What do you mean, Supply Chain Security?

A Taxonomy and Framework for Knowledge Sharing

Jess Smith
WSU and SEL
Jess_Smith@selinc.com
Pullman, WA

Jeremy Teuton
PNNL
Jeremy.Teuton@PNNL.gov
Richland, WA

Abstract

Supply chain security is a hot topic for research, but the specific phrase "supply chain security" has different definitions for different groups. This paper presents a brief taxonomy for both the terms supply chain and security, and then explores a basic framework to help describe areas of research in supply chain security. Security is broken down into confidentiality, integrity, and availability; supply chain is detailed as the networks, processes, and elements. By creating a method for describing the research, we can begin to create a framework of the research in supply chain security. This framework allows us to see where prior work has been done and allows us to focus on less-explored areas. It also allows us to compare and translate the supply chain research being performed in one field (electronics), to other fields (e.g. food production, clothing manufacturing).

1. Introduction

"Supply chain security" is a phrase with many meanings in a variety of fields. For those in the logistics world, it means, "can I get what I need when I need it" [1]. For a business person, it may mean, "can I ensure the security of the proprietary information about my product" [2]. A software designer must be interested in all the different people who have submitted code to the project, and a hardware vendor cares about who manufactured what components and how. In the modern marketplace, supply chain security may also include ensuring that the workforce and products involved with the creation of a product is ethically sourced [3, 4]. Prior work has also focused on ensuring physical supply chain security, especially focused on terrorism-driven challenges [5].

This wealth of meaning has translated into two different problems, both based on the difficulty of communicating outside of a given field. The first problem is that there are holes in the research, areas of interest that have not yet been explored because researchers just don't know they are holes. The other problem is unnecessarily repeated research due to different focus areas use a variety of different words to describe the same concepts.

To remedy this, two things are needed: a taxonomy and a framework. The taxonomy grounds the conversation, facilitating communication between researchers from different backgrounds. A framework is needed to lay out the areas of research, to describe sections that have been explored and what requires more research. Until groups share a language, they cannot share research. Without a shared language, research is isolated. Without a common map or framework, research areas will be missed or unnecessarily repeated. The goal of this paper is to lay out a general map (framework) of the supply chain security world, sketching in rough borders and creating a basic shared language (taxonomy).

The first section of this paper provides a framework that can be built upon to solve these problems. The second section of this paper lays out a high-level taxonomy, describing both the terms "security" and "supply chain" at a level which will be applicable from integrated circuit manufacturers to hot-dog producers. The third section builds upon this and lays out a basic framework for research, while the fourth section presents case studies where the techniques of one field have been migrated into another field. We conclude in the fifth section with a discussion of future work needed to develop the framework into an actionable resource.

2. Prior Work

Prior work in supply chain management has largely focused on access, such as just-in-time manufacturing, and the necessary modeling to ensure that access [6, 7, 8]. Modeling a network is a critical area that is well suited to cross the boundaries of different fields, but is not broad enough to allow for the discussion on integrity and confidentiality. In this paper, we have drawn from these sources to build a definition for the network of a supply chain.

Supply chain security has been of great interest to the governments and militaries of various countries [9, 10], with a focus on ensuring that the products received are not fake/counterfeit or maliciously tampered with. From the language laid out in these procurement and regulatory guidance, we were able to draw a basis for the definition of integrity.

Most of our work on supply chain confidentiality has been drawn from prior work on supply chain privacy; most organizations wish to

URI: http://hdl.handle.net/10125/41708
ISBN: 978-0-9981331-0-2

reduce public information about their supply chain. [11] However, there has been an increase in the research performed on methods for safely and securely communicating information about a supply chain, including both vertical exchanges [12] and horizontally [13].

3. Taxonomy

As described in the introduction, both "security" and "supply chain" have a range of different meanings in different applications. This taxonomy will isolate and fix certain meanings, as they will be needed for the later framework.

3.1. Security

The term "security" has been defined as a combination of confidentiality, integrity, and availability for the information and cyber realms. This definition has been well explored and accepted; as such, it is used as the base for the supply chain security definition.

