A Method for Whole of System Analysis of RFID Security

Luke Mirowski
School of Engineering and ICT
University of Tasmania
Hobart, Australia
Email: Luke.Mirowski@utas.edu.au

Abstract

Existing methods for analysis of security in Radio Frequency Identification (RFID) systems take a relatively localized view of security. Rotter (2008) proposed a privacy and security risk assessment framework which was used to assess domain risks using three criteria. Mitrokotsa et al. (2008; 2009) structured threats into system layers, enumerating the threats as well as offering potential defenses for each layer. Since then there has been limited focus on a reference model based approach to RFID security. Therefore, work reported here addresses the existing gap in the RFID security analysis field by introducing a 'whole of system' approach to analysis, made possible by way of a reference model, consisting of the three horizontal layers suggested by previous authors: real world, RFID and strategic. But at the same time, adds vertical security partitions for such things as the problem context. This provides a structure that allows existing methods to be applied systematically and across the 'whole system'.

Keywords Trust, RFID, security.

1 Introduction

In today's world, the basic premise of Radio Frequency Identification (RFID) is that objects are marked with tags which emit serial numbers obtainable by readers using radio signals (Weinstein, 2005). Not only in the present day scenario, but for over 50 years RFID has been used to identify objects (Garfinkel and Holtzman, 2005). Some significant areas where RFID has been used are the Identification Friend or Foe (IFF) scheme for distinguishing Allied aircrafts from enemy aircraft during World War Two, the Electronic Article Surveillance (EAS), developed by Sensormatic, Checkpoint, and Knogo in the 1960's to counter the theft of merchandise and for electronic toll collection in Europe, introduced in 1980 and later in the United States.

Once a tag's serial number has been obtained, a reader retrieves information about the serial number from a database, and acts upon it accordingly. Tags fall into two general categories: active and passive. Active tags contain their own battery power, while passive tags obtain their power from the signal of a RFID reader. Passive tags are therefore, usually small and cost less than active tags. Electronic Product Code (EPC) technology, developed by the Auto-ID Center, established at MIT in 1999 and now managed by EPCglobal, was introduced as an extensible range of tag standards and is leading the widespread adoption of RFID technology into various operations (Garfinkel and Rosenberg, 2005). Importantly, the widespread adoption of RFID technology into various operations across diverse fields brings along with it a need for structured analysis of security.

Past methods for analysis of security in RFID systems take a relatively localized view of security. Rotter (2008) proposed a privacy and security risk assessment framework which was used to assess domain risks using three criteria: the system's deployment range; the link between the RFID tag and identity-related data; and the domain's security demands. Mitrokotsa et al. (2008; 2009) structured threats into system layers, enumerating the threats as well as offering potential defenses for each layer. In 2010, Mitrokotsa et al. (2010) introduced a layered security model which captures threats and solutions at layers: RFID edge hardware layer (containing tags and readers), communication layer (containing links between tags and readers) and back-end layer (contains the middleware components like databases and web servers), in addition to attribute columns for such things as cost and potential damage. Although there has been much RFID analysis focused on encryption, it seems there has been limited work on analysis from the tag through to the reader and beyond in a single model based approach.

As such, this paper addresses the existing gap in the RFID security (and revisiting earlier research) field by introducing a 'whole of system' approach to analysis, made possible by way of a reference model, consisting of the three horizontal layers suggested by previous authors: real world, RFID and strategic (Mitrokotsa et al, 2008; Mitrokotsa 2009). But at the same time, it adds vertical security partitions for such things as the problem context. This provides a structure that allows existing methods to be applied systematically and across the 'whole system'.

2 Background

This section briefly reviews approaches to security analysis in RFID which take a model based approach to representing the relationships in RFID and security. Each of the following security models introduces a means of classifying threats and solutions, and subsequently, deriving an indication of the amount or type of security to employ.

