Trust Framework for RFID Tracking in Supply Chain Management

Manmeet Mahinderjit- Singh and Xue Li

School of Information Technology and Electrical Electronic
University of Queensland, Australia

Abstract. RFID tracking systems are in an open system environment, where different organizations have different business workflows and operate on different standards and protocols. RFID tracking to be effective, it is imperative for RFID tracking systems to trust each other and be collaborative. However, RFID tracking systems operating in the open system environment are constantly evolving and hence, the related trust and the collaborations need to be dynamic to changes. This paper presents a seven-layer RFID trust framework to promote the resolution of merging with both social and technology traits in enhancing security, privacy and integrity of global RFID tracking systems. An example of integration of our trust framework with supply-chain management applications and trust evaluation is also presented.

1 Introduction

In the business world, trust is tremendously important [1, 2]. Trust counts in selecting partners, software and hardware infrastructure used and even information transmitted. Trust is distinguished as a decision making instrument when joined together with security, privacy and integrity to improve the adoptions and reliance of the system. Trust is not symmetric even if *A* trusts *B*, expecting *B* to return the equal trust to *A* is not possible. Besides that trust is also intransitive as if *A* trusts *B* and *B* trusts *C*, *A* may not trust *C*.

The significance of trust in a new emerging ubiquitous technology known as RFID is critical. RFID, a term for Radio Frequency Identification provides non-line sight and a better item-tracking manner compared to barcode systems. However public acceptance in RFID implications systems is still an open question. There are a few questions denoting the needs of trustworthiness in RFID systems that are related to the characteristics of tags, communication channels and operational natures. In a large-scale item-tracking environment, the co-existence of multiple network protocols, different standards and data structures from different organizations, and the need for reliable operations are essential[3]. For two different partners, one using EPCglobal (http://www.epcglobalinc.org) network and the other using UCLA WinRFID, how would the different set of integration platforms, data structures and even communication protocols between them operate with 100% reliability and confidence? Besides that, the lack of security capability on RFID tags due to its hardware

Mahinderjit Singh M. and Li X. (2009).
Trust Framework for RFID Tracking in Supply Chain Management.
In *Proceedings of the 3rd International Workshop on RFID Technology - Concepts, Applications, Challenges* , pages 17-26
DOI: 10.5220/0002172400170026

constraints and the insecure communication channels makes system vulnerable to the security threats. A competitor capable of tracking and tampering the sensitive information on tags might result in counterfeiting and cloning or fraud product labels [8]. Data on tag means the information in the enterprise database. Even though, there is little data stored on tag, it would be sufficient to be misused by distrusted parties in launching attacks. So, how we protect and ensure that tag content is only accessible by legitimate parties becomes a problem. In addition, the facts that tags are readable from the distances outside the range without owners' knowledge can cause the *link ability threat* in supply chain management. In supply chain management, ownership changes can be automatic and at a high speed. Unauthorized reading of RFID tags might happen after tags left supply chain warehouses. This explains why we need to exploit trustworthy to handle the ownership changes during the lifespan of RFID tags in supply chain applications. The existing RFID trust services management designed by Verisign (http://www.verisign.com/static/028573.pdf) for the EPCglobal supply chain only provides trust decision based on authentication and authorization mechanisms (*hard trust*) without any concerns on security threats and the detection or the *soft trust* such as past history [4]. Hence our idea here is to design a seven-layer trust framework with the capability of prevention and detection, so to act as a reputation system based on the supply chain partners' experiences and beliefs. The proposed trust framework aims to deal with security attacks such as cloning and fraud RFID tags. This framework is the first of its kind. The contributions of this study are that (1) it provides a complete framework for embracing trustworthiness for large scale RFID global tracking systems; (2) it suggests a guideline to design and implement the framework; and (3) it shows an evaluation guideline for this framework.