Confidentiality

One of the main historical tenants of security has been confidentiality. Troop movements, the details of a secret sauce formula, and news of a possible merger with another company all require confidentiality. Confidentiality is defined by Bishop [14] as not allowing unauthorized users to access information or objects. For the purpose of this framework, *confidentiality is keeping information about the supply chain (e.g. intellectual property, contracts, and shipping plans) limited to authorized users.*

Integrity

Information that has integrity is complete, without fault, and correctly functioning. In the supply chain, this translates to *integrity being the ability to trust that the element that has just been moved or otherwise changed is still possessing of the same level of integrity as it had prior to the change*. [15]

For example, if a pound of ground beef with high integrity goes through an untrusted process, the output has low integrity (having possibly experienced uncertain and or unsafe additives/treatments). The integrity of the overall supply chain is dependent upon the correctness of the network. Integrity asks the questions: Did the parts go where, and only where, they are supposed to? Did they get routed through some untrusted third party? Was it the best route possible?

Availability

To be useful, an object must be accessible when and where it is wanted, in the form it is needed. A breakdown in availability means a stoppage in the movement of the supply chain. Where confidentiality explores denying unauthorized users access, availability seeks to ensure that authorized users have access. [16] *Availability in the supply chain requires that all of the machinery, trucks, people, products, electricity and so on are available when and where needed.*

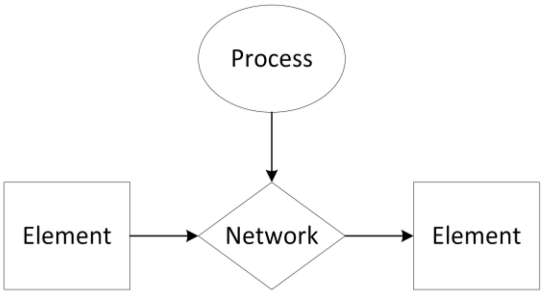

Figure 1. Simple Supply Chain

Availability is not a binary measurement. An element will rarely be completely cut off with no availability. Instead, an element may have reduced availability due to higher cost or transportation interruptions.

3.2. Supply Chain

Describing a supply chain as "a network in which processes act upon elements" divides the supply chain into the objects that we are acting upon (the elements), the actions performed on those elements (the processes), and the physical structure (the network) needed to perform those actions. We can evaluation a portion of the supply chain by looking back from a specific output element. Graphically, we can describe a supply chain as shown in Fig. 1. A sample supply chain is presented in Fig. 2.

Elements

An element is an item (e.g. a hot dog, an integrated circuit (IC), an iPad, a book, etc.). An element is both the output of the supply chain and the input. Each element can be combined with other elements to create a higher level element. For example, an IC may be created through the supply chain and then combined with other elements like an LCD screen, software, and a network control board to create a SCADA control system. That SCADA control system may then be joined with elements such as a nuclear reactor and cooling system to create a nuclear power plant.

This idea of elements and sub-elements allows us to look at both the end element as it is delivered and any of the input elements at any step of the supply chain. A flexible level of granularity is necessary to allow for the application of this term to many production fields, or to allow the exploration of the security metrics at different stages in the supply chain.

Processes

The processes are actions that transform elements into higher level elements. These actions may include terms like "mix" (in baking instructions) and "solder" (in construction of a printed circuit board), and more temporal terms like "rest", or spatial terms including "transport" and "lift". A process may result in the joining of two or more elements into a higher level element, or it may describe the transformation of a single element into another single element that is further along the supply chain. It can also include the creation of a element, through a transfer from the human mind to a physical product; this can be seen in the creation of software, literature, or art.

A process can be performed via a machine, an individual's direct or indirect actions, or by basic physical functions such as gravity. The process needs the instantiation of the network to act upon the elements.

Network

The network are the elements and the interconnection of those elements that perform processes on other elements. Everything from roads and factories to trucks and ink pens and how they work together makes up the network. A network is easy to visualize when considering a final element. Take a piece of paper and work backwards to look at every physical item that has touched that piece of paper or any of its input elements, as in the top of Fig. 2. The piece of paper was changed from pulp to paper in a given factory, and that given factory has specific tools that process the pulp. That factory and all of the equipment it contains is part of the paper's supply chain. Moving further back is the sawmill that made the pulp and the forest that provided the tree. We also must include any of the roads and vehicles that were used to move any of these input elements.

