Modeling a Secure Supply Chain Integrity Preservation System

Rasib Khan, Md Munirul Haque, Ragib Hasan
SECRETLab, Department of Computer and Information Sciences
University of Alabama at Birmingham
Birmingham, AL 35294, USA
Email: {rasib, mhaque, ragib}@cis.uab.edu

***Abstract*—It is important to preserve the integrity of a product as it is transported through the channel of distribution and delivered to the final consumer. In real world cases, manufacturing plants are sited at different parts of the world. Thus, it is an absolute necessity to have a secure mechanism which allows the supply chain integrity to be preserved. In this paper, we proposed a novel three-way bounded protocol for generating asserted holding and transferal proofs for preserving the integrity of the supply chain system. Additionally, the proofs are used to create a provenance chain for preserving the chronological order of the path of the product. The proposed protocol allows us to ensure the authenticity of the product with respect to its supply chain. We also provide a security analysis of the proposed architecture to illustrate the feasibility of the design.**

***Keywords*-Holding proofs; Information integrity; Provenance preservation; Supply chain; Transferal proofs.**

I. Introduction

A product cycle is driven by suppliers around the world. A product travels through a sequence of locations till it reaches the consumers, and is created by combining multiple intermediate products. Thus, in today's world, there exists multiple business-to-business and business-to-consumer delivery channels in the production of each finished product. The efficiency and security of the supply chain is a crucial concern for all industries. The transit of goods as it travels through the global supply chain system has critical effects on a nation's economy and security. Apart from disruptions in the supply chain, a nation can have highly unfavorable impacts with criminal and adversarial networks trying to exploit the system. We have seen the supply chain in global economy has increased efficiency in recent times. However, products supplied from varied sources have introduced a greater risk in maintaining the integrity of the supply chain.

Most works on supply chains include managing the supply chain, and the strategies used to optimize the process [1, 2]. References and models, such as the Supply Chain Operations Reference (SCOR) by Stephens [3], address the economic, financial, and managerial perspectives of the supply chain system. The process of validating and evaluating the supply chain performance can be a complex operation. There are numerous proposals on how to identify the necessary components to evaluate such supply chains [4].

With an ever-increasing field of commercial activities, gray market distribution and monitoring counterfeit products have become a daunting task. The range of counterfeit products varies from relatively non-injurious products to serious health and safety related goods like medicine and insecticides. Starting with collection of raw materials to the finished product, the very nature of the freight life-cycle provides ample opportunities to predators for replacing the authentic products with counterfeit items. With numerous number of hubs, assembly, and distribution points, it becomes a challenge to protect and actively monitor the supply chain. CNN reported in May 2012 that counterfeit electronic components from China have been incorporated into critical U.S. military systems [5]. This included operation helicopters and surveillance planes which had put the troops at risk. The investigation for this case had actually been going on for a while before it was detected [6].

In this paper, we propose a secure supply chain integrity preservation model, based on the location provenance of a product. The supply chain provenance is the history of the product's locations over time. Continuous tracking and reporting of locations violate the privacy and is not scalable for distributed environments. A more feasible and scalable approach is to require the product owner to obtain proofs of presence from each of the intermediate locations in the supply chain. To issue a proof, the authorities at a location first ensure the product's presence within a specific bounded region using secure localization techniques. A proof of presence can then be issued to the product owner, which can later be used to prove the product's location to a third party auditor. The supply of an item from the source to its final destination involves multiple intermediate locations and delivery authorities. Thus, a provenance chain is formed as the item travels through the supply chain. The provenance chain is delivered with the item at the final destination. The receiver of the supplied item can thus verify the obtained provenance chain, and validate the integrity of the item with respect to the intermediate locations, times, and chronological order of the visits for its supply chain.

Contributions: Our contributions in this paper are:

1) We provide an in-depth analysis of the security concerns for the global supply chain system. We present the requirements and deficits of the current process, and provide the necessary motivations for the work. The observations are used to illustrate our system model and the threat model.

2) We present a novel endorsement oriented scheme to preserve the integrity of the supply chain mechanism. The proposed architecture addresses the preservation of information as a product travels through the supply chain to reach the consumers.
3) We provide evaluation of the security for the proposed architecture to illustrate the feasibility of the design.

