SAND2012-7010C

Leveraging a Crowd Sourcing Methodology to Enhance Supply Chain Integrity

Han Lin, Moses Schwartz, John Michalski, Mayuri Shakamuri, Philip Campbell
Networked Systems Survivability and Assurance Department
Sandia National Laboratories
Albuquerque, New Mexico

***Abstract*—Supply chain integrity (SCI) is emerging as one of the top security issues facing critical systems. The government's reliance on commercial off-the-shelf (COTS) products is apparent, as is the threat of critical systems being designed and manufactured overseas. To date, few tools or capabilities exist to prevent or even detect these classes of attacks. Programs, such as DARPA Trust, exist to identify solutions; however, alternative strategies must be explored. It is extremely challenging to establish the trustworthiness of a supply chain for a product or system in today's globalized climate, especially given the complexity and variability of the hardware and software, and the diverse geographical areas where they are made. Counterfeit items, from individual chips to entire systems, have been found both in commercial and government sectors. Supply chain attacks can be inserted at any point during the product or system life cycle and can have detrimental effects to mission success.**

We hypothesize that wisdom of crowds techniques may be applicable to the analysis of supply chain integrity. Current supply chain security efforts are hindered by a lack of detailed information on a product's entire supply chain. End-users have virtually no access to supply chain information, and even major manufacturers may have difficulty getting access to their suppliers' sub-suppliers. Component testing and even reverse engineering can be used to mitigate risks, but these approaches are imperfect, time consuming, and expensive.

This paper will discuss the development of a semi-automated supply chain integrity risk analysis framework to assist the supply chain security analysts in assessing the level of risk associated with a component of a mission critical system. This capability can provide the system designer a more rigorous and efficient approach to assess the security of the components in the design. By fusing all of these tools into a centralized framework, we hypothesis that we can create a capability that will enable analysts to more effectively interrogate the data and extract trending as well as critical information.

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

I. Introduction

In order to maintain a competitive advantage in the marketplace, manufacturers and system vendors are relying more on commercial off-the-shelf (COTS) products than ever before. Rarely do companies have the desire or capability to design, develop, build, test and evaluate every component for their systems in-house. Reliance on suppliers and sub-suppliers around the world enables them to reduce development cost and design time. Although, there are many benefits to this development model, there is an inherent risk to supply chain integrity.

Supply chains for critical systems must be protected from deliberate or inadvertent manipulation. However, given our inability to control, influence, or even understand the supply chain, our exposure to supply chain attacks through insertion of counterfeit parts, software backdoors, or other untrustworthy components is real. Supply chain attacks may be injected at any point during the system design life cycle: requirements, design, implementation, testing and evaluation, deployment, maintenance, and retirement (See Figure 1.), and may have a significant impact on critical infrastructure, military mission-critical operations, and government operations.

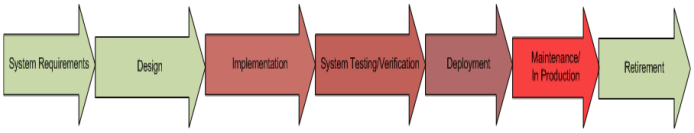

Fig. 1. Product Life Cycle Phases.

The goal of this paper is to describe a risk identification and mitigation method to address supply chain risks, using a statistical, wisdom of crowds [3], approach to provide a probabilistic answer to the supply chain security issues. The core concept is to leverage networks of individuals with diverse backgrounds and qualifications to make a prediction or estimate a probability. In many cases, the aggregation of their feedback tends to converge to the correct answer. An example is the television game show "Who Wants to Be a Millionaire?", on which the contestants are given a chance to crowd source the answer to a question by calling a friend or family member, or asking the audience to vote. Friends or family members provide correct answers about 65% of the time, but the audience provides the correct answers 91% of the time [3].