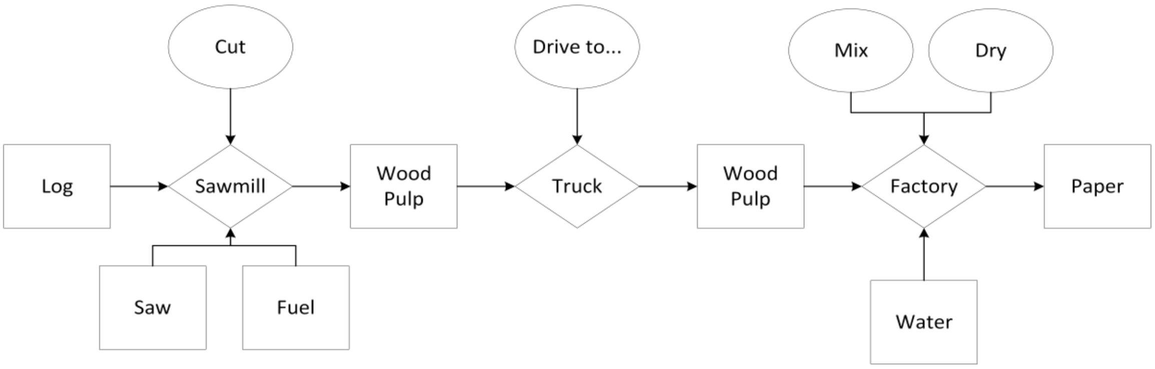

Figure 2. Intermediate Supply Chain

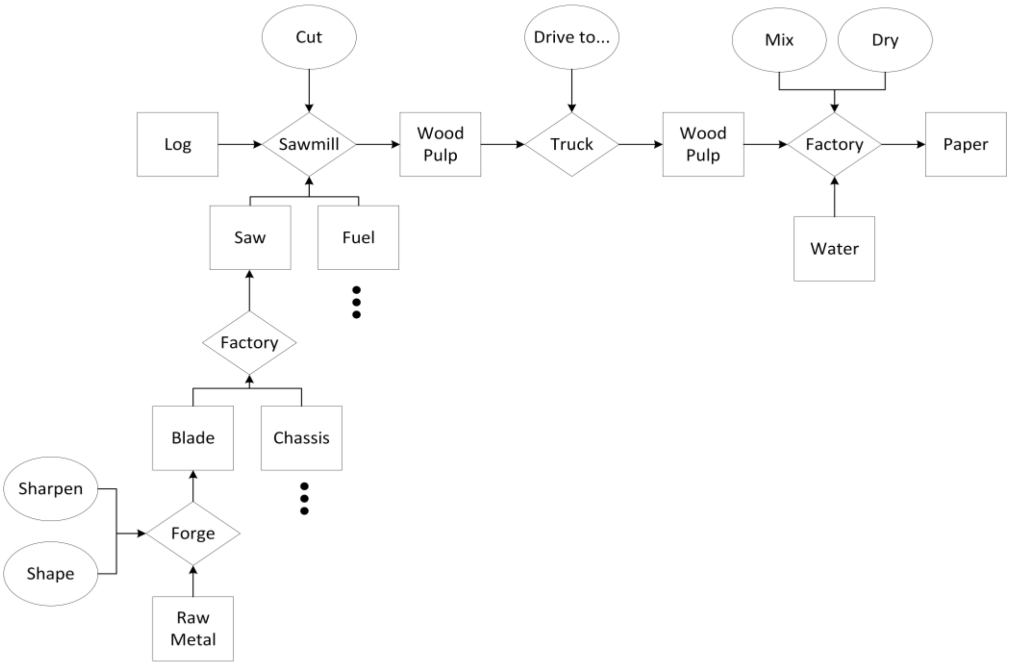

Figure 3. Supply Chain with Single Depth Line

3.3. The Challenge of Including People

Throughout the entire supply chain people are needed to push the button to make the process start, to use the network to move elements, to provide the intelligence to apply processes in a given order, and to lay out the network in the best way. Is a human a process or an network object? For the purpose of this framework if the human body is used (lifting, moving), it is part of the network. If the human mind is involved (following instructions, choosing a path), it is part of the processes.

3.4. Depth

The "full depth" of a given supply chain is a very complex thing. Many supply chains may contribute to the chain of leading to the final element of interest, creating a massive depth to the supply chain analysis. We must ask, can the tools that make the tools that make perform the processes be trusted? What of the tools that make the tools that make the tools? How far down the rabbit hole must we go to ensure full, 100% security of the supply chain for a piece of paper? This problem is a rapidly expanding one, as can be seen in Figure 3, and at some point we must trust the supply chain.