The rest of the paper is organized as follows. Section II discusses the concerns of the current global supply chain system, and the motivation behind the work presented in this paper. The system model and the threat model is presented in Section III and Section IV respectively. Section V presents a novel secure supply chain integrity preservation scheme. The design analysis of the proposed scheme is discussed in Section VI. Section VII discusses the most related works in this field. Finally, we provide the conclusions and the future works in Section VIII.

II. Motivation

The global supply chain system is dependent on an interconnected network of transportation, supplier, manufacturer, and information technology. As a result, the cross-operational entities allow significant risks across a broad geographic and industrial topology. A report published by The White House discusses the national strategies for global supply chain security and suggests active collaboration with the international community [7, 8]. The report discusses the strategies to promote the timely, efficient, and secure movement of goods, such that to preserve the supply chain from exploitation. It also suggests the requirement to improve verification and detection capabilities to identify contaminated, tampered, and prohibited items. Given the circumstances, we believe, a secure and trustworthy supply chain integrity preservation scheme can effectively track and monitor the route of a product before it is delivered to the consumers.

In another article, Borg [9] has summarized the five different phases in the supply chain: (a) design, (b) fabrication, (c) assembly, (d) distribution, and (e) maintenance phase. In each of these phases, it is extremely important to protect the infrastructure from malicious firmware. Therefore, there should be strict control in the environments where the products are handled, with appropriate use of logical and physical tamper-proof seals. Additionally, access control and proper logging mechanisms should exist to keep track and monitor activities at the corresponding sites of the supply chain [9].

III. System Model

In this paper, we present a scheme to protect the integrity of the channel of distribution for an item. The supply chain information is stored as location proofs, based on the path through which a particular product travels. Our proposed scheme for preserving the supply chain information is based on certain entities in the system. In this section, we present the system elements, the corresponding type of proofs, and the system capabilities for modeling a secured supply chain integrity preservation scheme.

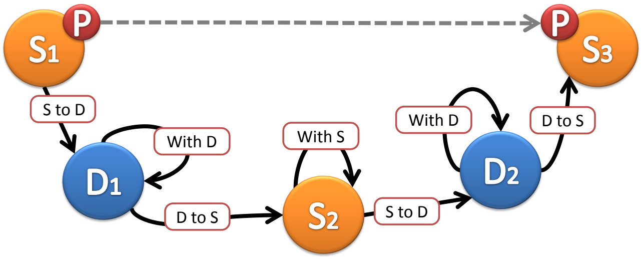


Fig. 1: Points of Interest in the Supply Chain System. The figure illustrates a product transported from S_1 to S_3, and the corresponding points of interest to preserve the supply chain information.

A. System Elements

The following explains each of the elements in the system model, their purpose, and their functionalities.

- **Product (P):** A product is the item which is being transported through the supply chain system. A product is identified with its bar code information, which stores the product identity and the product code.
- **Site Authority (S):** The site authority is the entity which is responsible for any given site in the path of the supply chain system. A site authority can be a manufacturing authority, and actually manufactures a specific component for a larger product. Alternatively, a site authority can also be an intermediate authority, where the particular product has been located at least once, during the process of being delivered from the manufacturer to the final consumer.
- **Operation Supervisor (O):** Each site authority needs to have an operation supervisor, who is present on site during the delivery or dispatch of a product. Therefore, all manufacturing and intermediate authorities have an operation supervisor available for his services at the given site. The operation supervisor asserts valid deliveries and valid dispatches from a particular site in the supply chain.
- **Delivering Authority (D):** The delivering authority is the entity in the scheme which is responsible for transporting a particular product between two destinations in the supply chain system. A delivering authority receives a particular product from a site authority, and delivers it to the next site authority according to the supply chain system.
- **Auditing Consumer (C):** The auditing consumer is the final recipient of a product. The auditing consumer is delivered the product along with a supply chain provenance. The supply chain provenance can then be validated to verify the claimed supply chain for the delivered product.