Wisdom of crowds is not a new concept. Companies like eBay, TripAdvisor, Wikipedia, and Google have leveraged crowd-sourcing and wisdom of crowds techniques to ensure the confidence of the buyers, sellers, and readers using ratings and

feedback from diverse groups of users. For instance on eBay, if someone conducts themselves well then their trust ratings will increase as buyers and sellers will be able to rate them based on their business transactions. Conversely, if someone behaves inappropriately, then their trust level can be diminished. Likewise on TripAdvisor, a website that provides ratings of hotels, restaurants, cruises, and such, where the ratings are based on reviews by tourists who have stayed in the hotels, taken the flights, taken the cruises, etc. Trip Advisor sorts the reviews based on characteristics such as those who traveled as a "family," those who traveled as a "couple," those who traveled on business, and so on. Reviewers are invited to indicate which of five items—"excellent," "very good," "average," "poor," and "terrible"—applies and they are also invited to provide free form text. Wikipedia provides a platform for people all over the world to collaborate and create contents, combine knowledge, and exchange ideas. Google ranks website search based on how they link to each other, implicitly gathering information from a diverse set of sources [5].

These platforms provide a trust model to assist users with decision by harnessing the collective knowledge of a group, relying on the fact that the group has more knowledge for solving a problem than an individual. We hypothesize that wisdom of crowds and other crowd-sourcing techniques can be applied to the supply chain integrity problem.

This rest of this paper is organized as follows. Section II describes a framework that we developed to evaluate SCI based on crowd sourcing and wisdom of crowds techniques. Section III presents the preliminary results of our approach. Finally, Section IV presents our conclusions and findings.

II. Framework

Performing supply chain assurance on each electronic component that is being utilized in a system critical operation is time consuming and laborious. Nevertheless, there exist limited alternatives to ensure that counterfeit electronic devices and malware subversions are both detected and prevented from entering into the supply chain. There are varieties of methods that an analyst may use to accomplish this task, including conducting Internet searches to gather information in order to gauge the trustworthiness of the part. Most of these methods are tedious, manually intensive, and not scalable.

This process, of conducting a single search, has significant disadvantages. It only provides insight into a single snapshot in time. Once searches are completed, they are often not re-done in any periodic fashion. Thus, they do not provide indicators/proactive measures to mitigate any emerging or post-search threats that may have been discovered. Given the ephemeral nature of technology, coupled with rising cost pressures, designs and components change rapidly between product revisions. Completing the micro-method for each release is not feasible or practical.

A more scalable approach is to utilize a web crawler and use the textual information derived from source documents to analyze the information about the component from each incoming page. The analysis is then used to determine which new link to follow such that a knowledge base of curated data can be built and used as a decision support system. In this framework, a three-tier software architecture will be used to provide a user interface component (presentation tier), an analysis component (logic tier), and a database component (data tier).

A. Presentation Tier

The presentation tier consists of a front-end web-based client that enables the security analyst explore the gathered data, construct queries to build new views, and review the results after the analysis is completed (Figure 2.)

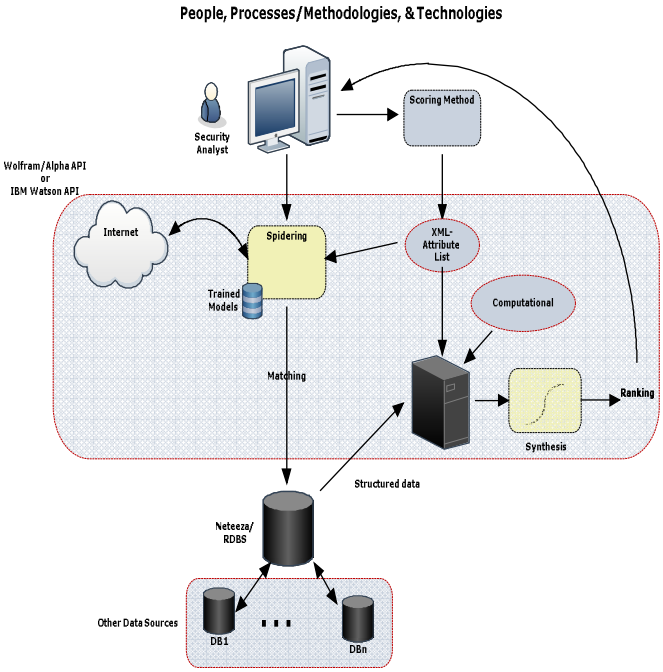

Fig. 2. Crowd Creation and Crowd Voting Architecture.