The significance of our proposed frameworks will be demonstrated by illustrating RFID cloning attacks and showing how cloning attacks within supply chain can be handled by this trust framework. RFID tag cloning represents a serious counterfeiting problem in a supply-chain environment [5]. At hand, methods used to handle counterfeiting attack caused by RFID tag cloning are track and trace mechanism [5], product authenticity [6] and RFID tag authentication [6]. In this paper, we only focus on securing RFID tags by employing a trust framework. The trust framework proposed in this paper does not consider the trust of Quality of Services (Qos) that are used for data quality and traceability. This paper is structured as follows. Section 2 discusses the related work. Section 3 describes a seven-layer trust framework. Section 4 studies the assimilation of the trust framework and RFID supply-chain applications in handling cloning and fraud attacks. Section 5 discusses further research issues and presents the conclusions.

2 Related Work - Trust in Sensor Networks and Ubiquitous Computing

Trust in ubiquitous computing environments plays a vital role in ensuring system security [1, 2]. The fusion between security concerns, the social aspects, and technology demands represents the ability of building a trust foundation. Trust represents both human factors as well as technological factors. Yang [1] defines the trust as a

combination of system usage experiences and social perspective. She also describes that when partners interact cooperatively and share positive experiences, the impact on any technology usage will increase dramatically simply because human positive attitudes and beliefs boost the trust.

In contrast, Hossain and Prybutok [7] introduce a few vital concepts in the trust establishment including privacy, security and regulation issues aiming at increasing customer's confidence. They assert that users personal tolerance in taking certain extend of risks when dealing with security and privacy works independently [7]. Meanwhile, policies and regulations can raise user's trust [7]. The trust can be conveyed by evaluating security and privacy threats and inset solutions.

Our trust framework is different from Yang's [1] concepts in terms of the technological trust factors. Yang's work emphasizes the importance of user decision-making level, which asserts the essences of experiences in interaction of knowledge and shared values among partners. Whereas, we concentrate on the system vulnerabilities and on how to employ security, privacy and detection functions to deal with the threats. Our framework focuses on both the prevention and detection that are unified as a system function. Given that RFID technology is widely accessible and is bringing socio-economic advantages, the concerns on both performance and trust is equally highly regarded. Besides, we will make use of the category factors involving beliefs, attitudes and cultures in organizations since each of these social aspects are important in establishing trust.

3 RFID Trust Framework

Fig.1 shows the trust attributes in our proposed framework. There are seven layers from inside out. An outer layer function is built upon its inner layers and each layer is equally vital. Beginning from layer 1 up to layer 7, the transitions from technology core to social perspectives are shown. Each layer function is describe as follows.

- Layer 1 (Security-Authenticity) Any connected RFID system should be authenticated using lightweight protocol both symmetric and asymmetric authentication catering to the hardware constraint in the system itself. Besides that, each component should be mutually authenticated and identifiers must be encrypted using hash algorithms with keys generated randomly to maintain uniqueness. Once the product is secured the need to maintain privacy will be minimal.
- Layer 2 (Privacy – Locality, Timeline) The context of privacy factor such as time and locality are utilized based on different applications the framework will work with. As for certain application which requires tracking such as supply chain pharmaceutical drugs pedigree tracking, privacy is in concern since the tracing and tracking process might breach the privacy. In contrast, the identification application can embrace this layer functionality better.

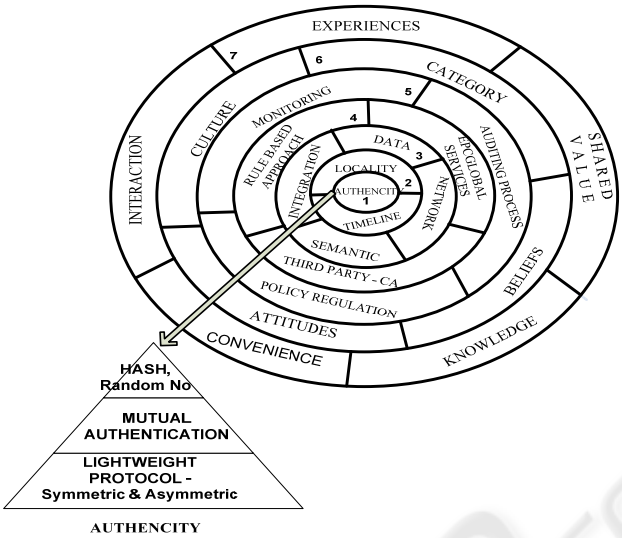

Fig. 1. Seven Layers RFID Trust Framework.