For example, Mitrokotsa et al. (2008; 2009) classified threats by system layer, and solutions were related to each threat at a layer. The physical layer comprises the physical RFID devices and these are vulnerable to physical modification by an attacker, removal of a tag from its entity, physical damage or destruction using the Kill command. Defenses to physical layer attacks can include increased physical security; enhanced attachment of tags to entities; or stronger kill passwords.

Many attacks could have influences across the layers. One is the "replay attack". An attacker may record a radio signal and reuse it at a later time in order to gain physical access to a part of the system. Similarly, tag removal, whilst depicted at the physical layer, would mean that a denial of service attack occurs at the strategic layer. Thus, localizing threats and solutions limits the capacity to represent the relationships which exist between attacks and solutions throughout the system.

Subsequently, Mitrokotsa et al. (2010) introduced a layered security model which captures threats and solutions at layers: RFID edge hardware; communication; back-end. The RFID edge hardware layer contains the tags and readers. The communication layer contains the radio link between tags and readers. The back-end layer contains the middleware components like databases and web servers.

Elements of each layer are subdivided into three security properties: confidentiality, integrity and availability.

Another characteristic of the model is that each classification has assigned values for various attributes: associated damage caused by threat; cost to implement threat; type of tags most vulnerable to threat; possible countermeasures; and associated costs. As security principles are not always confined to the layer at which an attack occurs, there is an opportunity to improve on this characteristic.

An alternative analysis approach performed using a model is the Rotter (2008) framework. It has been used to derive a classification of various domain risks using three criteria: a system's deployment range; the link between the RFID tag and identity-related data; and the domain security demands. Using these properties, various systems have been classified, and their security demands determined.

When considering the above approach to security analysis, it seems likely that many of the influential system properties are not considered when a classification is derived. This may mean that a system's security requirements may not be as effective if derived through the approach.

3 Methodology

Following the brief review of previous work, it is proposed that existing models would not facilitate the 'whole of system' approach to security analysis. As a result, some methods are examined in this section, which will offer an alternative analysis approach.

A "reference model" facilitates increased understanding of a system by modeling a system's architectural properties - usually by examining individual system elements and modeling these elements along conceptually similar system functions enables derivation of these architectures. For example, one way of modeling elements in systems, is to hide individual characteristics using layers.

There does not appear to be an established method for constructing a reference model, however, Misic and Zhao (2000) have proposed that consideration be given to a reference model's syntactic (how the model is represented in a modeling language like UML), semantic (how the model describes the domain) and pragmatic properties (the association of the model with the intended audience) in order for the model to achieve sufficient quality.

Understanding the analysis methods which could be facilitated by the reference model would be useful in order to choose which would more effectively yield useful information when used for the analysis of a specific system. To this end, the three main concepts behind the security analysis of RFID systems are: Analysis of actual RFID systems (based on their functional capabilities under standard operation); Analysis of security threats (which result in a system moving from a standard operating situation, to one where operations are invalidated by attacks); Analysis of solutions (in the context of system properties in conjunction with threats, to achieve practicable security requirements).

Therefore, one method to define what broadly constitutes a system's standard operations is "domain analysis". To determine how a system functions, usually two analysis stages are undertaken: data analysis (when a domain's basic elements are identified as entities, operations, events, or relationships) and classification (uncovering information structures which characterize classes of elements (Arango, 1994)).

As a basis for understanding how security is needed in RFID systems, it makes sense to begin by understanding what constitutes the elements of a system. One method that can be applied in a domain model approach is Object Oriented Analysis (OOA). Another approach is the "entity-relationship" modeling technique, which represents relationships in data (Pressman, 2000). This method usually results in an Entity-Relationship Diagram (ERD). Another method for a domain model is "feature construction", which enables the derivation of features from existing features in data. Several types of approaches to feature construction exist, such as Hypothesis driven methods (constructing new features based on a previously generated hypothesis or discovered rules (Alfred, 2008)), Data driven methods (construct new features by directly detecting relationships in data (Alfrid, 2008)) and knowledge driven methods (Wnek and Michalski, 1994).