This tier can be considered the crowd creation tier. It allows stakeholders from diverse groups to act as analysts to participate in this form of crowd sourcing. The advantage is that we are able to get a broad range of questions and perspectives in regard to the supply chain integrity of the components up front. For example, the types of questions that professional cyber security analysts would normally ask are: "How trustworthy is the vendor that produces this integrated circuit? Does this vendor follow security best practices in their design process? Is there a history of security breaches with this company?" However, other professionals such as financial experts or software developers may be most interested in information that is not explicitly related to SCI, but still has applicability. These other professionals may ask questions such as: "Is this a Fortune 500 company? Does this vendor outsource everything offshore?" Although these questions are not explicitly SCI related, but are likely applicable. For example, Fortune 500 companies have a reputation to protect, and may be more inclined to to adopt security best practices.

B. Logic Tier

The role of the logic tier is to answer queries by evaluating data that is consumed by the database tier. Based off of a variety of techniques including heuristics, machine learning, and statistical analysis, this tier will enable analysts to make sense of and interrogate the data interactively or to develop programs for autonomous, continual analysis. Some of the strengths of using a common logic tier for the analysts are that it is possible to share information such as markup, queries, and crowd-sourced ratings. This allows the SCI problem to become a more data driven process that can be run in a semi-autonomous fashion. By looking at the data from the same source of information, analysts can now vet and evaluate (through voting or some other mechanism) on the veracity of the claims that another analyst makes. The analysis performed on this data can also be through the presentation layer.

Advanced knowledge engines like IBM Watson [7] and Wolfram|Alpha [8] might be utilized as the logic tier for this proposed architecture. IBM Watson is one of the world's most advanced natural language processing machines that can understand unstructured and complex questions and responds with precise, factual answers. Watson combines advanced analytics and machine learning to weight and evaluate responses based on relevant evidence. Likewise, Wolfram|Alpha is another computational knowledge engine that can compute and analyze queries written in natural language. It is built on the foundation of the Mathematica computational engine.

C. Database Tier

The database tier is comprised of data storage systems that have the ability to gather, consume, store, and retrieve unstructured information. This part of the system provides a central point to look at all of the data that has been collected from a variety of sources including web crawls, manuals, reports, etc. that may provide some information supporting the integrity of a supply chain component.

III. Results

As a first step toward implementation of this framework, we developed a questionnaire to capture information about suppliers that can then be used for initial analysis. The questionnaire is based on the Supply Chain Risk Leadership Council's "Sample Supply Chain Security Self-Assessment Questionnaire for Suppliers or Other Supply-Chain Partners," [2] with additional questions based on experience gained from our previous supply chain risk management efforts.

The questionnaire is divided into 9 different sub-categories: Physical Security, Access Control, Personal Security, Procedural Security, Education and Training, Cyber Security, Research and Development Process, Manufacturing and Distribution , and Company Characteristics. Within each sub-category, we have developed a set of standard questions that is relevant to the topic of supply chain integrity (see Table I).

TABLE I. SCRM Questionnaire.

Physical Security
Does your facility use security guards?
Is your facility fully enclosed by perimeter fencing or walls?
Does your facility utilize security cameras for monitoring perimeters, entries and exist, loading bays, or other areas?
Does your facility have locks on doors, windows and gates?
Are the locks kept locked at all times to prevent unauthorized personnel from entering?
Do you have bars, screens, or other materials over the windows?
Do you have an alarm intrusion system?
Is your facility exterior lighted/illuminated at night?
Is the shipping/receiving area secure at all times to prevent access by unauthorized personnel?
Are outgoing shipments stored in a separate area that is secure and prevents unauthorized access?
Are guard logs regularly reviewed?
Do you have third-party security audits?
Access Control
Do you use an employee badge system for entry and monitoring onsite activities?
Do you have access controls in place at entry points to your facility?
Is vehicle access into your facility controlled?
Are vehicles and drivers screened or inspected prior to entry to your facility?
Do you identify, record, and track all visitors?
Are physical access logs regularly reviewed?
Personnel Security
Are employee work history background checks completed prior to hiring?
Are employee criminal background checks completed prior to hiring?
Are non-employee contractors allowed routine access into your facility (janitorial service, delivery drivers, food vendors, etc.?)
If yes, are employment and criminal background checks completed prior to access being allowed?
Is access restricted to these workers so that they may only access facilities that they need to be in?
Are these workers restricted from accessing the shipping and receiving areas?
Are these workers required to wear identification badges?

