity (e.g., too many outsourced services). Supply chain vulnerabilities pose threats ranging from quality issues (e.g., counterfeits) that lead to

reliability of the end system to malicious intent by actors to compromise confidentiality, integrity, or availability of end systems. To illustrate the criticality of the supply chain problem, the following are examples of recent supply chain vulnerabilities:

- Senator Carl Levin and Senator John McCain reported to the Senate Armed Services Committee that many of the DoD supply chains have been compromised by counterfeit electronic parts. The number of counterfeit incidents being detected rose from 3,868 incidents in 2005 to 9,356 incidents in 2008. Counterfeit electronic parts increasingly pose a risk to national security and the reliability of U.S. defense systems. [12]

- A recent GAO report 12-361 found that four national security-related departments, [the Department of Energy (DoE), Department of Homeland Security (DHS), Department of Justice, and DoD] are inadequate in countering the information technology (IT) supply chain threat. Lacking are protective measures, monitoring capabilities, and policies to address the threat. Also lacking are monitoring capabilities to verify compliance with and effectiveness of any such counter measures. Reported threats to the IT supply chain include [7]:

    - Installation of hardware or software containing malicious logic
    - Installation of counterfeit hardware or software
    - Failure or disruption in the production of distribution of critical products
    - Reliance on a malicious or unqualified service provider for the performance of technical services
    - Installation of hardware or software that contains unintentional vulnerabilities

- A notable supply chain attack incident occurred during August 2004 to March 2005 when more than 100 mobile phones belonging to members of the Greek government were illegally wiretapped. Switches made by Ericson were compromised through software upgrades. Rootkit was installed to enable wiretapping while disabling audit logs [5].

II. Current Approaches

Traditional supply chain risk management (SCRM) processes have focused on the availability of supply and avoiding disruptions while minimizing cost (e.g., due to natural disaster impacts). Today, management of supply chain security and integrity needs to consider the entire sequence of events that bring raw material from its source of supply to ultimately the customer (end-to-end). This becomes challenging when trying to develop holistic analytics. Risks to the end receiver typically are judged with respect to schedule and cost. Only recently has the risk of maliciously altered components been acknowledged. Decision makers have limited control and influence over a supply chain network due to globalization (foreign supplier operations). Limited approaches in the open literature address supply chain vulnerabilities. This section provides a brief overview of current work.

A variety of reports acknowledge that the supply chain problem is a real threat [7] [14][12][16]. Limited works exist on how to address the problem. Since the start of the Comprehensive National Cybersecurity Initiative (CNCI) in 2008, few major publications have addressed the supply chain risk. These reports primarily are in the information communication technology (ICT) area including the Information Assurance Technology Analysis Center (IATAC) State-of-the-art Report (SOAR) in 2010, and a series of NIST guidelines, namely NIST SP 800-161, NIST 800-53r4, and NIST IR 7622 [3] [8] [2] [6]. The DoD acquisition office also provided guidance on developing Program Protection Plans (PPP) and managing supply chain risk over the lifecycle of a program.

The 2010 SOAR focused specifically on the ICT supply chain [8]. It identified ICT supply chain threats that generalized into two high-level categories: threats to the supply chain process and threats to products in the supply chain. These threats affect four components of assurance, integrity (not tampered), authenticity (not counterfeited), trustworthiness (not malicious or defective), and availability (not disrupted). SOAR described several potential scenarios that might manifest these threats. Based on open literature research and SME reports, tampering can occur during fabrication, testing, packaging, and physical distribution. The report suggested two generalize approaches, one of risk avoidance and the other of mitigation. The avoidance approach implied "custom-built" government-owned suppliers that are required by certain highly critical products that have unquantifiable consequences if compromised or inadequate mitigation options to contain supply chain risk. Alternatively, the mitigation approach included leveraging highly well-vetted "trusted suppliers" and application of best practices for other critical products. SOAR outlined and described a list of mitigation classes:

- Reduce exposure
- Inventory control
- Increase transparency of supply chain flow (product and data)
- Increase accountability
- Increase security of supply chain management data flow
- Improve security requirement and evaluation of acquisitions
- Secure version and configuration control for IP and product development

- Develop product assurance measure
- Improve tamper-proofing
- Provenance and pedigree analysis
- Detect malicious intrusion
- Evolve system engineering resilience techniques
- Practice avoidance and custom production

The SOAR report included an overview of various SCRM initiatives across government agencies to foster security improvement, e.g., acquisition security initiatives, SCRM policy guidelines, anti-counterfeiting initiatives, and supply chain intelligence initiatives.