Methods which can analyze the threats to RFID systems are briefly reviewed. Attack Trees are a threat modeling method proposed by Schneier (1999). Attacks are modeled from an attacker's perspective as a tree structure. In effect, this can be a recursive process until sufficient decomposition has been attained, showing attacks across the entire system.

One approach to analyzing solutions on a 'whole of system' basis is to study solutions in the context of actual systems. A method is reviewed, which may be suitable for analyzing security solutions in RFID systems on a 'whole of system' basis.

Agent Based Modeling and Simulation (ABMS) is a simulation methodology which models a system as a collection of agents and the relationships between those agents, and is considered suitable for solution analysis in RFID systems on a 'whole of system basis'. An agent executes various simple independent behaviors (Macal and North, 2005). While the individual rules of each agent could be simple, the model's agents collectively exhibit more complex behaviors than a single agent. This is called emergent behavior. Thus, highly complex systems can be modeled using relatively simple components, whilst still attaining the behavior of the 'whole system'.

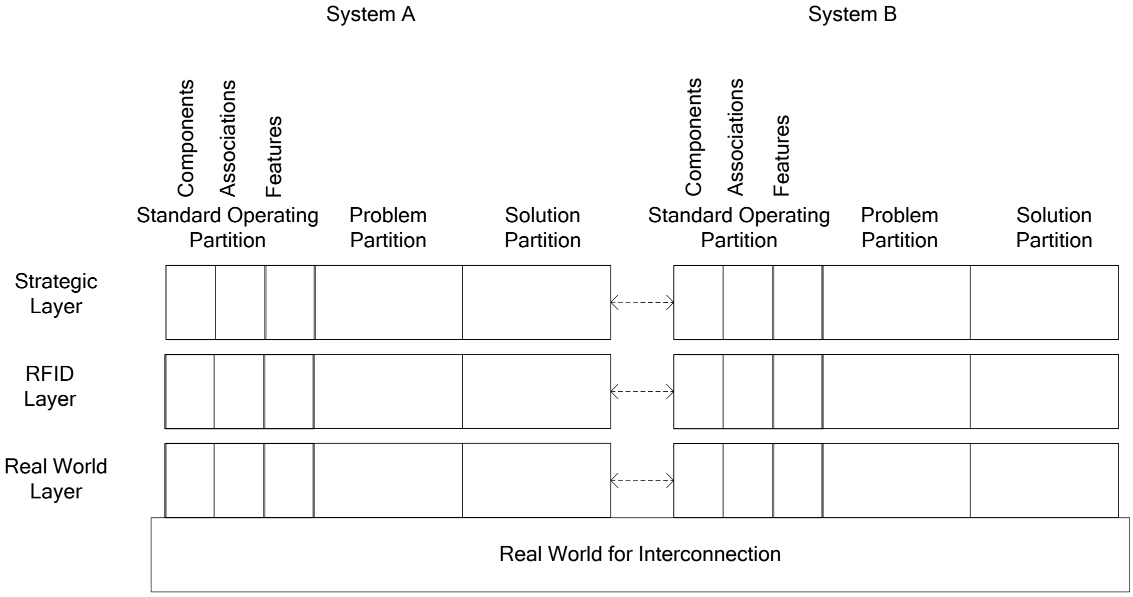

Figure. 1. *- The integrated layered and partitioned reference model (by the author)*

ABMS can be implemented more easily using toolkits (Gilbert and Bankes, 2002). An example toolkit is the Multi-Agent Simulator of Neighborhoods (MASON) (Balan et al, 2003; Luke et al, 2004), which provides some of the core elements needed for ABMS, modeling and visualization. Robinson (2004) has proposed that simulators have modes, ranging from highly accurate representations of systems for predicting outcomes in real systems (Mode One), to less formal representations, which facilitate a group of individuals through discussions which take place during the modeling process (Mode Three). A Mode Two simulator is developed for problem understanding and appears to be the most relevant method for 'whole of system' approach.

Together the above methods can be combined to produce a systematic method for analyzing systems holistically.

