Applying RFID to Secure the Pharmaceutical Supply Chain

Brian King
Indiana University Purdue University Indianapolis
e-mail : briaking@gmail.com

Xiaolan Zhang
University of Illinois
e-mail : zhang_xiaolan@ieee.org

Abstract

In [5], a protocol was described how to apply RFID to currency to provide integrity (e.g. reduce counterfeiting) while simultaneously supporting privacy. Here discuss how RFID can be applied to increase integrity and confidence in the pharmaceutical supply chain. A secured pharmaceutical supply chain will increase integrity, improve consumer confidence, and aid regulators in tracking pharmaceutical products, thus producing a "pharmaceutical drug pedigree". At the same time privacy will need to be preserved. We provide an analysis of the pharmaceutical supply chain, and propose a security model for the system.

1. Introduction

Pharmaceutical products are among the most expensive retail merchandise due to the complexity and cost of its development and manufacturing. The price gap between manufacturers, due to various standards, provides considerable incentive for drug traffickers and forgers to gain a significant profit. According to [1], pharmaceutical products from Canada can be manufactured at a lower price than those made from the U.S. [1] Thus, pharmaceutical products have become a very attractive candidate for counterfeiting and/or smuggling. Consequently manufacturers are interested in mechanisms for identifying counterfeiting and government is interested in mechanisms that help determine smuggling. The counterfeiting problem has become widespread internationally and has increased in magnitude according to the research by Robin Koh et al. [2]. In addition, since pharmaceutical products are consumed by humans, any mistake during manufacturing may cause serious harm to people's health and even lead to death. The importance of drug authenticity is obvious. In the United States, Food and Drug Administration (FDA) has been considering the use of RFID tags to prevent counterfeit pharmaceutical products [3]. Since the manufacturing of pharmaceutical products can be done in a more cost-effective manner in other countries, for example Canada. The U.S. has been reluctant to allow the import of such products due to inability to provide a complete pedigree of the product. Thus any mechanism that can provide the integrity of a products' pedigree could alone provide the means for increasing imports of generic alternatives and alleviating consumer's concerns for the integrity of the product.

Besides its use for anti-counterfeiting, automatic identification also has received significant attention from manufacturers, distributors and retailers. A pharmaceutical product may go through complex manufacture process that involves several transitions, through several locations. At each location, the product (or soon to be product) should be registered to monitor and control the flow of manufacture. Traditionally, registration is done manually. RFID technology can automate the identification of products in a much shorter time and

[1] The pricing of pharmaceutical products is complex due to many factors including development, research, liability, ect. ...).

higher level of accuracy. It is also true that distributors and retailers need to ship and inventory products in large quantities. Thus, automatic identification within manufacturing would improve the process. At the same time, the consumer of pharmaceutical products would have more efficient management of the medicines they take or they are responsible for. In a hospital setting nurses want to provide patients the correct medicine in a punctual manner. At home, some patients may want their medicine chest to be smart enough to identify drugs' status. With the aid of remote identification equipment, they will be able to monitor validation and compliancy, the goals are very promising.

The focal point of our work is that information concerning the pharmaceutical product should flow with the product as the product moves through the supply chain and consumer environment. Further, this information needs to be freely available to those that require it. In addition this information needs to possess a high-level of integrity concerning its accuracy, and should only be able to be modified by authorized parties. Lastly, this flow of information needs to be conducted in a manner that the privacy of all parties should be preserved and that the information should be provided to only those parties who are authorized for it. That is, any information that a consumer possesses, drugs/medication can lead to discrimination. Consequently such information cannot be transmitted in public. If we use an RF signal to transmit information concerning pharmaceutical information then we must "hide it". The solution is to encrypt this information. However observe that static ciphertext can reveal consumer, that is if a time t1 a party recognizes a static ciphertext from a previous transmission that occurred at time t0 then they know that the one of the parties at time t0 is present at time t1. In this work we suggest the use of active RFID technology to provide access to this information concerning the pharmaceutical products. We suggest the use of cryptographic protocols to ensure the integrity of the information. Today's RFID tags are not manufactured to provide the necessary memory space, but suitable modification would ensure its use in our outlined protocol.

2. An Analysis of the Pharmaceutical Supply Chain

The life cycle of a drug[2] is such that the drug needs to travel through a pharmaceutical supply chain, as well as a "consuming chain". The manufacturer, distributor, warehouse, pharmacy and consumer are members of the supply chain. Later, the consumer and recycle center consists of the consuming chain. Furthermore, how the drug is manufactured, distributed, consumed and disposed may need to be monitored and in some cases investigated by law enforcement agencies.