B. System Proofs

Given the activities within a supply chain, we are considering four different points of interest for our proposed scheme. As shown in Figure 1, a product P is being transported from site authority S_1 to S_3. In the supply chain system, the product actually is received from site authority S_1 by a delivering authority D_1. The product P is then transported to another location, and delivered to site authority S_2. Subsequently, delivering authority D_2 receives the product *P*, and delivers it to site authority S_3.

Given the above context, we observed four points of interest where the integrity of the information should be preserved. According to Figure 1, the four points of interest for a product *P* are: **(a)** the product residing with a site authority, **(b)** the product being transferred from the site authority to a delivering authority, **(c)** the product residing with the delivering authority, and **(d)** the product being transferred from the delivering authority to another site authority. The four cases cover the possible scenarios while a product travels through the supply chain system.

Thus, given the four points of interest for preserving the integrity of the supply chain information, we have modeled the following proofs for the proposed scheme.

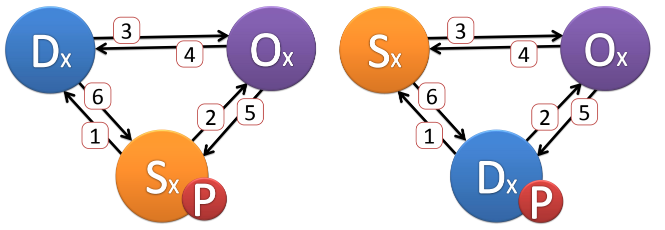
- **Holding Proof:** A holding proof is a logical evidence, which verifies the holding of a particular product at a particular site authority or a delivering authority.
- **Transferal Proof:** A transferal proof is a logical evidence, which verifies that a particular product has been handed over from a site authority to a delivering authority, or vice-versa.
- **Supply Chain Provenance:** A supply chain provenance is a sequence of site proofs and transferal proofs, which is chained together such that the order of the sequence cannot be altered. The provenance chain can thus be utilized to prove the sequence of sites that a particular product has traveled.

C. System Capabilities

We assume that each site authority *S* has server and WiFi network establishments. Additionally, the operation supervisor *O* and the delivering authority *D* carries mobile devices, which are capable of communicating with other devices and site authorities over WiFi networks. The devices have local storage for storing the supply chain proofs. It is assumed that the owner has full access to the storage and computation of the device, can run an application on the device, and can delete, modify, or insert any content in the data stored in the device. Additionally, it is assumed that the site authority, operation supervisor, and the delivering authority can access each others' public key.

A site authority *S* periodically updates the available operation supervisors list. When required, the site authority selects a supervisor from the list at random and sends a request to assert a proof for the given product *P*.

Upon completion of a schematic communication among all the parties, each entity receives a proof, which has been mutually asserted by the other entities. Based on the context, the proof can either be a holding proof or a transferal proof. At a later time, the auditing consumer uses the individual proofs from the supply chain provenance and the yielded assertions in the proofs to determine the validity of the claimed locations in the supply chain system.



(a) Product with Site Authority (b) Product with Delivering Authority

Fig. 2: Holding Proof Generation. The figures illustrate the sequence of messages interchanged among three entities during the process of generating a holding proof for two cases: (a) when the product is with the site authority and (b) when the product is with the delivering authority.

IV. Threat Model

We consider different classes of adversaries, and also combinations of these adversaries in a collusion attack to exploit the integrity of the supply chain. In our threat model, we lay out the assets of the supply chain system and the capability of attackers. An adversarial entity in this context refers to any outsider, or an insider, who has an ill intention of modifying the information within the supply chain.

The two main targets considered in our threat model are the place and time of the corresponding proofs within the supply chain, both of which correspond to a particular product *P*. An adversary should not be able to create a proof for any site authority or delivering authority, where the product *P* has not ever been located at. Also, even if the product *P* has been held by a specific authority, an adversary should not be able to create a proof for a different (local) time than the actual time of holding. Thus, a false proof of presence for a product *P* is one that asserts to the product *P*'s presence at a location, which has not been visited by the product, or for a different time than the actual time of visit.