NIST published several guidelines addressing supply chain risk. High-level supply chain risk mitigation measures suggested in their guidelines include:

- Conduct due diligence review of suppliers (hardware, software, firmware, services) prior to acquisition
- Use trusted shipping and warehousing
- Employ independent analysis and penetration testing.

NIST 800-53r4, NIST SP 800-161 and NIST IR 7622 are recent major publications on ICT SCRM. NIST 800-53r4 covers general security and privacy controls guidelines. The latest revision (4) provides new additional guidance on applying security control measures to mitigate supply chain risk [6]. It establishes a security control baseline that lists supply chain protections SA-12(1-15). The report states that a significant challenge is to determine the most cost-effective, appropriate set of security controls, which if implemented and determined to be effective, would mitigate risk. Depending on the criticality of the system, the guideline suggests initially establishing baseline security controls.

Once the baseline is identified, additional security controls are to be considered for tailoring to the specific system and organization. A security control catalogue is used to provide guidance on what additional protection points and best practices might be implemented. The final security controls are documented and evaluated based on a review board of SMEs to ensure that adequate protections are implemented.

NIST SP 800-161 is an initial public draft published by NIST for review at the time of this report [3]. The draft provides guidance on supply chain management practices to identify, assess, and mitigate ICT supply chain risks for federal information systems and organizations. The report proposes a four stage process in SCRM:

1. Frame —establish the context for risk-based decisions and the current state of the system or ICT supply chain environment,
2. Assess —review and interpret threat, vulnerability, and related information,
3. Respond —select, tailor, and implement mitigation controls, and
4. Monitor —continue to monitor changes to information system or supply chain environment, using organizational communications and feedback loop for improvements.

In order to address the complexity of the supply chain problem, the report suggests a three tiered risk management approach. The first tier begins at the organization level to set broad strategic directions. The second tier is the mission/business level that influence program requirements such as cost, schedule, performance and other "ilities" (e.g., reliability, availability, etc.). The third tier occurs at the information systems level that influences system level details. Those details include such as requirements, architectural design, development, delivery, installation, integration, maintenance, and retirements. The SCRM process overlaps across all three tiers. The "frame" step helps set assumptions, constraints, risk tolerances and priority trade-offs. The "assess" step collects available data to conduct risk assessment. Assessment includes performing criticality analysis, vulnerability analysis, and threat analysis to determine the likelihood of adversarial exploitation. NIST SP800-161 suggests that critical functions identified through criticality analysis are used for vulnerability and threat assessment. In the context of the report, vulnerability assessment is done on systems or components to identify weakness of design, development, production, or operations that can be exploited. In the respond step actionable mitigation control options (based on the assessment step) are performed to reduce supply chain risk. Decision makers are provided with alternatives such that assumptions, constraints, and trade-off tolerances are met as determined in the organizational level analysis. Finally, the "monitor" step allows for program and projects to be routinely evaluated to maintain or adjust the risk posture.

NIST IR 7622 provides a notional set of repeatable and commercially reasonable supply chain assurance methods and practices offering an understanding of, and visibility throughout, the supply chain [2]. Most of the practices and procedures suggested in this report are based on NIST SP 800-53r4. The report details suggested activities that would help implement each of the SA-12 supply chain protection checklist based on roles (i.e., Acquirer, Integrator, and Supplier).

The DoD Acquisition, Technology and Logistic (AT&L) provides additional guidelines and requirements for any DoD acquisition process [1]. This includes establishment of a Program Protection Plan (PPP) that, in part, addresses supply chain risk. Consistent with NIST guidelines, the DoD AT&L's process in establishing a PPP starts with performing criticality analysis based on critical program information. Critical functions then are analyzed for threats and vulnerabilities. Collected data are used for risk assessment and identification of mitigation options.