4 Proposed Security Model

To address apparent limitations in previous work, this section introduces and describes an alternative model which makes possible a 'whole of system' approach to the analysis of security in RFID systems. It is distinguished from previous models on the basis of integrating layer and partition properties. The layers are real world, RFID, and strategic and the partitions are standard operating, problem, and solution. The model integrates these layers and partitions using a reference model approach.

The discussion of the layers starts with the real world layer. The real world layer contains a system's local application environment (including supply chain 'custodians', 'zones' in a toll way, or 'rooms' in a building) and its characteristics. Depending on the level of abstraction needed, characteristics could be modelled using geometric concepts like those defined by a coordinate system such as the Global Positioning System (GPS).

In the proposed model, tags and readers operate at the RFID layer through radio frequency and anti-collision protocols, as does the middleware which links the RFID technology to the rest of a company's information systems. RFID technology is contained in a single layer, which downplays the influence of the technology on analysis. The strategic layer captures the information goals of the company which implements an RFID system.

Vertical partition properties capture the security concepts like standard operations, threats (or security problems), and solutions. The standard operating partition captures the intended operating principles of RFID systems. This is where the standard domain components are modeled, such as in a domain model. For example, the model proposed by Hassan and Chatterjee (2006), which has depicted different RFID components, could be inserted here as this partition is concerned with valid operations. The problem partition captures the security problems which affect RFID components which have featured in the standard operating partition. These are usually the threats. This partition is where such a threat analysis would take place and the results situated. The improvement imparted by this model, over previous work, in particular the work by Rotter (2008) and Mitrokotsa et al. (2010) is that threat analysis if done in this partition, is automatically aligned with the standard operating partition and the solution partition, as partitions are aligned with each other. Thus, the context of actual systems is taken into account during threat analysis.

Partitions can be further decomposed into minor partitions. Figure 1 depicts the standard operating partition with the inclusion of three minor partitions. These have organized the standard components to consider: the components, their associations with each other, and the information which can be gained through their interactions, as separate concepts. The three minor partitions are introduced: components, associations, and features.

At the RFID layer, a component would be a tag or reader. The association partition comprises the data view which emerges when components in the component partition interact. The feature partition represents metrics which can be constructed from the data associations between components in the previous two partitions.