- Layer 3 (Data – Network, Semantic, Integration) The framework allows the use of open RFID architectures in which heterogeneous standards and networks from different partners are able to work together with the mapping functions. The internet communication channel can be secured by using asymmetric key encryptions such as RSA and AES [8].
- Layer 4 (Detection – EPCglobal, Third-Party CA, Rule Based Engine) EPCglobal services need to add on the EPC Product Authentication Services (EPC-PAS) and EPC-Trace Analysis Service (TAS) in detecting cloning tags [6]. The need to regulate middleware EPC services such as ONS, DS and EPCIS (http://www.epcglobalinc.org) upfront could help in reducing errors in any application implementation. Existing Certificate Authority (CA)[11] can be used here since asymmetric techniques are commonly used in sensor networks. CA will be placed in the EPC network core for establishing transitive relationships between the partners and handling key management. There are several IDS expert system-algorithms and techniques that can be used.
- Layer 5 (Monitoring – Auditing Processes, Policy Regulation) Monitoring tools include the third party system policy regulation such as Bill of Rights [9] and ISO standards. The tools will monitor the whole RFID operation based on the policy enforcement and auditing processes. If any risk is encountered, the monitoring function will eventually records and alarm business owners and react on attacks.
- Layer 6 (Category - Culture, Attitudes, Beliefs) Social aspect of one's culture, beliefs and attitudes will impact tremendously to the positively shared experiences in the next level of business decisions. An example will be if a partner's RFID experiences are positive, then the impact on his beliefs and attitudes will be demonstrated in the (next) level 7 when interactions among business partners are established [1].

- Layer 7 (Experiences - Interaction, Shared Values, Knowledge, Conveniences) When two partners begin to share their added value past experiences and knowledge especially the positive ones by the means of communication and interactions, the confidence level of RFID products will increase.

The core of the whole framework is Layer 1 - the security attributes which consist of authentication modules. Now we will compare our trust framework against the latest Pedigree Standard ratified by EPC global (http://www.rfidupdate.com/articles/index.php?id=1277). The standard of e-pedigree is known as GS1 EPCglobal Electronic Pedigree Standard aims to protect consumer from counterfeit drugs by tracking the drugs. Since this standard track the authenticity of drugs, the Layer 1 security can be embedded within this standard. In handling drug counterfeit, the need to authenticate, and track the history of location, time and drug serialization is important. However, our trust framework provides more than that, because it is able to detect the counterfeit attacks in the first place by using its Layer 4 (Detection) modules. Next sections will demonstrates how our trust framework will function in a supply chain environment in handling the cloning attack using our trust evaluation scale.

4 Trust Framework for RFID Tracking in Supply Chain Management

In this section, the developments of the proposed RFID trust framework is presented within a scenario of supply-chain management, definition of clone and our trust framework evaluation is also given here.

A. An Example of Supply Chain Management (SCM)

Supply chain management (SCM) is one of the important applications that use RFID for tracking products movement between suppliers, manufacturers, shipping handlers, distributors, retailers, and customers in an open system environment. The flow of goods is from the manufacturer to distributors and then to wholesalers. In a supply chain utilizing RFID technology, all transactions including individual consumer purchases can be automated. The global tracking requires the interactions between various organizations, partners, and technologies. There are different workflows for different businesses, different data flows for different standards and protocols, and different item movements for different ownerships and needs of handling (e.g., at either container or item level of movements). In RFID, supply chain process mostly uses two ranges of electromagnetic spectrums which are 13.56 (HF) and 860-960 MHz (UHF). The problems lie in supply chain applications are the insecure and vulnerable communication channel of products movement, multiple network architectures, different standards among partners [3], and security key management issues between tags and readers. There are a few assumptions that need to list before we can portray our solutions.

- The transaction between supply-chain partners is performed on the Internet via EPC network.