The majority of the NIST and AT&L papers provide high-level abstraction of supply chain threats, vulnerabilities, and mitigations. They suggest performing criticality analysis, threat analysis, and vulnerability analysis. The assumption is that one can readily identify the threat, vulnerabilities, and consequences, and therefore apply the proposed mitigation actions. There is a lack of metrics to measure or quantify effectiveness, and a lack of tools to perform vulnerability assessments of the supply chain. These processes focus on identifying what the risks are. They do not address how these threats can be realized, which is critical in understanding the supply chain vulnerability space. Heavy focus on criticality analysis neglects the concept of adversaries leveraging the easiest and most accessible avenues of attacks.

III. Supply Chain Lifecycle Analytics

The goal of this research and development effort is to develop decision-support technologies that enable decision-makers to perform risk-based cost-benefit prioritization of security investments to manage supply chain integrity and risk. The key challenges are the complexity of the end-to-end supply chain lifecycle problem, and the scalability of the supply chain representation. To overcome this complexity a hierarchical decomposition methodology for examining the supply chain lifecycle is proposed. The decomposition consists of (1) information-based mapping of the supply chain lifecycle and flow representation, (2) vulnerability and mitigation modeling, (3) application of new difficult and consequence security risk metrics that can be used to evaluate vulnerabilities throughout the supply chain lifecycle (i.e., design, implementation, testing, deployment, maintenance, retirement), and (4) solving the mathematical optimization models that evaluate threats and mitigation based on the security metrics. This approach systematically examines the lifecycle phases (e.g., design, implementation, testing, deployment, maintenance, retirement) of supply chains and assesses risk by leveraging a new security risk metric based on the degree of difficulty an adversary will encounter to successfully execute the most advantageous attack scenario [15]. This metric will enable decision-makers to overcome the complexity of quantifying security risk. It is suited for cost-benefit optimization. The methodology enables the decision maker to have the flexibility to scale the problem and to evaluate the supply chain at various depths (e.g., components, sub-component, sub-assembly, systems, etc.), and to leverage each decomposition to address system or enterprise level supply chain vulnerabilities. This approach will enable decision makers to recognize emergent behaviors from low to high level and their global effects.

The Supply Chain Lifecycle Decision Analytics framework consists of four integrated components; See Figure 1, for the hierarchical supply chain representation, vulnerability and mitigation modeling, risk assessment and visualization, and optimization.

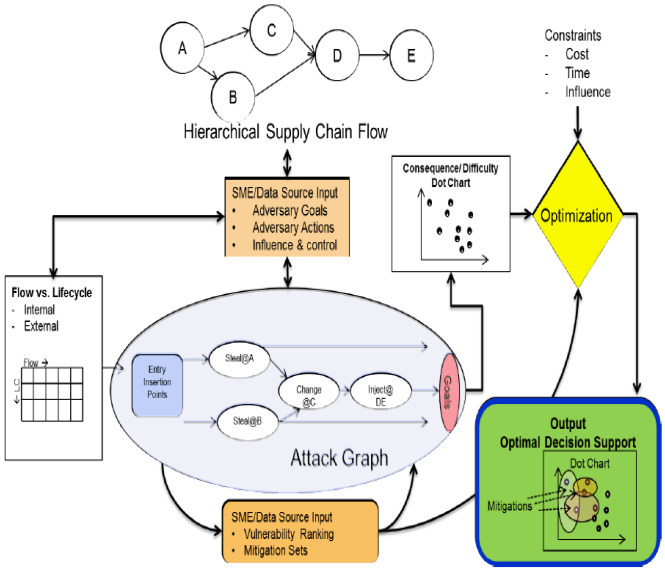

Fig. 1. The Supply Chain Lifecycle Decision Analytics Framework.

The modern supply chain is globally distributed with complex dependencies and interconnection among set of organizations, people, processes, products, and services. The supply chain is part of every lifecycle stages of a program or product (i.e., design, implementation, testing, deployment, maintenance, retirement). To evaluate the vulnerabilities across the supply chain, one must first capture the end-to-end supply chain. To represent the supply chain effectively, complexity must be overcome by balancing scalability and fidelity. The first component of the Supply Chain Lifecycle Decision analytics framework is the hierarchical supply chain representation. This effort developed an information-based approach that enables a hierarchical decomposition of the supply chain. The representation is a directed graph (DAG) that can represent high level flow diagrams to detail processes, and is scalable based on the level of fidelity provided by subject matter experts (SMEs).