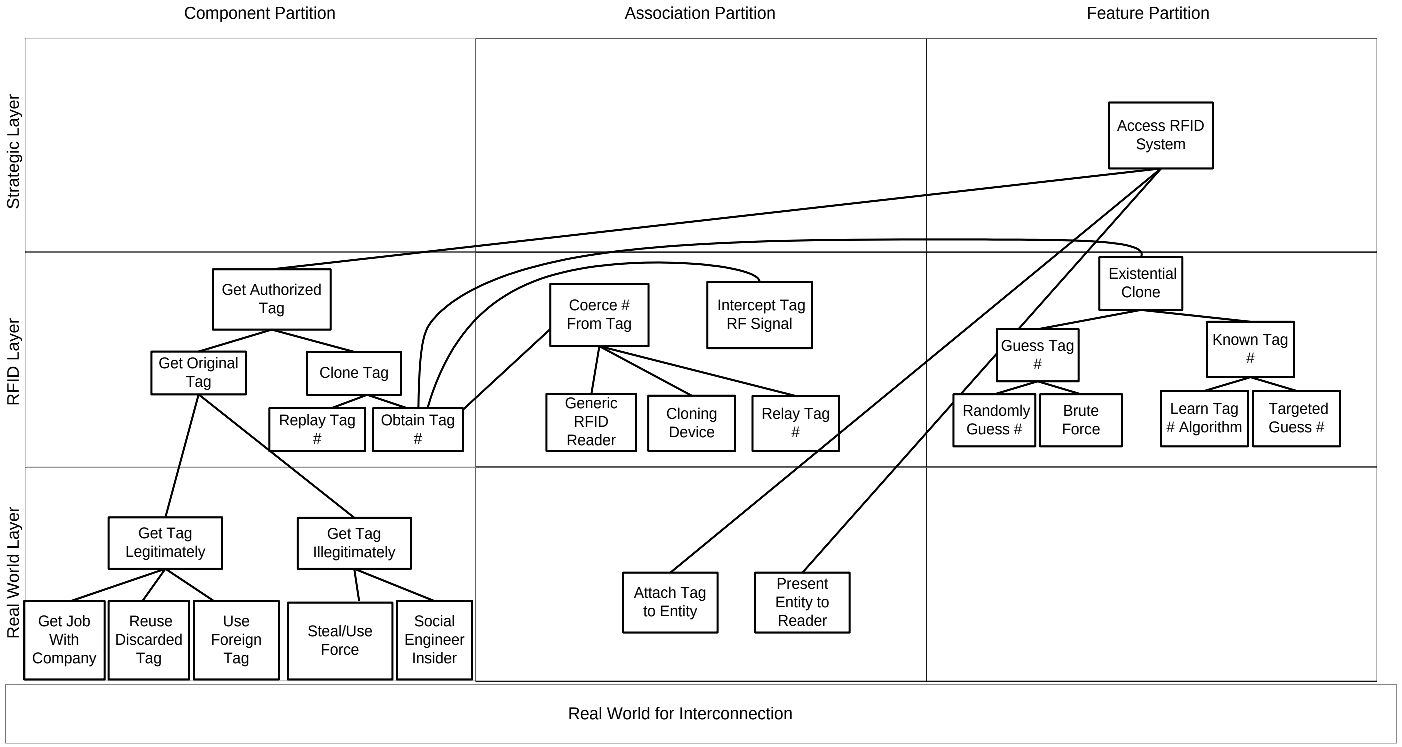

Figure. 2. – RFID authorisation system attack tree (by the author)

Partitions enable the separation of independent but related security concepts – standard operations, threats, and solutions. Through the integration of layers and partitions, it is possible to consider RFID and security concepts collectively.

5 Applying the model: pharmaceutical supply chains case study

In this section the 'whole of system' approach is applied through pharmaceutical supply chains case study. These supply chains are complex systems in which RFID is integrated across a number of locations called "custodians". RFID is used for the purpose of producing information suitable for Electronic Pedigrees which are essentially documents each containing a history of a drug's movement through a supply chain, and are used to validate the drug as authentic (or for recall purposes).

In pharmaceutical supply chains, the RFID system can be thought of as a series of smaller but interconnected RFID systems. Each subsystem is situated within a custodian's location, to act as a source of part of the information for an electronic pedigree. The reference model organizes components across the layers of the reference model and illustrates their interconnections. The pharmaceutical supply chain is modeled at the real world layer, the RFID system at the RFID layer, and the electronic pedigree at the strategic layer.

The strategic layer contains the electronic pedigree which establishes a secure chain of custody of pedigree documents shared between custodians in the pharmaceutical supply chain. This electronic pedigree uses three elements: pedigree data format (represents the physical entity's information, such as the drug, in a format which can be distributed amongst custodians), pedigree processing (authenticates an electronic pedigree document, validating the transactions of previous custodians from the document before the product arrives), and pedigree information transmission mechanisms (used to transfer data to custodians) (Inaba, 2008).

The pedigree information transmission can happen in two ways - the propagating document approach or the fragmented data approach. The propagating document approach represents pedigree data into a single document which is appended, resigned, and forwarded by each successive custodian in the supply chain. As each custodian appends and resigns the document, a new layer is added to the document, effectively, creating a link between all custodians which can be unwrapped to verify a product's point of origin whereas the fragmented data approach allows custodians to retain electronic pedigree information for a document in their own database or a third-party database, rather than propagating it down the supply chain (Inaba, 2008). Although this produces smaller pedigree documents, it increases the amount of network traffic to source pedigree information. It also means that a custodian could modify data after the product has been shipped. Effectively these belong to the strategic layer's association partition. As products may be assembled or aggregated in the real world layer, individual pedigree documents are combined into a Pedigree Business Document (Inaba, 2008).