Do employees have U.S. government security clearances?
Does the company have high* employee turnover? (*must define high)
Is U.S. citizenship required for employment?
Are employees tested for drug use?
Are employees required to take a polygraph?
Procedural Security
Is there a Security Manager and staff?
Are physical security procedures documented?
Are access control security procedures documented?
Are computer access procedures documented?
Are IT security procedures documented?
Are personnel security procedures documented?
Are education/training of security procedures documented?
Are there procedures for employees reporting security problems and addressing the situation?
Are there procedures for responding to security incidents?
Are there procedures for marking, counting and weighing outgoing shipments?
Are there procedures for documenting outoing shipments?
Are there procedures for storing and identifying incoming and outoing shipments?
Are there procedures in place for storing shipment documentation (packing list, commercial invoice, etc.)?
Education and Training
Does your company provide a security awareness program related to protecting product integrity and facility security?
Is your company certified in a supply chain security or known shipper/consignor program? (e.g., AEO, PIP, etc.)
Do you require cargo integrity training for employees in the shipping and receiving areas and opening mail?
Do you require education on recognizing internal conspiracies and protecting access controls for all employees?
Cyber Security
Do you allow remote network access?
Do you require secure (VPN) technologies for remote network access?
Do you require the use of antivirus programs on corporate resources?
Do you use off-site backups for critical information?

Are your off-site backups physically located in the U.S.?
Do you logically (VLAN) segregate your networks?
If yes, do you use firewalls to enforce VLAN segregation?
Do you physically segregate your networks?
Do you have third-party security audits (penetration tests)?
Research and Development Process
Do you outsource your hardware R&D?
Do you outsource your software R&D?
Do you use secure software development methodology?
Do you follow relevant industry standards?
Do you use vetted algorithms?
Do you use in-house tools for R&D?
Do you use COTS tools for R&D?
Do you use open-source tools for R&D?
Do you use a version control system?
Do you have a code review process?
Do you have a regular patch/update cycle for your products?
Manufacturing and Distribution
Do you have a process for selecting and vetting suppliers?
Do you have a process for selecting and vetting distributors?
Do you outsource manufacturing?
Do you outsource manufacturing internationally?
Do you do device functionality testing?
Do you test every device?
Are procedures in place for securing outoing shipments against intrusion? (anti-tamper)
Does a 3rd party physically pack these shipments?
Are containers examined prior to loading to ensure no explosives or other contraband is present?
Are high security bolt seals used on ALL ocean/truck trailer container entry doors?
Are there procedures for reporting problems/delays in the movement of cargo?
Do you track movement/delivery of cargo/products?
Do you have policies to identify counterfeit parts?
Do you have policies to control distribution of products that fail testing?

Company Characteristics
Is your company publicly traded?
Is there significant (25%+) foreign ownership?
Is there significant (25%+) foreign ownership (sensitive countries)?
Does your company have a positive net value?
Is your management U.S.-based?
Is your company a GSA-approved vendor?
Does your company have contracts with the U.S. Government?
Does your company have contracts with the Department of Defense?
Does your company sell outside of the US?
Is there a common language within your company?

To address concerns that a questionnaire may be biased or incomplete, we rate each question's importance through a "wisdom of crowds" system for rating supply chain risk properties based on the collective judgments of a pool of users including SMEs. Users were asked to rate the importance of every item in the questionnaire on an integer scale of 0 to 10, where 0 means "I think this question is completely irrelevant for supply chain security," and 10 means "I think this is one of the most important questions for supply chain security". Users were also encouraged to come up with new questions that are deemed relevant to the sub-category as they see fit, but these were not included in our analysis.