- A root Object Naming System (ONS) is used as an information directory of manufacturers regarding their products in the EPC network.
- Each supply-chain organization will have its own local ONS and local EPCIS (hub for product information).
- A root Discovery Service (records for EPCIS address) which functions as a "search engine" to provide information about an EPC, including other organizations that handle it during its lifecycle within a supply chain.
- Certificate Authority (CA) works as a third party authorization and is placed in an EPC network.
- Tags used here are EPC *class 1 gen 2* type and passive.

However before we proceed to discuss how our trust framework will function in handling RFID tag cloning within a supply chain application, it is essential to define clone in RFID tag context. Let assume set A contain the RFID genuine tags and set B contain cloned tags derived from set A. A genuine tag is known as TG and a cloned tag is known as TC. *I* denote an intruder. A list of attacks (*S*) includes Skimming (*S1*), Sniffing (*S2*), Active Attack (*S3*), Reverse Engineering (*S4*) and Cryptanalysis (*S5*) [6, 8].

Thus;

A = {TG1, TG2, TG3}
B = {TC1, TC2}
S = {S1, S2, S3, S4, S5}.

Hence TC1 is a clone of TG1; if and only if both tags have identical TIDs (tag identifier) and share the same form of characteristics. Once the TIDs are the same, all the data and structure of the tag's EPC code such as header, manufacturer id, object class and serial number are identical, i.e., |TG| = |TC|. A TC exists when *I* performs *S* either a single *S* or a combinations of *S* against TG. *S* will produce cloning attack. RFID Cloning is a process of injecting imitated EPC tags in a normal genuine EPC tags batch. Cloning attack can be detected mainly by counting the tags with the references to their locations and history traces, observing tag's abnormal behavior and by utilizing a third party clone detector. A direct consequence of cloning in SCM is counterfeiting, where a genuine article tagged with an RFID label may be reproduced as a cheap counterfeit and tagged with a clone of the authentic RFID label. Hence the lack of authentication allows an attacker to fool a security system into perceiving that the item is still present or fool automated checkout counters into charging for a cheaper item. Our trust framework can be used to ensure authentication; thus preventing the cloning from occurring at the first place and also detecting the cloning in the supply chain application.

The trust framework starts from inside out, from layer 1 up to layer 7 in handling cloning tag attack.

Layer 1 (Security) – Tag authenticity between two different partners will be provided by asymmetric key encryption using elliptic curve cryptosystem. Three-way mutual authentications are performed through random number synchronisations. This step will ensure authoritative access as only legitimate readers of partners can read the tags. Hence, two of supply chain security requirements, which are tag authenticity

and authoritative access, are complied [10]. The evaluation here is done by system analysis. Besides that the authenticity layer is also capable of authenticating supply chain partners and support various authentication protocol such as PKI and Kerberos [11].

Layer 2 (Privacy) – The privacy component is to support the handling of cloning attacks because tracking tags is an essential way towards cloning and this may compromise partners privacy. Thus this layer is to ensure the privacy protection while dealing with cloning attacks.

Layer 3 (Data) – At this situation, the ability for multiple partners to work together in an open system architecture is to be detailed. For instances, in supply chain there will be partners using different RFID integration platforms (e.g., EPCglobal or WinRFID), with various data semantics (e.g., PML or EPC), and different communication protocols. By using corresponding mapping functions, our trust framework will allow open architecture to work together as long as the channel is secured using asymmetric encryption (e.g., RSA) and tags authentication is guaranteed.

Layer 4 (Detection) – The usage of CA will manage the shared security keys between partners to guarantee RFID trustworthy. If EPC network is used, then Discovery service will also be used to help partners in track and tracing of products. Cloned tag can also be detected by Intrusion detection system (IDS). The evaluation on IDS is done based on IDS decision output and ROC curves (http://en.wikipedia.org/wiki/Receiver_operating_characteristic).

Layer 5 (Monitoring) – Once detected by IDS, through the response processes, the stages at which the cloning occurred is detectable. Partners will be informed on the event and further actions such as data cleaning and legal actions against the adversary can be initiated.