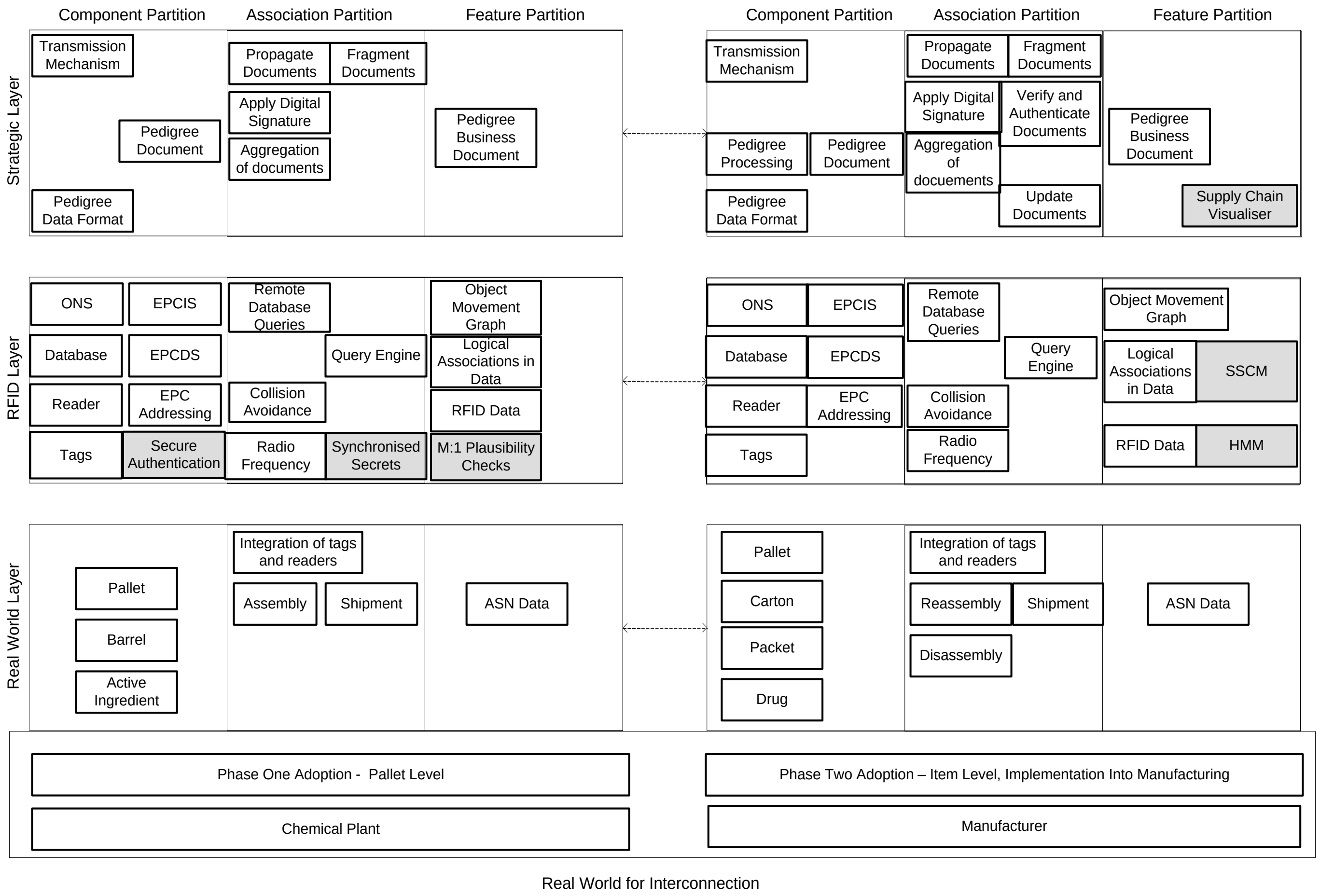

Figure. 3. *- The solution partition of pharmaceutical supply chains (by the author).*