Like many retailing applications, identification is a basic function that needs to be provided in a pharmaceutical supply chain. The integrity of the tag data is important to provide anti-counterfeiting. In post-sale applications, confidentiality is as important as other functions to provide privacy protection for patients.

2.1 Requirements in the drug supply chain

1. ***Anti-adulteration***. Some drugs have a very high market value, which attracts adulteration crimes, like mislabeling, dilution, misbranding, counterfeit, etc. RFID tag must make adulteration impossible, or at least much more difficult.

[2] For simplicity, the word "drug" is used to represent pharmaceutical products or medicine.

2. ***Auto-ID inventory*** By using RFID technology, a drug can be automatically marked and inventoried at any part of manufacturing line, or during its transportation. It saves labor by passing the traditional bar code scanning and speeds up inventory. It provides a real-time inventory monitor within the manufacturing location, warehouse, and retail store. It could possibly lead to the use of "smart medicine chest" which will automatically record stored drug, check or remind the use of drug, sort out expired drug, etc. For example, in clinics, tagged drugs will reduce mistakes when nurses try to find the correct medicine, correct dose and time for each patient. It also helps during the recycling procedure. When a drug is discarded, information stored in RFID tag will expedite the garbage classification.
3. ***Traceability***. Because drug may be illicitly distributed like trafficking, a complete history (origination, transportation, distribution, usage and disposal) of a drug may be useful for tracing within a crime investigation. Each drug should have a reliable history record for lawful tracing.
4. ***Accountability.*** After a drug is manufactured, some initial information concerning the drug should be written by the manufacturer. The data on the tag, label and elsewhere, is essential to identify the drug so they are not altered during the life of the drug. But more information may need to be added to a drug, like location, when it is transported and traded during the lifetime of the drug. This information can be used to trace and authenticate a drug so any modification of the data needs to be accountable to maintain a reliable record for each drug.
5. ***Privacy protection***. Drugs reveal the health status of a person. Disclosing what drugs a person takes may cause problems like discrimination, isolation, or theft. When we exploit the convenience of tagged drugs, privacy protection should be taken into account at the same time. The RF signal from a tagged drug should be indistinguishable from other drugs or even other tagged times. Only an authorized party should be able to determine the identity of a drug through the RF contact. Some relative information of a drug may also need to be protected due to commercial privacy. Usually manufacturers do not want others to know inside products and processes that they employ.
6. ***Compliance detection***. The proper compliance of some drugs is very important. Law enforcement or other responsible party may want to know whether a consumer has complied with the policy of usage or disposal. RFID tags may be required to identify such misconduct or crimes.

2.2 Public Pedigree Enhances Authentication

Many people worry about the authenticity of origin for pharmaceutical products. Because different countries require different market regulations, drugs from some areas may be more trusted than others. If a drug has a pedigree (authenticated history record of all the pre-sale custodians), it provides more information to a consumer where it comes from and how it is distributed. Such information helps a consumer to identify possible counterfeit or illegal drugs. According to [9], a pedigree increases cargo security and visibility for drug import control at customs and facilitates the precise distribution of them. We know that some enterprises may not want to pub- lish the supply chain because they are afraid that this information may be revealed to their competitors. Such competitors may use it for marketing

investigation and commercial spying. However, if every member in the pharmaceutical industry publish their pedigrees, then the advantages will be mutually realized. There will be a new platform for fair competition. Furthermore, pharmaceutical products are a public health concern so they should be more regulated than other commodities. The safety of consumers is more important than industrial privacy. On the other hand, the probability to identify a drug based on this supply chain is rather low considering the number of products the same manufacturer produces. Therefore, we think the pedigree should be public. There are two ways to implement a pedigree. SupplyScape Corporation [9] uses a database to register the history for each drug. All distributors need to access the database to retrieve the information. This solution has scalability limitations as the amount of drugs and participating parties increase. If the electronic pedigree becomes a standard that is adopted by many companies, who will be trusted to maintain the database? Who will be responsible for the expense of database? If the government runs the database, people will worry about the government acting as Big Brother. If only a few companies provide such service, they can monopolize the market, which will harm the other manufacturers and the interest of consumers. Another solution is an RFID on-tag pedigree. RFID tags provide instant access to pedigree without network infrastructure and central database. Considering the advantages of tags on multiple party access and distributed administration, it may be more suitable to maintain a pedigree using an RFID tag.

2.3 Parties within the pharmaceutical supply chain

We now examine the potential parties in a pharmaceutical supply chain/consumer chain, and the roles that they play. There are six parties involved in a drug's "life cycle". We now discuss the Six-Party Trust Model, their responsibilities, limitations and requirements in detail.