Given the end-to-end supply chain, the second component of the framework, vulnerability and mitigation modeling, provides analysts with the ability to perform vulnerability and mitigation assessment on the supply chain. The supply chain representation, in combination with lifecycle phases, provides a structure for analysts to systematically identify potential vulnerability insertion points. Once the insertion points are identified, SME can develop attack scenarios based on adversary goals to subvert the supply chain. However, the vulnerability assessment can be highly subjective. The supply chain vulnerability space is too large for manual analysis to provide comprehensive coverage. To streamline the SME efforts and reduce the subjective nature of attack path generation (e.g., red-teaming), a functional ontology is developed for both adversary and mitigation actions that relates actionable functions to supply chain. The ontology consists of a set of actions and a set of objects that can be applied to a set of locations based on the supply chain representation. As an

example, an adversary can acquire the product design at the design house (location). The ontology helps to encapsulate the problem into manageable elements. This enables an efficient way to infer attack scenarios (i.e., directed graph representation of attack vectors) against the supply chain. By generating a rich attack space through such ontology, one can hypothesize that the attack data can help calculate and measure the overall supply chain risk through new Sandia-developed difficulty and consequence metrics.

The mitigation space can be evaluated in a similar manner. Mitigation actions can be applied at various nodes and edges along the attack vectors. The goal of the framework is not to provide analysts a tool with which to manage individual vulnerabilities. Instead, the goal is to empower the analysts to evaluate the supply chain holistically and the subsequence supply chain vulnerability space comprehensively, such that mitigation addresses multiple vulnerabilities. Identifying common nodes that are part of multiple attack scenarios could provide broader mitigation. A reactive approach in addressing individual vulnerabilities one at a time would be futile because of the complexity of the problem, constraints, and limitations such as time and cost.

Once the supply chain vulnerabilities have been identified, the third component of the framework, risk assessment and visualization, provide risk assessment of the vulnerabilities. This process enables the analysts to rank and prioritize the vulnerability space of the supply chain. A newly developed Sandia Risk Assessment Methodology was applied that enable the evaluation of attack scenarios based on difficulty and consequences [15]. Mapping the attack scenarios to the difficulty and consequences space then enables optimization techniques to be applied for risk-based cost-benefit decision analysis.

The fourth part of the framework, optimization, provides decision support for the decision maker to select the best mitigation strategies to counter the discovered vulnerabilities. Optimization models enable decision makers to perform risk-based cost-benefit prioritization of mitigation strategies. The Sandia Risk Assessment Methodology enables analysts' rankings of the attack scenarios and provides input for optimal prioritization. The goal of the decision support component is to find the best set of mitigation strategies so that attack scenarios becomes increasingly difficult for the adversary and to have less impact if the attack is successful. Initial canonical optimization models, such as the variation of the set covering problem, have been applied as a proof of concept.

IV. SANDIA'S RISK-BASED COST-BENEFIT ANALYSIS

The Sandia Risk Assessment Methodology is a risk-based cost-benefit analysis method used to prioritize security investments to overcome the shortcomings of traditional risk assessment. It was internally developed through Laboratory Directed Research and Development (LDRD). The intent of the Sandia Risk Assessment Methodology work is to enable security analysts to describe the benefits of security risk reduction measures based on the degree to which they increase the difficulty for an adversary to prepare and execute an attack successfully that produces a given level of consequences. The resulting method is highly scalable. It enables robust risk-based cost-benefit security investment prioritization to be performed at levels of granularity ranging from single target up to multiple target of facilities across enterprise[15].