The authors of this paper do not have the answer, and doubt that a definitive answer will be provided in the near future, to a method for ensuring the full depth the supply chain is secure. This problem is too complex to simply map, much less solve. Therefore, we suggest focusing on a limited subset of critical input elements and processes. By considering the important properties of your output product, you can provide selectively greater depth for processes and objects that influence those properties. The complexity of the supply chain can become unmanageable unless limited to reasonable depth and scope.

4. Research Framework

The previous section described two groups of terms - those that describe security and those that describe the supply chain. Another way to look at this is having a description of what will happen and a description of the subject of those actions. Integrity, confidentiality, and availability may exist in any of the network, processes, and elements. This section will provide a framework that describes this combination of needs and areas.

The table in Figure 4 gives a visual overview of this idea with brief examples included. This table serves to give a high-level overview of the framework but is not highly comprehensive. A fully-formed framework would require a much larger document and a specific field or element's supply chain. Since this is not useful for exploring how to apply this framework to a wide array of areas and does not contribute towards sharing overall security principles between fields, this discussion will remain in broad terms.

It should be noted that while each of these areas of security and supply chain components are generally described as standalone concepts - each with its own areas of concern and research, there are actually a myriad of interconnects. To ease the introduction of this concept these interconnects are glossed over here. Later work(s) will be dedicated to exploring them.

Confidentiality	Information about suppliers, capabilities, or routes are kept confidential.	The exact process steps or types are kept confidential.	Intellectual property about the element is kept confidential
Integrity	The layout of the objects in the network is correct and efficient	The workers performing the processes are trained properly and correct instructions are available.	The element is what it claims to be (e.g., not counterfeit).
Availability	The physical structure of the network is not disrupted, slowed, or made unavailable.	The workers and the equipment needed to perform the processes are available.	As an input to either a new supply chain or to a retailer, the element is available when and where needed.
	Network	**Process**	**Element**

Figure 4. Research Framework for Supply Chain Security

4.1. Network

Confidentiality

When competing for limited resources, a company may wish to keep its suppliers secret. The choice of suppliers may reveal information to a competitor or attacker. The organization of objects in the network within a single facility may reveal where elements may be stolen or replaced with counterfeits. Either the objects that make up the supply chain or their specific layouts may need to remain confidential for an organization to remain competitive or trustworthy.

Recently, this could be seen in the friction between Samsung and Apple, as they fought over LCD screens made by Sharp. Because Sharp has limited resources, the confidentiality breach that allowed Samsung to learn of Apple's dependence on the supplier led to an availability problem with Samsung attempting to purchase all of the available screens. New competitors may also try to take advantage of who exactly is supplying what to their competitors to find sources of their own. [17, 18]

Integrity

The integrity of the network is critical for chain of custody concerns. If the network is incorrect or nondeterministic, it cannot be trusted that the processes have been performed correctly and the elements are what they should be. A network with high determinism is also efficient, providing a correct layout of objects without delays and deviations. When considering the integrity of the network, both the objects (the machines, trucks, and roads) and the layout of those objects are equally important.

Unexpected deviations in the network, such as the re-routing of an airplane carrying freight to an untrusted nation, is a violation of the integrity of the network. If unknown or uncertain processes have been applied at the locations along the network that the element must pass, the network cannot claim it has integrity. In this way, the integrity of the network affects the integrity of the whole supply chain.

Availability

The availability of the network is easily described as anything that disrupts the physical structure of the supply chain is a failure of availability. This disruption may be complete, totally denying the supply chain use of a piece of machinery or a road, or partial, with only a delay to the accessibility of the object. This delay is a concern for any organization because it can decrease supply and drive up prices, hurting the bottom line.

In 2011, the Great Tohoku Earthquake and Tsunami shut down much of the automotive production in Japan and nearby countries. As a result of this lapse in availability, Japanese automakers suffered a loss in market share and users of these vehicles experienced an increase in repair costs. On the other end of the supply chain, the workers who provide the brain-power behind the processes were also affected by a decrease in wages due to plant shutdowns. [19]

4.2. Processes

Due to its data-based nature, process security comes much closer to traditional information security than the security of the elements or network. While it is possible to affect the integrity of a process, keeping the details of the process confidential is a more common concern.