Layer 6 and 7 (Category & Experiences) – Along with the accumulation of experiences and successful neutralization of attacks, more transactions amongst supply-chain business partners will get through successfully. This will progressively establish the trust and the confidence between the business partners and between the interoperating systems. A reputation system consisting partners experiences information will be evaluated. This reputation system can be constructed centrally or in a distributed manner across SCM partners. Next section we will look into our trust structure based on cloning attack and supply chain discussed above.

B. RFID Tag Cloning Threat in Supply Chain & Trust Evaluation

We will present a modeling framework representing the problem and conduct formal reasoning and measurement to trustworthiness in a RFID supply chain environment that aims for a better operational decision-making. Mathematical formalisms offer analysis, but these approaches require strong assumptions, and are only good for specialized, idealized environments, while practical approaches have no analysis and hard to adapt [12]. Hence, trust formalization should support formal reasoning and should have the ability to deal with interactions between technology and human social behavior. A basic concept related to RFID trust is as listed below:

RFID Business Partner, RBP = {A, B Є RBP}

The trust definition for several partners includes:

(i) If RBP A trusts RBP B in dealing RFID services transaction, S then there is a TRUST $_A$ (B, S)
(ii) If RBP B trusts RBP A in dealing RFID services transaction, S then there is a TRUST $_B$ (B, S)
(iii) If RBP ЄA trusts himself in providing RFID services transaction, S then there is a TRUST $_A$ (A, S)
(iv) We use TRUST = {(A, B, S), A, B Є RBP, S Є S and Trust A = (A, S)}. It means RBP A trust RBP B in providing Service S
(v) Relationship of Trust
(vi) Optimistic Approach Rule

Next, we give trust reasoning rules based on the concept structure above. For our trust framework to be used for the security and privacy challenges, the need for every attack to be studied is essential. Learning of the vulnerability of how the attacks occur to the RFID system is to understand the ways the attacks happen. As a result, the type of an attack threat will determine the need for whether Layer 1 – Authenticity or Layer 2- Privacy is needed or not. For instances, the reasoning for cloning attack can be shown by four different rules.

- *RULE 1 (PREVENT)*

  Authenticity (Layer1) => PREVENT
  ⌐ Privacy (Layer 2) => PREVENT
  (Authenticity (Layer 1) ^ ⌐ Privacy (Layer 2) => PREVENT)

This shows that cloning attack requires the authenticity and not the privacy approach in preventing the threat of cloning to ever occur in the RFID system. If sufficient prevention measurement is taken, the first foundation against cloning can be achieved.

- *RULE 2 (DETECT)*

  (Detection (LAYER 4) ^ Monitoring (Layer 5) => DETECT)

The second rule needs both the detection modules such as intrusion detection and monitoring to function hand in hand to handling the cloning attack. Any attack can be encounter by using either one layer.

- *RULE 3 (INTERGRATE)*

  RULE 1 ^ RULE 2 => DATA
  (Authenticity (Layer 1) ^ ⌐ Privacy (Layer 2) ^
(Detection (Layer 4) ^ Monitoring (Layer 5) =>INTERGRATE)

This rule emphasize on Layer 3, the data integration layer. Both Rule 1 and Rule 3 would be embedded into the integration layer.

- *RULE 4 (SOCIAL)*

The social rule is for the culture and experience layers.

Culture (Layer 6) ^ Experience (Layer 7) => SOCIAL
¬ DATA (LAYER 3) => ↓ SOCIAL => ¬ TRUST
DATA (LAYER 3) => ↑ SOCIAL => TRUST

Where ↓ means low and ↑ means high. When the integration of prevention and detection is not done, the social factor consisting Layers 6 and 7 will be low. Consequently, the trust confidence will reduce. But when Layer 3 function is preserved, the social layers will be boost and the impact will be in higher confidence rate.