Traditionally, risk is defined by a table of triplets $< s_i; p_i; c_i >$ where s_i is a scenario, p_i is the probability of that scenario, and c_i is the consequence of that scenario, i.e., the measure of damage. These triplets correspond to three assessment questions:

1. What can happen?
2. How likely is it that will happen?
3. If it does happen, what are the consequences?

Analysis can capture risks fully if a complete table of all possible scenarios can be generated [9]. The evaluation of risk correspond to assessing the likelihood of threat T, P_{Ti} associated with the scenario Si, the conditional likelihood of success, $P_{sj/Ti}$, of exploiting vulnerabilities of the scenario, and the consequence C_i. Risk is calculated by

$$\text{Risk} = P_{Ti} * P_{sj/Ti} * C_i$$

In real-world practice, P_{Ti} values are highly uncertain. P_{Ti} depends strongly on unquantifiable factors like dissuasion, deterrence and an adversary's level of commitment. It also changes wildly over time and is dependent on the specific adversary groups. As a result, analysts often neglect P_{Ti} in the evaluation. When estimating P_{Ti} , s_i often is assumed to be mutually exclusive, and that the P_{Ti} is independent to vulnerabilities. In the real-world, P_{Ti} is highly dependent on what vulnerabilities are available in the scenarios.

The Sandia Risk Assessment Methodology modified the traditional risk definition to overcome the unrealistic evaluation of probability of threat. The modified definition considers the difficulty for an adversary to successfully accomplish an attack on a target. The revised risk questions consist of:

1. What can happen?
2. How difficult is it for an adversary to make this scenario happen?
3. If it does happen, what are the consequences?

Difficult d_i is defined as the difficulty for an adversary to perform attack scenario s_i. As a result, the revised risk definition no longer require the assessment of P_{Ti} . Each attack scenarios are independent of threat. The evaluations are independent of the type of adversaries. Using this definition, risk evaluation do not require revision as adversary motivations change because this risk definition characterizes scenarios and targets rather than estimating the adversary's probability of attack. The modified definition characterizes the attack scenario and target, and is independent of specific adversaries. It is less sensitive to the uncertainties of changing threat assumptions. It provides a less subjective assessment, and an more objective assessment of what is known, rather than volatile assumptions of adversaries.

V. Hierarchical Supply Chain Representation

In a directed graph representation of a supply chain, nodes are locations involved in the production of the item(s) of interest. Nodes might represent suppliers, distributors, manufacturers, and so on. Directed edges in the graph represent the flow of information or objects through the supply chain. A bill of materials (BOM) may flow from a design house to a manufacturer. The supply chain representation is hierarchical. It can include as much detail as is available or desired to faithfully analyze attacks and mitigations. If much information is not available, then an abstract representation may be used. At this level of detail, a node might be described simply as a supplier located in a particular country. When more information become available, and if a more detailed analysis is desired, then it can be included as well. As an example, a detailed representation of the internal processes of a manufacturer may be included if that information is available. This is illustrated in Figure 2.

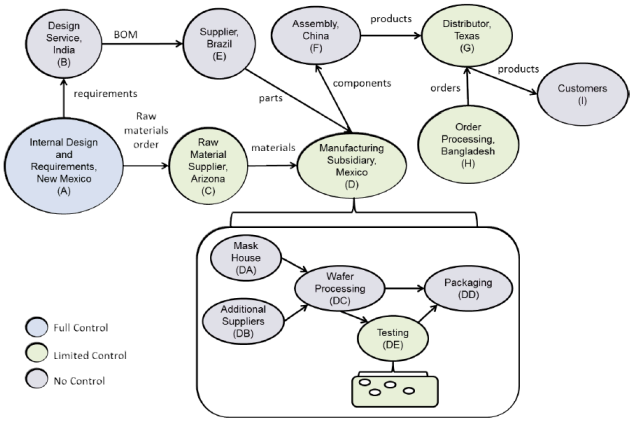

Fig. 2. A hypothetical example of hierarchical directed graph representation of a supply chain.

The framework leverages a tool called Generic Modeling Environment (GME) to capture the structure of the supply chain and attributes [11]. GME is a domain specific model synthesis tool using meta-models (schemas) to define the structure of the supply chain representation. The representation is a directed graph (DAG) that can represent high level flow diagrams to detail processes. Such representation enables the analysts to reduce the complexity of the supply chain representation problem into manageable pieces for further evaluation. By design, the hierarchical and recursive nature of the representation can be expanded to address the supply chain problem holistically at various depths.

VI. Adversary Modeling

A formalized, streamlined approach has been developed for representing locations, objects and adversary and defender activities in a supply chain. The supply chain representation and the adversary and defender behaviors can be expressed at any level of detail that is available or desired.