Confidentiality

The methods used to perform an action are often as valuable as the output of that action. The exact process steps need to be kept confidential to allow the organization to maintain its competitive edge. To provide physical security, the organization may need to keep information about the people performing the processes confidential.

In traditional Japanese sword-smithing, the exact steps, temperatures, and folding techniques used to create a masterwork samurai edged weapon, such as a katana or naginata, were considered both sacred and highly confidential. [20] The weapon itself is of great value, but the skill of the smith and the process he followed to create the weapon is of much greater value. The confidentiality of the information the smith imparted to his apprentices was of the utmost importance.

Integrity

The integrity of the processes is maintained through mechanisms such as correctly training workers or appropriately calibrating the machines used to perform the process. A process without integrity will not perform the appropriate action upon the element Sometimes this is loss of integrity is immediately recognized, but often it may be that the alteration, especially if malicious, will not be instantly detected.

While software is not often considered in a traditional supply chain mindset, it is still an element which has processes operating on it. In the early 2000's, the integrity of Microsoft's operating system code was called into question. In response, Microsoft's upper management famously decreed a halt to all work for two weeks in order to provide mandatory security training. [21] In this way, they were able to increase the integrity of their output element, the software, through an increase in the integrity of the processes through which they created the software.

Availability

To perform some processes, there must be workers and electricity available, as well as the instructions or knowledge for those workers to carry out the process. Without the availability of the processes, the network changes from a very dynamic system into a static, largely useless set of objects. The elements can no longer move or change and are stuck where they currently reside.

The lack of workers is a serious problem for leaders in China, who are beginning to feel the effects of the one-child policy. [22] Without the workers to perform basic tasks in factories, it may soon be impossible for Chinese-based companies to provide the extremely cheap products for which they have been known for the last decade. This lack of availability of people to perform processes may have worldwide impacts, shifting manufacturing to other realms and increasing wages in China.

4.3. Elements

Confidentiality

The intellectual property surrounding many elements is often critical to an organization and keeping the exact understanding of how an element works out of unauthorized hands is of high priority. This can include the need to keep an element confidential to prevent reverse engineering or to provide confidentiality for the data contained in an element. [23]

In the military world, the need for confidentiality of the design of elements, such as airplanes, goes to a new level. To ensure that these elements did not find themselves in unfriendly hands, the military in WWII designed auto-destruct features to destroy any sub-element that required complete confidentiality. This could be seen in the auto-destruct designed into the Norden bomb-sights. This ensured the confidentiality of the design, should it fall into enemy hands. [24]

Integrity

The integrity of an element is critical, both for an element that is an end-item (a computer or a pizza) and for an element that will be combined with other elements to make a more complex element. End-item elements are directly used by individuals and as such are subject to stringent controls on allowable chemicals, labeling, and other integrity-based controls. A lack of integrity in a sub-element may affect the integrity of the super-element. Without understanding the integrity of sub-elements, the integrity of the super-element cannot be asserted.

Counterfeit handbags, Trojan Horses in software, and improperly labeled fish are all breakdowns in the mechanisms that should protect the integrity of the element. While counterfeit handbags have a direct effect on the profitability of a company, other counterfeits have recently been seen coming into the market that are much more serious; a recent IEEE magazine article highlighted the practice of re-using old integrated circuits or other elements that may be used in critical systems. [25]

Availability

Without the elements, a network has no purpose and the processes have nothing to act upon. As such, the availability of the elements is critical for the correct movement of the entire supply chain. The sub-elements must be available when and where needed to create higher-level elements, and output elements must be available when and where people need them. A high level of availability ensures that the supply chain moves along; where as a low level of availability may cause stoppages or slowdowns throughout the entire depth and breadth of the supply chain.

Ensuring the availability of elements has been a major concern for just-in-time manufacturing. A great deal of work has been performed in this area by a range of researchers [26, 27, 28] to ensure that the availability of elements is supported. This area is of concern to both industry partners with a bottom line to consider, as well as governmental organizations, such as the military or Department of Energy, who may need specific and hard to acquire minerals or basic elements (such as uranium, magnesium or tungsten).

4.4. Tradeoffs and Supports

There are tradeoffs between the goals in supply chain security. For example, having an element be available immediately might decrease the amount of time to ensure the integrity of the element. However, there can also be places where the goals support each other. For example, high confidentiality of the steps of a process may ensure that the output element has higher integrity. The availability of an element will support the availability of the network, and the integrity of the network will help to ensure the integrity of the elements.