In an optimistic trust approach the need the whole trust framework such that in the example for RBP A and B for RFID service, S is as follow:

(PREVENT RBP A ^ PREVENT RBP B ^ DETECT RBP A ^ DETECT RBP B => INTERGRATE (A, B) => ↑ SOCIAL => TRUST (A, B, S))

The successful deployment of the trust framework is determined by the above rule. In order to handle cloning attack effectively, a prevention system for RFID business partners should be in place. There should also be a cloning intrusion-detection system and monitoring system in both ends of business partners. The prevention and detection module is integrated together through the data and network architecture designs in the integration layer. As a result, with all these components in place, the social impact will increase and enhance the trust towards the RFID supply chain open system entirely.

5 Conclusions and Further Research

In this paper, a comprehensive and novel seven-layer trust framework is introduced. The framework is presented with essential attributes in designing a secure and trustworthy open system for global RFID-enabled item tracking. Nevertheless, producing a working trust framework does not come without trade-offs. The introduction of such a trust framework will increase tag-processing overhead, key management overhead, and reduce the speed of tag reading. The framework aims to help business owners cope with the effectiveness of global item-tracking tasks that involve different infrastructures, communication channels, and partners. With increasing business owner's intention to use RFID system in their organizations, the proposed trust framework could be used as a 'cooking book' to treat security threats by modelling prevention, detection, and monitoring functions in a seven-layer control mechanism. Even though a great deal of research is currently in progress on RFID security and privacy issues, the problem such as cloning is still not handled properly. Detecting cloning tags is a relatively simple task by utilising timestamps, synchronisation features, and rule-based inference engine [9]. However there isn't a standardised intrusion detection system which provides a low false alarms and high precisions at the moment [13]. Besides that prevention of cloning from happening is still an open issue. As a result, we are currently developing an expert system for detecting cloned tags in an open system environment. Our future work will look into a depth research

on an optimistic cloning prevention mechanism that can provide a range of prevention services for industries to select from based on their business requirements.

References

1. Yang.G,"Trust and Radio Frequency Identification (RFID) Adoption within an Alliance", 38th Hawaii International Conference on System Sciences – 2005.
2. Wolfe S.T, Ahamed S.I *et al.* "A Trust Framework for Pervasive Computing Environments", 2006 IEEE, Computer Systems and Applications, March 8, 2006 pp. 312 – 319.
3. Derakhshan R., Orlowska M. E and Li X, "RFID Data Management: Challenges and Opportunities", 2007 IEEE International Conference on RFID Gaylord Texan Resort, Grapevine, TX, USA
4. Lin, C., Varadharajan V., Wang Y., Mu Y.: On the design of a new trust model for mobile agent security. In: The 1st International Conference on Trust and Privacy in Digital Business (TrustBus04), Lecture Notes in Computer Science, Vol. 3184, pp. 60–69. Springer, Zaragoza (2004)
5. Koh, R., *et al*., White Paper: Securing the Pharmaceutical Supply Chain.2003, AUTO-ID CENTER, Massachusetts Institute of Technology.
6. Lehtonen.M, "Trust and Security in RFID-Based Product Authentication Systems" Systems Journal, IEEE, 2007
7. Hossain.M and Prybutok V, "Consumer Acceptance of RFID Technology: An Exploratory Study", IEEE Transactions on Engineering Management, Vol. 55, No. 1, Feb 2008.
8. Juels. A, "RFID security and privacy: a research survey" IEEE journal on selected areas in communications, vol. 24, no. 2, February 2006, 2006. 24(2): p. 381-394.
9. Johnston.G, "An anticounterfeiting strategy using numeric tokens. International journal of pharmaceutical medicine", 2007.
10. John P.T. Mo, Sheng Q.Z. Li X., Zeadally S., "RFID Infrastructure Design: A Case Study of Two Australian National RFID Projects", IEEE Internet Computing, Vol 13 No 1. Jan/Feb 2009, pp.14-21.
11. Sklavos N., Zhang X., "Wireless Security & Cryptography: Specifications and Implementations", CRC-Press, A Taylor and Francis *Group,* ISBN: 084938771X, 2007
12. Lehtonen, M., F. Michahelles, and E. Fleisch, "*Probabilistic Approach for Location-Based Authentication"*. 2007.
13. Mirowski,.L, Deckard: "A System to Detect Change of RFID Tag Ownership". IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.7, July 2007, 2007.