Considering first adversary and defender behaviors at the most abstracted level, generalized actions are represented. For adversaries, these actions are:

1. Acquire
2. Modify
3. Delay
4. Insert

For defenders, the actions are:

1. Tamper Prevention
2. Tamper Detection
3. Review
4. Test
5. Implement Best Practice
6. Chain of Custody

These high-level activities can be expanded to provide more detailed descriptions of actions within the supply chain. With more information about the supply chain, mitigation options, or adversary, the analysis then can be more specific. For example, the adversary's goal is to acquire an object or information. The adversary first may recruit an insider from the adversary's organization. The adversary also may acquire something through interception during transportation or communications. Each activity could be expanded to provide greater detail. After devising a set of actions, any desired level of detail can be used in the subsequent analysis. This approach easily allows accommodation at various levels of detail. As detailed information becomes available, it can be included in the analysis. When little information is available, more abstract, generalized descriptions can be used. It is possible to make meaningful, relative comparisons of attack paths and mitigations when the representation is abstract. A worst-case model could be used, or a model based on similar parts of other supply chains.

Once a suitable set of actions has been developed, it is applied to the directed graph representation of the supply chain. In the representation, nodes are locations involved in the production of supply chain items. Supply chain nodes might represent suppliers, distributors, manufacturers, and so on. Directed edges in the graph represent the flow of information or objects through the supply chain. For instance, a BOM may flow from a design house to a manufacturer. The supply chain can include as much detail as is available or desired. If much information is not available, then an abstract representation may be used. At an abstract level, a node might be described simply as a supplier located in a particular location. However, when more information is available, and if a more detailed analysis is desired, then it can be included in the analysis as well. For instance, a detailed representation of the internal processes of a design house may be included if that information is available. Now, combine this directed graph representation of the supply chain and the description of adversary and defender actions. For this, adversary actions are

performed on objects at particular locations. The actions are permitted to be associated without any particular location since some adversary actions, such as modifications to an object, may occur outside of the supply chain. Defender actions are performed at locations or on objects. Defender actions change the properties of a location or a subject. A defender may have the control to add more security staff at a location, making it harder to force entry, or use overnight shipping of an object in transit. This gives the attacker less time to attack an object in transit. Having the appropriate information associated with each location and object is crucial to support analysis that leverages this supply chain representation. Some location example attributes are:

- Security
- Integrity of personnel
- Amount of time location has been operational or in business
- Amount of time objects or information is retained
- Amount of time between when an object is received and a product object is first delivered

For objects, some example attributes are:

1. Reverse-engineering difficulty
2. Level of provenance (expressed as, e.g., the probability that an object is what it seems to be)
3. Complexity (e.g., number of transistors, sub-components, etc.)

These attributes allow the creation of a useful assessment of difficulty and consequence in later analyses.

VII. Risk Assessment

Given a representation of the supply chain and a suitable method for representing adversary behaviors within it, a method is needed to analyze the risk of supply chain attacks and a convenient approach for visualizing that risk for decision makers. For this, consider representing risk using the concept of (difficulty, consequence) pairs introduced in [15]. In this approach, each adversarial attack graph path is assigned a (difficulty, consequence) pair in order to assess risk. This model eliminates the need to consider the likelihood or probability of a specific attack. It focuses only on the difficulty (or the ease) and the consequences of an attack. To visualize the supply chain risk, the (difficulty, consequence) pairs for all attack graph paths could be plotted. A notional example is presented in Figure 3.

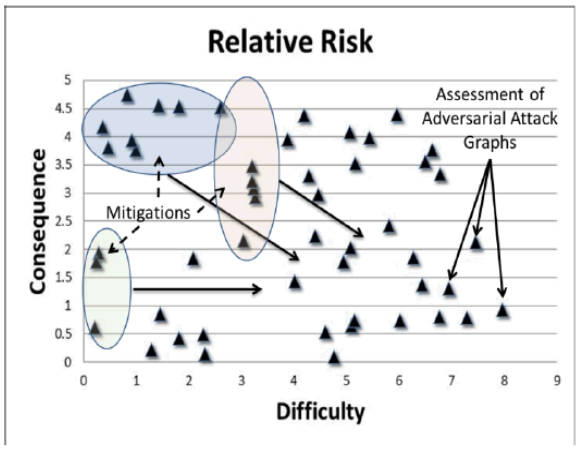

Figure 3. A notional (difficulty, consequence) plot indicating relative risk.