As the Pedigree Business Document serves as a wrapper to consolidate the individual pedigree records, it is an inferred information structure, so it has been modeled in the strategic layer's feature space. These wrappers specify information unique to each pedigree document (identifier, version of format, timestamp); and information unique to the product package (drug name, manufacturer/distributor, object identifier, National Drug Code (NDC), manufacturing date, expiry date, dosage form, strength, container size, lot number, parent package object identifier). Finally, the custodian that is shipping a product, and hence, a business document as well, has to sign the document. Upon receipt of the goods and documents, the receiving custodian validates the digital signature (authentication) and after matching the received products with the pedigree document (verification), they then sign the pedigree to confirm receipt (confirmation).

The RFID layer contains the RFID system which is a source of information for electronic pedigrees. RFID data can be distributed between custodians using various infrastructures. One such infrastructure is the EPC Infrastructure, proposed by the Auto-ID Labs, and now advanced by EPCglobal as the EPC Network. The main components of the infrastructure are object name service (ONS - a multi-layered directory service – containing root and local services - which locate information about tag EPC's), EPC discovery service (EPCDS - used by trading partners, such as custodians, to store and provide access to product information), and the EPC information service (EPCIS - a directory of addresses for other EPCIS servers to locate data about an EPC). As these components are networked components, most likely accessed over the internet, custodians would associate to these using remote data-base queries to derive RFID data for their electronic pedigrees, which is why this has been modeled in the association partition of the RFID layer. The adoption of RFID within pharmaceutical supply chains determines the horizontal production of data – between custodians – and the vertical production of data – within a custodian's location (Bapat and Restivo, 2005). Modeling the RFID layer between the strategic layer and real world layer enables the interrelationships to be considered.

The real world layer contains the pharmaceutical supply chain's physical components and processes. These enable the movement of drugs between all custodians to deliver the drug all the way to the consumer. This layer is interfaced to the RFID layer by the physical tags and readers when they are associated with different physical entities in the real world layer association partition.RFID systems that operate in pharmaceutical supply chains are vulnerable to a variety of attacks. A 'whole of system' approach will now be illustrated to facilitate consideration of threats in relation to actual system elements. Different kinds of attacks (depicted by attack trees can occur on a pharmaceutical supply chain). One possible attack can be the introduction of counterfeit drugs. This has been pictorially depicted in figure 2.

The insertion of a counterfeit drug using attacks propagated through the RFID system would appear to be highly involved as RFID is deployed to varying degrees at different layers, and in different custodian locations.

In order to understand which solutions may be practicable for this system, 'whole of system' analysis made possible by the reference model is applied to the solution partition in Figure 3. In this section, continuing a 'whole of system' approach, the reference model is used to examine, how applying 'whole of system' analysis assists in identifying solutions as feasible, how the reference model exposes areas of the system which may be supportive of solutions which do not incur the penalties associated with tag based security, how a number of solutions can be implemented to achieve robust defense in this specific system context. To this end, figure 3 depicts the solution partition of pharmaceutical supply chains.

6 Conclusion

Rather than attempting to develop new methods to secure a particular RFID component, the idea employed within this work has focused on a 'whole of system' approach to the analysis of security in RFID facilitated by a reference model.

Specifically examined in this work was security of pharmaceutical supply chains and the RFID systems within them. In order to produce information which effectively creates a history of a product, RFID has to be integrated in the supply chain. This integration involves not only RFID but also real world and strategic elements. The underlying system of a supply chain was characterized by: a variety of custodian locations which had implemented RFID in different ways and to different extents; limitations on tag reading at different stages; product assembly/disassembly complicating tag reads and also which entities were monitored; and when various identifiers in the system were enabled/purged. The reference model was illustrated as capable of capturing these elements.

The main analysis outcomes, having deliberated through the model, appear to be practicable security requirements. As the system model encapsulated the elements which influenced RFID implementation, threat analysis, using attack trees, indicated that only a limited number of threats were relevant. On that basis, some solutions were suggested as effective when integrated in this context.