V. System Architecture

In this section, we present the architecture for a secure supply chain integrity preservation system. The following subsections illustrate the schematic description for generating the required proofs and constructing a tamper-proof provenance chain for the supply chain system.

A. Holding Proof Generation

A holding proof refers to a proof of possession of a product at a particular time, and implies the accountable entity responsible for the product at the given time. Thus, as a product travels through the supply chain, a product may reside with either a site authority, or a delivering authority. Figure 2a and Figure 2b illustrate the sequence of messages for each case of generating a holding proof.

Holding Proof for Site Authority: As shown in Figure 2a, the site authority S_X is in possession of the product *P* and receives an asserted holding proof accordingly. The sequence of actions for the process are described as follows:

1) Site authority S_X sends a message to the delivering authority D_X, and requests for a holding proof for

product *P* at S_X. The request includes the product identity for product *P* and a signature from the site authority S_X.

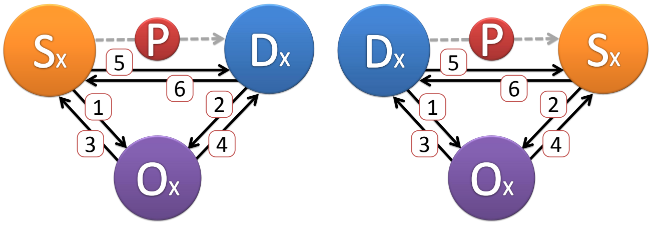
2) Site authority S_X sends a message to an available operation supervisor O_X, and requests for a holding proof for product *P* at S_X. This request also includes the product identity for product *P*.
3) The delivering authority D_X sends a request to the operation supervisor O_X to assert the validity of the claim of possession of product *P* by the site authority S_X. The request includes the identity of the site authority S_X, as well the identity of the product *P*, all of which are signed by the delivering authority D_X.
4) The operation supervisor O_X, at this point, validates the information received from the delivering authority D_X, and compares it to the initial request received from the site authority S_X in step 2. Once the information is successfully validated, the operation supervisor O_X sends an asserted response for the holding proof back to the delivering authority D_X.
5) The operation supervisor O_X then sends a copy of the asserted proof to the site authority S_X, the one which has been sent to the delivering authority D_X in the previous step.
6) The delivering authority D_X receives the asserted holding proof and validates the assertion provided by the operation supervisor O_X. Once the assertion is successfully validated, the delivering authority D_X sends the asserted proof to the site authority S_X.

After all the phases have completed, the site authority compares the two copies of the asserted proof: the one which was received directly from the operation supervisor O_X, and the other one which was received via the delivering authority D_X. If both the copies correspond to each other, the holding proof for product *P* at S_X has been successfully generated. In case there is a failure in matching the two copies, the site authority S_X issues an invalid assertion notification to the delivering authority D_X and the operation supervisor O_X, and discards the proof accordingly.

Holding Proof for Delivering Authority: As shown in Figure 2b, the delivering authority D_X is in possession of the product *P*, and receives a holding proof accordingly. The sequence of actions and messages are similar to the procedure described above. In this case, the delivering authority D_X initiates the process for generating an asserted holding proof. Subsequently, the site authority S_X and the operation supervisor O_X creates the asserted holding proof, and sends the proof to the delivering authority D_X. Similar to the method described previously, the delivering authority D_X compares the two copies of the asserted holding proof. If successfully validated, D_S stores the proof, or discards otherwise.

B. Transferal Proof Generation

The transferal proof is a logical statement which validates a successful transfer of authority and responsibility for a particular product *P* and a specific time. Implicitly, the transferal proof implies the release of liability of the product from a certain party. The transferal proof can be generated in two cases: (a) the product *P* has been transferred from the site authority to the delivering authority, or (b) from the delivering authority to the site authority, as shown in Figure 3a and Figure 3b respectively.



(a) Transfer from Site Authority (b) Transfer from Delivering Authority

Fig. 3: Transferal Proof Generation. The figures illustrate the sequence of messages interchanged among the three entities during the process of generating a transferal proof for two cases: (a) when the product is being handed over from the site authority to the delivering authority and (b) when the product is being handed over from the delivering authority to the site authority.