5. Case Studies

Adaptation of an existing paradigm to a novel field is nothing new. New regulatory rules are often grounded to some level of fidelity in existing regulation. There are advantages and disadvantages to this, but it is often a matter of expediency or efficiency. While it not always the intent, the lessons learned in applying a regulatory framework to a new field, and the ability to translate the outcomes in the new field back to the parent field, may outweigh the disadvantages by gaining novel insight on the established field and seeing the new subject from the perspective forced by fitting it to the existing framework. By creating this framework and taxonomy, the authors hope to encourage the sharing and re-evaluation of specific supply chains.

5.1. Adaptation of Maritime Precedence Rules to Aviation

In the early 20th century, the field of aviation began growing to a size and at a rate that necessitated navigational guidelines. It cannot be proven, but the aviation etiquette adopted by early aviators suggests that the rules of maritime navigation were adapted naturally and then codified into law. Even if this is not the case, if aviation were to spring fully formed into the modern world without the benefit of history, it would be reasonable to base aviation regulation in maritime navigation norms.

In many ways, this adaptation of the basic rules was beneficial. The green light on the right side, red on the left, maritime lighting standard works equally well on aircraft and this standard is now being adapted to work on the Cygnus spacecraft. [29] Similarly, rules on overtaking, approaching head-on, and converging in FAA regulations [30], taken from the International Regulations for Preventing Collisions at Sea [31], are highly applicable. However, some modifications are needed when adapting the maritime to the aviation. For example, [30] cover several situations involving fishing vessels; it is unlikely that many aircraft will hover in a single location for hours at a time, negating the need for such a rule.

5.2. Adaptation of the Toxicology Framework to Nanotechnology

Nanoparticles are an example of a technology whose products became commonplace so rapidly that there was no time to develop a completely new regulatory regime. Currently most nanoparticles are regulated by toxicological rules as chemicals [32]. Toxicological assays and regulatory rules were mainly developed for drug safety testing decades ago and have found further use regulating pesticides, chemicals, cosmetics and foodstuffs. It was logically extended to nanotoxicology regulations, especially when the nano-product falls into one of these categories. There is strong evidence however, that nanoparticles cannot be assumed to have the same properties as their parent compounds. Nano-preparations of compounds have been shown to have significantly different kinetics of adsorption, dispersion, metabolism, and excretion [33] , and novel biological interactions emergent from nanoparticle properties that have toxic effect pathways not shown by the parent compound. [34] Silver and Gold, elements normally considered to have minimal reactivity, have demonstrated nanoparticle size and shape dependent effects on cellular uptake and anti-microbial activity. [35, 36] Thus, the potential toxic effects or effective dose of nanoparticles cannot be extrapolated from knowledge of their chemical composition.

Unfortunately, there are documented cases of nanotoxicology reinventing safety testing for cytotoxicity and mutagenicity without drawing from the decades of development and validation of these assays for chemicals used in cosmetics. [33, 36] There is strong evidence that modern assays developed and optimized for nanotoxicology will be adaptable to the benefit of toxicology and the other fields for which classical toxicology has become crucial. [37, 38, 39, 40] The specific properties of nanoparticles illustrate the disadvantage of using regulation and protocols born of another field. The rapid construction of a useful framework that has been adapted to suit the new field demonstrates the advantages of this approach. Further, this common framework appears to be facilitating technological transfer between fields.

6. Future Paths

This paper laid out a general map of the supply chain security world, sketching in rough borders and creating a basic shared language. This work needs to be expanded upon in a variety of directions.

Each field, be it electronic manufacturing, meat processing, or jewelry crafting, needs to customize this framework to better fit that specific world. The selected terminology was left broad to accommodate for this and to facilitate the sharing across fields, but there needs to be depth into the field to support the breadth.

The current framework is currently limited by the definition of security as confidentiality, integrity, and availability. Future research should be directed to developing a more specific set of definitions for security that grows deeper into subsets of CIA. Authorization, non-repudiation, privacy, and fault-tolerance need to be considered as well.

Feedback from more researchers on this framework and the applicability to their field is critical. The creators of this framework come from computer science and biology backgrounds; more business and manufacturing people are needed to explore the framework and taxonomy and develop a more well-rounded system.