When the examples of previous work are considered (Rotter, 2008; and Mitrokotsa et al., 2010), which have taken a relatively localized view of security, it seems likely this alternative approach and model, 'whole of system' analysis, leads to a more effective understanding of security requirements.

References

Alfred, R., Dynamic Aggregation of Relational Attributes Based on Feature Construction Advances in Databases and Information Systems, 2008. 5207: p. 2-13.

Arango, G. A Brief Introduction To Domain Analysis. in ACM Symposium on Applied Computing. 1994.

Balan, G. C., C. Cioffi-Revilla, S. Luke, L. Panait and S. Paus. MASON: A Java Multi-Agent Simulation Library. in Conference on Challenges in Social Simulation. 2003.

Bapat, V. and G. Restivo, Reaping The Long-Term Benefits Of Integrating Radio Frequency Identification (RFID) Into Pharmaceutical Manufacturing. Pharmaceutical Engineering, 2005(3): p. 32-44.

Garfinkel, S. and B. Rosenberg, RFID: Applications, Security, and Privacy. 2005: Addison Wesley.

Garfinkel, S. and H. Holtzman, Understanding RFID Technology, in RFID: Applications, Security, and Privacy, S. Garfinkel and B. Rosenberg, Editors. 2005, Addison Wesley. p. 15-36.

Gilbert, N. and S. Bankes, Platforms And Methods For Agent-Based Modeling. Proceedings of the National Academy of Science of the United States of America, 2002. 99(3): p. 7197-7198.

Hassan, T. and S. Chatterjee. A Taxonomy For RFID. in 39th Hawaii International Confer-ence on Systems Sciences. 2006.

Inaba, T., EPC System For A Safe And Secure Supply Chain And How It Is Applied, in Net-worked RFID Systems and Lightweight Cryptography, P.H. Cole and D.C. Ranasinghe, Editors. 2008, Springer. p. 191-210.

Luke, S., C. Cioffi-Revilla, L. Panait and K. Sullivan. MASON: A New Multi-Agent Simula-tion Toolkit. in Eighth Annual Swarm User/Research Conference. 2004.

Macal, C.M. and M.J. North. Tutorial On Agent-Based Modeling And Simulation. in Winter Simulation Conference. 2005.

Mišic, V.B. and J.L. Zhao. Evaluating The Quality Of Reference Models. in 19th Interna-tional Conference on Conceptual Modeling 2000.

Mitrokotsa, A., M. Beye, and P. Peris-Lopez, Threats to Networked RFID Systems, in Unique Radio Innovation for the 21st Century: Building Scalable and Global RFID Net-works, D. Ranasinghe, M. Sheng, and S. Zeadally, Editors. 2010, Springer-Verlag. p. 39-63.

Mitrokotsa, A., M. Rieback, and A. Tanenbaum, Classifying RFID Attacks and Defenses. Information System Frontiers, 2009. 12(5): p. 491-505.

Mitrokotsa, A., M. Rieback, and A. Tanenbaum. Classification Of RFID Attacks. in 2nd In-ternational Workshop on RFID Technology. 2008.

Pressman, R.S., Software Engineering: A Practitioner's Approach. 1st ed. 2000: McGraw Hill.

Robinson, S., Simulation: The Practice of Model Development and Use. 2004: Wiley.

Rotter, P., A Framework For Assessing RFID System Security And Privacy Risks. IEEE Pervasive Computing, 2008. 7(2): p. 70-77.

Schneier, B. Attack Trees. 1999; Available from: http://www.schneier.com/paper-attacktrees-ddj-ft.html.

Weinstein, R., RFID: A Technical Overview And Its Application To The Enterprise. IEEE Computer Society, 2005. 7(3): p. 27-33.

Wnek, J. and R.S. Michalski, Hypothesis-Driven Constructive Induction In AQ17-HCI: A Method And Experiments Machine Learning, 1994. 14(2): p. 139-168.

Copyright

The following copyright paragraph must be appended to the paper. Author names MUST not be included until after reviewing. Please ensure the hyperlink remains for electronic harvesting of copyright restrictions.