Transfer from Site Authority: In this case, the transferal proof is generated at the time when the product *P* is being handed over by the site authority to the delivering authority. As shown in Figure 3a, the sequence of actions are described as follows:

1) Initially, as the product *P* is handed over to the delivering authority D_X, the site authority S_X sends a transferal proof request from the operation supervisor O_X. The request includes the 'offload statement', that is, the product identity, the duration the product was held in possession by the site authority S_X, a signature from the site authority S_X, and the identity of the delivering authority D_X to which the product is being handed over to.
2) At the same time, when the delivering authority D_X receives the product *P*, it sends a message to the operation supervisor O_X to notify of the receipt of the product. The message includes the 'onload statment', that is, the product identity, a signature from the delivering authority, and the identity of the site authority S_X from which the product is being received.
3) At this point, the operating supervisor O_X compares the 'offload statement' and the 'onload statement'. This ensures that the transferal of the product *P* is occurring between the desired parties. Once successfully verified, the operating supervisor O_X asserts the 'onload statement', and forwards it to the site authority S_X.
4) Next, the operating supervisor O_X asserts the 'offload statement' and sends it the the delivering authority D_X.
5) The site authority S_X, at this point, compares his own 'offload statement' and the asserted 'onload statement' received from the operation supervisor O_X. If the statements are successfully validated, the site authority S_X sends an acknowledgement of transferal proof to the

delivering authority D_X.

6) The delivering authority D_X also compares his own ‘onload statement’ and the asserted ’offload statement’ received from the operation supervisor O_X. Once the statements are verified, and an acknowledgement is received from the site authority S_X, the delivering authority D_X sends an acknowledgement of transferal proof to the site authority S_X.

After successful completion of the above steps, the site authority S_X and the delivering authority D_X store the corresponding transferal proofs for future records. Each copy of the transferal proof bears an assertion from the operation supervisor. In case any of the validation procedures failed, the proof is discarded, and an invalid assertion notification is sent to the other entities in the system.

Transfer from Delivering Authority: The procedure for generating a transferal proof during the transfer from a delivering authority to a site authority is similar to the method described above. Instead of the site authority initiating the process, in this case, the delivering authority sends a request for generating a transferal proof. The request includes the ‘offload statement’ from the delivering authority D_X, which implies that the product *P* is being offloaded from the delivering authority D_X, after it was held in possession by the delivering authority D_X for a specific duration of time. At the same time, the site authority receives the product *P*, and issues an ‘onload statement’ to the operation supervisor O_X. Similar to the previous process, the delivering authority D_X receives an asserted transferal proof with the ‘onload statement’ from the site authority S_X, and the site authority S_X receives an asserted ‘offload statement’ from the delivering authority D_X. At any point in the protocol, any failed verification results in an invalid assertion notification.

C. Maintaining a Supply Chain Provenance

The individual holding proofs and transferal proofs are generated at the corresponding locations according to the supply chain of a product. However, the individual proofs are not organized in any sequence. Thus, the supply chain provenance serves the purpose of chaining the proofs in a manner such that the order and sequence of the proofs cannot be altered. A holding proof for the site authority is required to be succeeded by a corresponding transferal proof from the site authority to the delivering authority. The next proof in the chain is required to be another holding proof for the delivering authority.

Figure 4 illustrates a provenance chain for the supply chain system. A product *P* is moved from site authority S_1 to S_2, and is transported by delivering authority D_1. The sequence of proofs in the provenance chain is thus: holding proof for S_1, transferal proof for S_1 to D_1, holding proof for D_1, transferal proof for D_1 to S_2, and holding proof for S_2. A supply chain provenance which exhibits the given sequence is a valid claim for the supply of the product *P* from site authority S_1 to S_2. In the proposed protocol, the sequence preservation of the proofs to create the provenance of the supply chain system has been done using hash chaining.

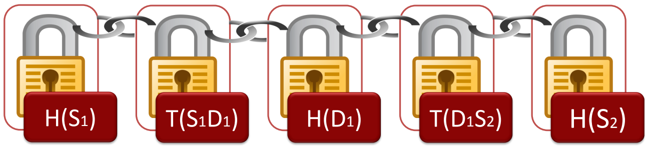


Fig. 4: A Supply Chain Provenance. The figure illustrates a product transported from S_1 to S_2, and the corresponding proofs which are being used to create a secure supply chain provenance.