In Figure 3, note that the low difficulty, high consequence attacks in the upper left quadrant generally will be the most concern. The highly difficult, low consequence attacks in the lower right quadrant are of least concern. See how this risk analysis approach is amenable to visualization of the impact of various supply chain mitigations. An individual mitigation will impact some subset of the potential adversarial attack graphs by changing the difficulty of the attack, the consequence of the attack, or both. Decision makers can observe this impact by seeing the position of dots representing individual attack graphs shift in response to proposed mitigation strategies.

VIII. Constrained Optimization to Prioritize Security Investment

The adversary and mitigation modeling enable attacks to be mapped in to the two dimensional difficulty and consequence space. Similar to adversary modeling, impact of mitigation on adversarial behaviors also can be modeled. Given a well-defined difficulty and consequence space, a constrained optimizer can be built to determine which subset of mitigations should be applied to have maximal impact on the supply chain, e.g., constraints for this optimization may include time, cost, and influence. Influence is a measure of the ability to modify operations or apply mitigations to a particular event within the supply chain. If a mitigation is an option that can be offered by a supplier, then there is high influence. If mitigation requires a supplier to modify their business practices without concrete benefit, then influence is low.

To this end, initial canonical optimization models, such as the variation of the set covering problem, have been applied as a proof of concept. The basic set covering model and several of its variations are summarized in the review paper by Paschos [13]. The supply chain lifecycle problem roughly reduces to the set cover problem as follows: (1) the elements to be covered are the population of attack scenarios, (2) the mitigation options represent subsets of the attack scenarios

that the corresponding mitigation option can reduce risk, and (3) the minimal set of mitigation options that fully can cover the population of attack scenario of the supply chain lifecycle is the set of interests. The optimization becomes finding the best set of mitigation options that reduce risk (i.e., reduce consequence or increase difficulty) and cost. Other models such as the Budget Maximum Coverage Problem [10] with set cover and knapsack problem substructures were also considered. Greedy and enumeration algorithms similar to [10] were implemented for solving these models.

The supply chain problem however is more complex than the set cover problem. Unlike the set cover problem, mitigation options typically will not completely eliminate vulnerabilities, but only reduce risk. In addition, mitigation options are subject to cost and possibly other constraints and objectives. Further research will be needed to address uncertainty and the probabilistic nature of the mitigation and vulnerability space. An underlying compositional problem exists as mitigation options can affect various attack scenarios differently, i.e., individual mitigation options might have independent effects. However, collectively the resulting behavior may influence the vulnerabilities differently. Finding the right balance and trade-offs, and understanding the compositional effect is non-trivial. Other optimization methods such as approximation methods, meta-heuristics, and control theoretic approaches, are under consideration as well.

IX. Discussion and Conclusion

In this paper we have presented a decision analytics framework that can be used holistically to analyze supply chain security. In our framework, the end-to-end supply chain lifecycle problem is decomposed into (1) information-based mapping of the supply chain lifecycle and flow representation, (2) vulnerability and mitigation modeling, (3) risk assessment (difficult and consequence) that can be used to assess vulnerabilities throughout the supply chain lifecycle (i.e., design, implementation, testing, deployment, maintenance, retirement), and (4) optimization, solving the mathematical optimization models that evaluate threats and mitigation based on the security metrics.

Moreover, this supply chain analysis method produces a bounded problem space important for analysis at any desired level. The supply chain directed graph has a finite number of nodes and edges. The adversary and defender actions also are finite sets. A bounded, formalized, automatable method is developed for representing supply chains and the vulnerabilities and mitigations that apply to them. That is extensible to whatever level of detail is available or desired. This representation is amenable to visualization using (difficulty, consequence) plots. It is suitable for input to constrained optimizers to determine the most appropriate set of mitigations to deploy. This approach is applicable to any supply chain. More generally, this framework may be applied to the analysis of other types of problems by making appropriate modifications to the actions of adversary and defender and to the system representation.

Supply chain problems often are so large and complex that analysis can be overwhelming. For this reason, minimizes human input is desired for approaches for mapping mitigations onto the supply chain and adversary actions. This will eliminate subjectivity so that a particularly popular or new mitigation is not artificially inflated.