Finally, more research is needed to fill in the holes of the framework in each specific field. The original purpose of this framework was to detail where research had been performed and where more focus was needed. For example, in the integrated circuit world, more research is needed into evaluating the integrity of an element. Each field will likely have areas that are needful of more attention.

Further crossing research between fields is also needed. It may be that the research done on availability of the processes for the furniture building field can be modified and applied to the availability of the processes for petroleum processing. Currently, there is much reinventing of the wheel in different fields and research is needed to help the research cross fields.

7. Conclusions

In this paper, a high-level taxonomy was presented to facilitate research in supply chain security. A basic map of the research world in supply chain security was laid out and filled in, and case studies presented to give examples of situations where the framework for one realm has been applied to another successfully. By combining the cyber/information security definition with a novel description of the supply chain, our goal has been accomplished. The next step will be to move forward towards refining this framework and taxonomy.

ACKNOWLEDGMENTS

This work is supported by the Pacific Northwest National Laboratory's Supply Chain Integration for Integrity project, funded by the Department of Energy, Office of Electricity Delivery and Energy Reliability, Research and Development Division, RC-CEDS-2012-02.

The authors would like to thank Stephanie P. Barga for her invaluable contributions to the paper.

REFERENCES

[1] D. Bowersox, D. Closs, and M. B. Cooper. Supply Chain Logistics Management, 2nd Ed. McGraw-Hill, 2002

[2] K. De, S. Venkatraman, and A. Gunda. "Test shells for protecting proprietary information in asic cores." U.S. Patent No. 5,903,578. 11 May 1999.

[3] S. Seuring, and M. Müller. "From a literature review to a conceptual framework for sustainable supply chain management." Journal of cleaner production 16.15 (2008): 1699-1710.

[4] S. Gold, S. Seuring, and P. Beske. "Sustainable supply chain management and inter-organizational resources: a literature review." Corporate social responsibility and environmental management 17.4 (2010): 230-245.

[5] M. Lanska,. "Supply Chain Security." Proceedings of The 9th International Conference on Logistics & Sustainable Transport. Celje: University of Maribor, Faculty of Logistics. 2012.

[6] H. Min, and G. Zhou. "Supply chain modeling: past, present and future." Computers & industrial engineering 43.1 (2002): 231-249.

[7] J. M. Swaminathan, S. F. Smith, and N. M. Sadeh. "Modeling supply chain dynamics: A multiagent approach." Decision sciences 29.3 (1998): 607-632.

[8] B. Beamon, "Supply chain design and analysis:: Models and methods." International journal of production economics 55.3 (1998): 281-294.

[9] Department of Energy and Idaho National Laboratory, “Cybersecurity Procurement Language for Control Systems”, Technical Report, 2009

[10] Department of Defense , “Requirements for Information Rlateing to Supply Chain Risk” October 30, 2015

[11] R. Kolluru, and P. H. Meredith. "Security and trust management in supply chains." Information Management & Computer Security 9.5 (2001): 233-236.

[12] H. Zhang "Vertical information exchange in a supply chain with duopoly retailers." Production and Operations Management 11.4 (2002): 531.

[13] L. Li and H. Zhang. "Confidentiality and information sharing in supply chain coordination." Management science 54.8 (2008): 1467-1481.

[14] M. Chen and D.W. Goodman. ”Catalytically active gold: from nanoparticles to ultrathin films.” in Accounts of Chemical Research, vol. 39, no. 10, pp. 739-746, 2006.

[15] T.M. Lee. "Using mandatory integrity to enforce commercial security," in Proceedings of the 1998 IEEE Symposium on Security and Privacy, 1988.

[16] M. Bishop, “What Is Computer Security?,” *IEEE Security & Privacy Magazine,* vol 1, no 1, pp. 67–69 (Jan. 2003).

[17] J. Leonard. (n.d.) ”Samsung muscles in on Apple’s supply chain. ” Computing. [Online] Available: http://www.computing.co.uk/ctg/news/2268804/samsung-musclesin-on-apples-supply-chain Viewed May 2016.

[18] C. Page. (n.d.) ”Samsung looks to pinch Apple suppliers due to Galaxy S4 demand. ” The Inquirer. [Online] Available: http://www.theinquirer.net/inquirer/news/2268925/samsung-looksto-pinch-apple-suppliers-due-to-galaxy-s4-demand Viewed May 2016

[19] A. Leckcivilize. ”The Impact of Supply Chain Disruptions: Evidence from the Japanese Tsunami.” London School or Economics and Political Science, London., Dec 2012. Available: http://personal.lse.ac.uk/leckcivi/JobMarketPaperA.Leckcivilize.pdf

[20] G. Irvine, *The Japanese Sword: The Soul of the Samurai,* London: Weatherhill, 2000.