A hash chain is a concept of creating hash values from a sequence of linked values using standard hash functions, such as SHA-256. The provenance chain in this case can thus be created accordingly. Initially, a hash is created for holding proof, $hash_{H_1} = [H(S_1)]$. After the transferal proof $T(S_1 D_1)$ is created, a hash is created by padding the previous hash with the current proof, $hash_{T1} = [T(S_1 D_1) + hash_{h1}]$. Therefore, the hash chain is formed as follows:

- $hash_{H1} = [H(S_1)]$
- $hash_{T1} = [T(S_1 D_1) + hash_{H1}]$
- $hash_{H2} = [H(D_1) + hash_{T1}]$
- $hash_{T2} = [T(D_1 S_2) + hash_{H2}]$
- $hash_{H3} = [H(S_2) + hash_{T2}]$

To secure the hash chain, at each step, the hash is signed by each of the entities *S*, *D*, and *O*. This ensures that the order and integrity of the sequence is preserved. In this case, the final hash value $hash_{H3}$, is signed by the site authority S_2, the delivering authority D_1, and the operational supervisor O_2. Subsequently, the corresponding signed hashes can be presented to the auditing consumer, along with the proofs. The auditing consumer can then securely verify each of the holding proofs, transferal proofs, and their order of sequence.

However, the hash chaining approach may lead to overhead data storage for the individual hash values for each phase. A possible solution for reducing the data storage for hash chaining can be implemented using Bloom filters [10]. Each hash value is included within a fixed length Bloom filter. At the end, the Bloom filter is provided along with the individual proofs. Unfortunately, the Bloom filter approach has its known disadvantages for having false positive results for verification. We are currently working on designing an efficient process of maintaining the provenance chain using Bloom filters, such that to have the false positive rate as low as possible.

VI. Design Analysis

For the purpose of our security analysis, we define the following symbols: honest site authority *S*, malicious site authority $\bar{S}$, honest delivering authority *D*, malicious delivering authority $\bar{D}$, honest operation supervisor *O*, and a malicious operation supervisor $\bar{O}$. A combination of the six behaviors gives us eight different scenarios: $SDO, \bar{S}DO, S\bar{D}O, SD\bar{O}, \bar{S}\bar{D}O, \bar{S}D\bar{O}, S\bar{D}\bar{O}$, and $\bar{S}\bar{D}\bar{O}$. The collusion patterns can thus be modeled using the different behaviors of the entities.

In our proposed solution, we enforced three separate interaction channels for generating a mutually asserted proof. The resulting asserted proofs are again cross-referenced against the other party. A successfully generated proof thus implies that each of the entities have willingly asserted the information available within the proof. Additionally, each of the entities are provided a copy of the proof for their own record keeping. Therefore, as long as at least one of the entities display honest behavior (*S*, *D*, or *O*), the protocol succeeds in generating secure and valid proofs for the supply chain. The only scenario in which the model fails is in case of a three-way collusion $\bar{S}\bar{D}\bar{O}$. However, we argue that all security protocols require at least one party to be trusted.

In a probabilistic model, given the eight combinations, we are successful in preserving the integrity of the supply chain for the seven combinations, where at least one entity is honest. Therefore, our system is stable for 87.5% of probable cases. On the contrary, for any other two-party protocol, as both parties need to be trusted at all time, the stability is only for 25% of the possible combinations.

VII. Related Works

Secure supply chain integrity preservation requires a reliable location reporting and tracking solution. Global positioning systems [11] serves general location reporting purposes. However, it is not suitable as a secure solution. Combining GPS signals with cellular tower triangulations and access network channel can be used to verify the location of a device. Gabber *et al.* proposed a model using multi-channel information to verify the location [12]. Unfortunately, malicious entities can bypass such combinatorial schemes [13, 14]. Additionally, GPS signatures [15] are not useful since they are open to spoofing attacks [13].