Each question answered by the knowledge engine is assigned a value of "1" or "0" where "1" corresponds to a "yes" answer and "0" corresponds to a "no" answer. The overall score is calculated as a Nx1* 1xN matrix multiplication for that particular sub-category.

As an example, consider three analysts (A0, A1, A2), trying to address the "Access Control" practices or lack thereof of a particular vendor by answering the five questions (Q0, …, Q4) in the "Access Control" sub-category.

Table II shows the relevancy of each question as perceived by each analyst. For example, analyst A0 considers the relevance of Q0 to be 2. Table III shows the responses generated by the knowledge engine for each question. For example, knowledge engine's response to Q0 is 0 (i.e. "no"). Table IV shows the intermediate score which is the product of the relevancy of each question for each analyst and the knowledge engine response. Table V shows the score (average of each row in Table IV) for each analyst.

TABLE II. RELEVANCY OF EACH QUESTION AS PERCEIVED BY EACH ANALYST.

Analyst	Questions				
	Q0	Q1	Q2	Q3	Q4
A0	2	4	6	8	9
A1	8	7	6	4	0
A2	0	0	0	0	0

TABLE III. KNOWLEDGE ENGINE RESPONSE.

	Questions				
	Q0	Q1	Q2	Q3	Q4
Knowledge Engine Response	0	1	1	0	1

TABLE IV. INTERMEDIATE SCORE.

Analyst	Product of Table II and Table III				
A0	0	4	6	0	9
A1	0	7	6	0	0
A2	0	0	0	0	0

TABLE V. SCORE.

Analyst	Score (Average of each row in Table IV)
A0	3.8
A1	2.6
A2	0

The questions listed in Table I serve as a starting point to gather information. Other questions can be added, or existing questions can be deleted, based on the analyst's knowledge of the system under evaluation.

A. Relevance Study

We performed the initial step, described in the simple example above, on all the questions in Table I using eleven SMEs (full-time technical staff at Sandia National Laboratories). We asked these SMEs to rate the relevancy of each question listed in Table I. Table VI and Figure 3 show the mean and standard deviation for each category. Table VII shows scores for the ten highest-rated questions.

TABLE VI. SME relevance ratings, summarized by question category.

Question Category	Mean	StDev
Manufacturing and Distribution	7.41	1.08
Cyber Security	6.95	0.84
Research and Development Process	6.81	1.40
Procedural Security	6.76	0.24
Access Control	6.62	0.63
Education and Training	6.57	0.57
Company Characteristics	6.13	0.81
Physical Security	5.97	0.81
Personnel Security	5.63	1.17

The SME group rated questions related to manufacturing and distribution (the most traditional definition of supply chain) very highly, followed by cyber security and R&D process. The lowest rated question categories were company characteristics (including ownership structure and finances), physical security, and personnel security. These ratings are unsurprising, given that the SME group was comprised of cyber security R&D professionals.

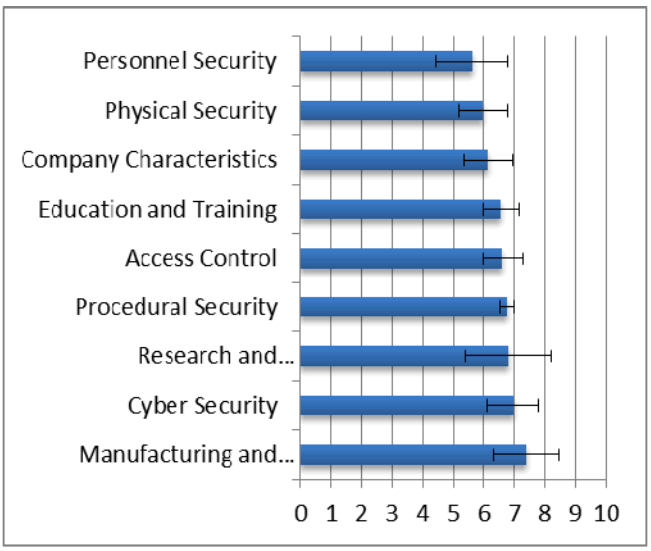

Fig. 3. SME relevance ratings, summarized by question category. Error bars show standard deviation.