[21] D. Richman. (2002 Feb 26) Microsoft security ’journey’ is well under way, but skeptics doubt company’s capability and commitment. [Online] Available: http://www.seattlepi.com/business/article/Microsoft-security-journey-iswell-under-way-1081642.php

[22] Y. Huang and C. Lynch. (2013, Mar 6) Where have China’s workers gone? [Online] Available: http://www.bloomberg.com/news/2013-03-06/where-have-china-sworkers-gone-.html

[23] Ironkey Specifications Sheet (2013) Imation. [Online]. Available: http://www.ironkey.com/en-US/secure-portable-storage/250-enterprise.html

[24] D. Zimmerman and H.T. Tizard. Top secret exchange: the Tizard mission and the scientific war, London. , McGill-Queen’s Press, 1996.

[25] J. Villasenor and M. Tehranipoor. "Chop shop electronics." in IEEE Spectrum, vol. 50, no.10, pp. 41-45, 2013.

[26] C.M. Harland. "Supply chain management: relationships, chains and networks." in British Journal of Management, vol 7, no. 1, pp. S63-S80, 1996.

[27] V.R. Kannan and K.C. Tan. "Just in time, total quality management, and supply chain management: understanding their linkages and impact on business performance." in *Omega,* vol 33, no 2, pp. 153-162, 2005).

[28] L.B. Schwarz and Z.K. Weng. "The design of a JIT supply chain: The effect of leadtime uncertainty on safety stock." in Journal of Business Logistics, vol 21, no 2, pp 231, 2000.

[29] ”ORBITEC Delivers First-Ever LED Lighting System for Orbital Science’s Cygnus Module Spacecraft Navigation Lighting” ORBITEC Press Release, February, 2011

[30] U.S. Government. Code of Federal Regulations Title 14, Chapter 1, Subchapter F, Part 91, Subpart B, Section 91.113, ”Right-of-Way Rules: Except Water Operations” January, 2013.

[31] International Regulations for Preventing Collisions at Sea, International Maritime Organization, 1972

[32] T. Hartung and M. McBride. ”Food for thought on mapping the human toxome.” in Altex, vol. 28, no. 2, pp. 83-93, 2011.

[33] M. Holl and M. Banaszak. ”Nanotoxicology: a personal perspective.” in Wiley Interdisciplinary Reviews: Nanomedicine and Nanobiotechnology, vol. 1, no. 4, pp. 353-359, 2009.

[34] N.J. Walker and J.R. Bucher. ”A 21st century paradigm for evaluating the health hazards of nanoscale materials?.” in Toxicological Sciences, vol. 110, no .2, pp. 251-254, 2009.

[35] S. Pal, Y.K. Tak, and J.M. Song. ”Does the antibacterial activity of silver nanoparticles depend on the shape of the nanoparticle? A study of the gram-negative bacterium Escherichia coli.” in Applied and Environmental Microbiology, vol. 73, no. 6, pp: 712-1720, 2007.

[36] A. Kroll, et al. ”Current in vitro methods in nanoparticle risk assessment: Limitations and challenges.” in European journal of pharmaceutics and biopharmaceutics, vol. 72, no. 2, pp. 370-377, 2009.

[37] T. Hartung. ”Toward a new toxicology-evolution or revolution?.” in Alternatives to laboratory animals: ATLA, vol. 36, no. 6, pp. 635-639, 2008.

[38] T. Hartung and M. Leist. ”Food for thought on the evolution of toxicology and the phasing out of animal testing.” in Altex vol. 25, no. 2, pp. 91-102, 2008.

[39] J.F. Nyland and E. K. Silbergeld. ”A nanobiological approach to nanotoxicology.” in Human & experimental toxicology, vol. 28, no. 6, pp. 393-400, 2009.

[40] R. Gornati, E. Papis, M. Di Gioacchino, E. Sabbioni, I. Dalle Donne, A. Milzani and G. Bernardini. *In vivo and in vitro models for nanotoxicology testing*. Chichester, England: John Wiley and Sons, 2009, pp. 279-302.