Research on hardware oriented approaches for localization requires additional functionality of devices [16–18]. Signal attenuation can also be utilized to verify the presence of a device in the vicinity [19–21]. Other approaches use asynchronous measurement of round trip times between the user devices and access points [22, 23]. However, these mechanisms suffer from channel noise, line-of-sight limitations, complexity of deployment, and manipulation of information by an attacker in close proximity of the devices. In our design, we have considered a three-party interactive solution. We propose using timing thresholds between each pair of communicating parties to ensure three-way proximity.

Secure and unforgeable location proofs was discussed by Waters *et al.* [24]. A secure geo-tagging service for user-generated content has been proposed by Lenders *et al.* [25]. However, these schemes require highly coupled entities with a monolithically centralized architecture. Saroiu *et al.* illustrated a mechanism using signed public keys of users and access points for creating timestamped location proofs [14].

Trusted Platform Module (TPM) and virtual machine based attestation for trusted sensor readings have been proposed by Saroiu *et al.* [26] and Gilbert *et al.* [27] respectively. Luo *et al.* have presented a method, which allows the generation of privacy-preserved location proofs [13]. Other methods of secure localization include utilizing social networks [28], or combination of wireless medium, such as WiFi and Bluetooth [29]. However, localization is only a part of the work. Our proposed scheme delivers a model to localize, and issue a secure holding proof or a transferal proof, based on the current context.

VIII. Conclusion

The supply chain system is globally interconnected network of transportation, suppliers, manufacturers, and information technology. The multitude of entities has introduced a greater risk in maintaining the integrity of the supply chain system. In this paper, we have described the motivation and desired properties of a secure supply chain process. Based on the given requirements, we have presented a model for the system elements and capabilities, system proofs, and the corresponding threat model. We utilized the model to design secure generation of holding proofs and transferal proofs, depending on the given context of actions within the supply chain. Furthermore, we also proposed a secure scheme for maintaining the supply chain provenance using hash chaining and Bloom filters. The paper also includes a security analysis of the design which illustrates feasibility of deployment for the proposed scheme.

The proposed scheme in this paper includes detailed description of the functionalities of the system. However, we would like to develop a completely distributed and decentralized prototype for the scheme, which can be used to practically evaluate the performance of the design. Additionally, our current work includes designing a modified Bloom filter which would allow us to reduce the false positives to as low as possible.

Acknowledgment

This research was supported by a Google Faculty Research Award, the Office of Naval Research Grant #N000141210217, the Department of Homeland Security Grant #FA8750-12-2-0254, and by the National Science Foundation under Grant #0937060 to the Computing Research Association for the CIFellows Project.

References

[1] J. T. Mentzer, W. DeWitt, J. S. Keebler, S. Min, N. W. Nix, C. D. Smith, and Z. G. Zacharia, "Defining supply chain management," *Journal of Business logistics*, vol. 22, no. 2, pp. 1–25, 2001.

[2] D. Simchi-Levi, E. Simchi-Levi, and P. Kaminsky, *Designing and managing the supply chain: Concepts, strategies, and cases*. McGraw-Hill United-States, 1999.

[3] S. Stephens, "Supply chain operations reference model version 5.0: a new tool to improve supply chain efficiency and achieve best practice," *Information Systems Frontiers*, vol. 3, no. 4, pp. 471–476, 2001.

[4] B. M. Beamon, "Measuring supply chain performance," *International Journal of Operations & Production Management*, vol. 19, no. 3, pp. 275–292, 1999.

[5] L. Shaughnessy, "Probe finds 'flood' of fake military parts from China in U.S. equipment," Security Clearance, CNN Security News. Available online at http://security.blogs.cnn.com/2012/05/22/probe-finds-flood-of-fake-military-parts-from-china-in-u-s-equipment/, Last accessed June 2013, Tech. Rep., May 2012.

[6] P. Courson, "Report: Bogus U.S. military parts traced to China," CNN U.S. Available online at http://www.cnn.com/2011/11/07/us/u-s-military-bogus-parts, Last accessed June 2013, Tech. Rep., Nov 2011.