Future research will focus on assessing the supply chain risk management given incomplete, imbalanced, and inconsistent information. We plan to develop a process for handling these cases and analyze alternatives when there is uncertainty.

Acknowledgment

This work is being performed under the Laboratory Directed Research and Development Program at Sandia National Laboratories. We would like to express our thanks to the Cyber Security Science and Technology committees for their guidance, support, interest and valuable discussions. The authors are grateful for this support. Sandia is a multi-program laboratory operated by Sandia Corporation, for the United States Department of Energy's National Nuclear Security Administration. This paper is approved for unlimited release as SANDXXXX.

References

[1] Defense acquisition guidebook. September 2013. https://acc.dau.mil/docs/dag_pdf/ dag_complete.pdf.

[2] Jon Boyens, Celia Paulsen, Nadya Bartol, Rama Moorthy, and Stephanie Shankles. Notional supply chain risk management practices for federal information systems. (NISTIR 7622), October 2012. http://dx.doi.org/10.6028/NIST.IR.7622.

[3] Jon Boyens, Celia Paulsen, Rama Moorthy, Nadya Bartol, and Stephanie A. Shankles. Supply chain risk management practices for federdal information systems and organizations. (NISTSP 800-161), August 2013. Initial Public Draft.

[4] Joel Brenner. America the Vulnerable. The Penguin Press, New York, 2011.

[5] Cassell Bryan-Low. Vodafone, Ericsson get hung up in Greece's phone-tap scandal. June 2006. http://online.wsj.com/article/SB115085571895085969.html [Online; accessed 20-September-2013].

[6] Computer Security Division. Security and privacy controls for federal information systems and organizations. (NIST SP 800-53r4), April 2013.

[7] GAO. IT supply chain: National security-related agencies need to better address risks. (GAO-12-361), March 2012 http://www.gao.gov/assets/590/589568.pdf [Online; accessed 29-September-2013].

[8] Karen M. Goertzel, Kristy Mosteller, Holly Lynne McKinley Schmidt, Stephanie Shankles, and Theodore Winograd. Security risk managemnt for the off-theshelf information and communications technology (ICT) supply chain: An IATAC state-of-the-art report. August 2010.

[9] S. Kaplan and B.J. Garrick. On the quantitative definition of risk. Risk Analysis, 1(1), 1981.

[10] S. Khuller, A. Moss, and J.S. Naor. The budgeted maximum coverage problem. Information Processing Letters, 70(1):39–45, 1999.

[11] Akos Ledeczi, Miklos Maroti, Arpad Bakay, Gabor Karsai, Jason Garrett, Charles Thomason, Greg Nordstrom, Jonathan Sprinkle, and Peter Volgyesi. The generic modeling environment. IEEE WISP 2001 Proceedings, May 2001.

[12] Carl Levin U.S. Senator of Michigan. Background memo: Senate armed services committee hearing on counterfeit electronic parts in the DoD supply chain.

http://www.levin.senate.gov/newsroom/press/release/background-memo-senate-armed-services-committee-hearing-on-counterfeit-electronic-parts-in-the-dod-supply-chain [Online; accessed 15-September-2013].

[13] V.T. Paschos. A survey of approximately optimal solutions to some covering and packing problems. ACM Computing Surveys (CSUR), 29(2):171-209,1997.

[14] Mike Rogers and Dutch Ruppersberger. Investigative report on the U.S. national security issues posed by Chinese telecommunications companies Huawei and ZTE. October 2012. http://intelligence.house.gov/sites/intelligence.house.gov/files/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf [Online; accessed 20-September-2013].

[15] Gregory Wyss, John Hinton, Katherine Guzman, John Clem, John Darby, Kim Mitchiner. “Risk-based cost-benefit analysis for security assessment problem.” In Security Technology (ICCST),2010 IEEE International Carnahan Conference on, IEEE, 2010.

[16] Lin, Han, Moses Schwartz, John Michalski, Mayuri Shakamuri, and Philip Campbell. "Leveraging a crowd sourcing methodology to enhance supply chain integrity." In Security Technology (ICCST), 2012 IEEE International Carnahan Conference on, IEEE, 2012.