Table VII. SME relevance ratings for the ten highest-rated questions.

Question	Mean	StDev	StdError
Do you have policies to identify counterfeit parts?	8.55	1.57	0.50
Do you have a process for selecting and vetting suppliers?	8.18	1.58	0.50
Do you outsource manufacturing internationally?	7.91	2.28	0.72
Are procedures in place for securing outgoing shipments against intrusion? (anti-tamper)	7.91	1.69	0.53
Do you require secure (VPN) technologies for remote network access?	7.82	1.20	0.38
Do you have a process for selecting and vetting distributors?	7.82	1.52	0.48
Do you outsource manufacturing?	7.82	2.11	0.67
Do you outsource your hardware R&D?	7.64	2.45	0.77
Do you outsource your software R&D?	7.64	2.45	0.77
Do you track movement/delivery of cargo/products?	7.55	2.15	0.68

Future efforts include incorporating knowledge engine to provide concrete results and soliciting ratings from more diverse groups (i.e., SMEs with backgrounds other than cyber security) will allow for a number of comparisons, and should provide some evidence of the consistency of this wisdom of crowds approach.

IV. Discussion and Conclusion

In this paper we have presented a framework for analyzing the integrity of a supply chain. In our framework, multiple analysts assign weights to different scoring criteria for a supply chain, and based on those weights and the results for each of those criteria we derive a final rating. Early versions of this process must use a predetermined list of criteria, and those criteria must be manually addressed to build a dataset. Eventually, we hope to automate significant portions of this process; the ideal end state would be for an analyst to create arbitrary criteria, which an expert system would automatically determine a probabilistic answer.

Our intermediate results are a supply chain questionnaire, and a summary of the relevance ratings that our group of SMEs (cyber security researchers) assigned to the questions. These early results show what the most important supply chain risk properties are based on the collective judgments of a pool of SMEs. Future work will include refinement of the vendor questionnaire, as well as an effort to solicit ratings from multiple groups (e.g., cyber security experts, physical security experts, and individuals without any security background) to quantify the differences in crowd-sourced question ratings. The development of an expert system to probabilistically answer analyst questions is an eventual goal.

The practical difficulties in using this framework for real-world supply chain integrity analysis are the lack of data about third-party supply chains, and the difficulty of validating the effectiveness of this approach. In a large part, this framework is an attempt to address the lack of supply chain information; we believe that even when it is only possible to collect a small amount of information, this quantitative framework using crowd-sourced ratings will allow for making the best decisions possible given the available data

ACKNOWLEDGMENT

We would like to express our thanks to Vincent Urias for his help, support, interest, and valuable discussions.

REFERENCES

[1] Thomas W. Malone, Robert Laubacher, and Chrysanthos Dellarocas, "Harnessing Crowds: Mapping the Genome of Collective Intelligence", Center for Collective Intelligence, Massachusetts Institute of Technology.

[2] Supply Chain Risk Leadership Council. Supply Chain Risk Management: A Compilation of Best Practices. August 2011. (http://www.scrlc.com/articles/Supply_Chain_Risk_Management_A_Compilation_of_Best_Practices_final[1].pdf)

[3] James Surowiecki, The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations, Anchor, August 2005.

[4] Software Security Assurance State-of-the-Art Report (SOAR)—Information Assurance Technology Analysis Center (IATAC), Data and Analysis Center for Software (DACS), August 17, 2010.

[5] David Austin, 2006, "How Google Finds Your Needle in the Web's Haystack", American Mathematical Society Feature Column.

[6] Charles MacKay, 1841, "Extraordinary Popular Delusion and the Madness of Crowds", ISBN 1853263494, 9781853263491.

[7] Favid Ferrucci; Eric Nyberg, et al, "Towards the Open Advancement of Question Answering Systems", IBM Research Report, April 22, 2009.

[8] Stephen Wildstrom, "Wolfram Alpha: A New Way to Search?", Business week, March 9, 2009.