[7] The White House, "National strategy for global supply chain security," *Available online at http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf*, Jan 2012.

[8] The White House, "National strategy for global supply chain security implementation update," *Available online at http://www.whitehouse.gov/sites/default/files/docs/national_strategy_for_global_supply_chain_security_implementation_update_public_version_final2-26-131.pdf*, Jan 2013.

[9] S. Borg, "Securing the supply chain for electronic equipment: A strategy and framework," *Internet Security Alliance Publication*, Nov 2008.

[10] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communication of the ACM*, vol. 13, no. 7, pp. 422–426, 1970.

[11] P. Enge and P. Misra, "Special issue on global positioning system," *Proceedings of the IEEE*, vol. 87, no. 1, pp. 3 –15, jan. 1999.

[12] E. Gabber and A. Wool, "How to prove where you are: tracking the location of customer equipment," in *Proceedings of the 5th ACM conference on Computer and communications security (CCS)*. ACM, 1998, pp. 142–149.

[13] W. Luo and U. Hengartner, "Proving your location without giving up your privacy," in *Proceedings of HotMobile*, 2010, pp. 7–12.

[14] S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs," in *Proceedings of HotMobile*, 2009, pp. 1–6.

[15] D. E. Denning and P. F. MacDoran, "Location-based authentication: Grounding cyberspace for better security," *Computer Fraud & Security*, vol. 1996, no. 2, pp. 12–16, 1996.

[16] S. Capkun and J. Hubaux, "Secure positioning of wireless devices with application to sensor networks," in *Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societie (INFOCOM)*, vol. 3. IEEE, 2005, pp. 1917–1928.

[17] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proceedings of the 2nd ACM workshop on Wireless security (WiSe)*. ACM, 2003, pp. 1–10.

[18] S. Čapkun and M. Čagalj, "Integrity regions: authentication through presence in wireless networks," in *WiSe '06: Proceedings of the 5th ACM workshop on Wireless security*. ACM, 2006, pp. 1–10.

[19] Aruba Networks, Inc., "Dedicated air monitors? you decide." Online at http://www.arubanetworks.com/technology/tech-briefs/dedicated-air-monitors/, 2006.

[20] S. Pandey, F. Anjum, B. Kim, and P. Agrawal, "A low-cost robust localization scheme for wlan," in *Proceedings of the 2nd annual international workshop on Wireless internet*. ACM, 2006, p. 17.

[21] P. Tao, A. Rudys, A. Ladd, and D. Wallach, "Wireless lan location-sensing for security applications," *Computing Reviews*, vol. 45, no. 8, pp. 489–490, 2004.

[22] S. Brands and D. Chaum, "Distance-bounding protocols," in *Proceedings of the Workshop on the theory and application of cryptographic techniques on Advances in cryptology (EUROCRYPT)*. Springer-Verlag New York, Inc., 1994, pp. 344–359.

[23] M. Youssef, A. Youssef, C. Rieger, U. Shankar, and A. Agrawala, "Pinpoint: An asynchronous time-based location determination system," in *Proceedings of the 4th international conference on Mobile systems, applications and services*. ACM, 2006, pp. 165–176.

[24] B. R. Waters and E. W. Felten, "Secure, private proofs of location," Technical report TR-667-03, Princeton University, January 2003.

[25] V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, "Location-based trust for mobile user-generated content: applications, challenges and implementations," in *Proceedings of HotMobile*. ACM, 2008, pp. 60–64.

[26] S. Saroiu and A. Wolman, "I am a sensor, and i approve this message," in *Proceedings of HotMobile*, 2010, pp. 37–42.

[27] P. Gilbert, L. P. Cox, J. Jung, and D. Wetherall, "Toward trustworthy mobile sensing," in *Proceedings of HotMobile*. ACM, 2010, pp. 31–36.

[28] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location privacy via private proximity testing," in *Proceedings of Network and Distributed System Security Symposium*, vol. 2011, 2011.

[29] P. Traynor, J. Schiffman, T. La Porta, P. McDaniel, and A. Ghosh, "Constructing secure localization systems with adjustable granularity using commodity hardware," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, 2010, pp. 1–6.