Law enforcement agency (LE): They monitor the manufacture, delivery, transaction, use and disposal of drugs regulated by law. They may need to be able to remotely collect data (name, serial number, originality, ingredient, history, etc.) of subpoenaed drugs to identify the owner or transactions. They may also inspect inventory or transaction records directly from custodians (factory, warehouse, laboratory, pharmacy, recycle center, etc.). But they cannot modify the data of a drug.

Manufacture system: Registered entities that involve in manufacture procedures of drugs. *Manufacturer (MA)* An entity within the manufacturing system, they produce, label, and package drugs. They produce secure traceable and counterfeit resistant drugs. They will also keep a manufacture record for each drug. In most cases, they will determine the supply chain (routing) and verify that each drug is delivered to the right pharmacy. They will get feedbacks from downstream parties. They initialize drug data which cannot be overwritten. *Internal distribution channel (ID):* An entity within the manufacturing system, they store, and sell drugs (semi-finished drugs). They will trace internal transitions between different locations and automatically inventory each drugs. They can append data about their transactions but cannot change existent data.

External distributor (ED): Registered merchants or firms (wholesaler, warehouse, etc.) that deliver products from manufacture system to pharmacies. They purchase, store, re-label, repackage, wholesale drugs. They want to identify and report counterfeit drugs. They check the supply chain history for each drug. They will automatically inventory and record transactions for drugs. If a drug has a pre-determined channel, they will verify the history and

confirm their ownership. They can change the distribution channel but such change should be accountable.

Pharmacy (PA): Registered retailers or dispensers that sell drugs to end consumers. They verify the history of drugs and identify counterfeit drugs. They will monitor store inventory in real-time and keep sales record. A medical clinic is also a form of PA in this sense. They will dispense drugs to patients. RFID technology will help them serve patient efficient but they should be responsible for customer privacy protection.

Consumer (CM): Registered individuals or entities that consume drug without reselling them. It includes ultimate customer (patient), research subject and those upper stream parties who discard some drug instead of selling them. They purchase, store, use, and dispose drugs. They will check drugs' history and identify counterfeit drugs. They should comply with policies of use and properly dispose certain drugs if necessary, they need to record their compliancy for lawful inspection. They may send feedback to manufacturers. But they don't want others to know what drugs they take. They cannot make any change to existing drug data, however they can append their personal information to this data. Compliancy is ideally recorded by the drug automatically and no manual change is allowed.

Recycle center (RC): Registered entities that classify and dispose drugs (or containers) properly. The private information should be completely removed but the identity of drug should be kept before dispose. They can record drug data (no private information) in their own database but they are not allowed to change or append data.

The pharmaceutical supply chain is modeled as a downward flowing trust chain. We assume that custodians downstream need to know the upper stream information of a drug via RFID tag. For example where the drug is made and where it comes from, in order to authenticate drugs. However, the upper stream custodians do not necessarily need to know the downstream information via RFID access. Most probably the supply chain has been initially planned as the drug is shipped. In the downward flow trust model, the upper stream entities provide their information via RFID tag to downstream custodians but downstream entities do not need to do so. When a drug goes to a new owner, the previous one may not have access to some of the RF data of the drug even though the current owner is able to. The preceding owner relays its “drug access trust” to the new owner via the pharmaceutical supply chain. However, there are exceptions. A recycle center should not know who the consumer of a drug is. Law enforcement is granted absolute trust when a drug or an entity is subpoenaed. Figure 1 demonstrates the relationship of trust between parties.

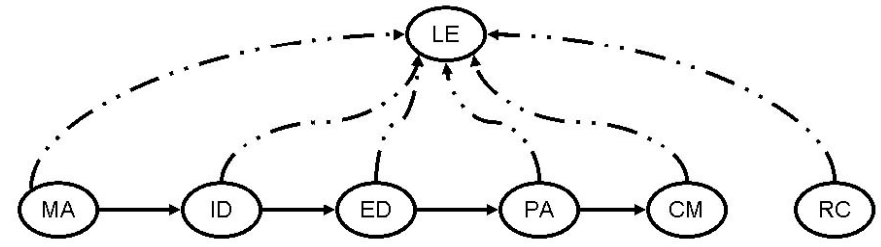


Figure 1

2.4 Over-The-Counter (OTC) vs. Prescription (PS) Drugs

The security environment differs significantly between over-the-counter (OTC) and prescription (PS) drugs. When drugs are shelved in a pharmacy store, every customer in the store is able to access OTC drugs but PS drugs are only reachable to the pharmacists. The probability of attacks on OTC drugs may be more significant than on PS. We do not necessarily differentiate OTC drugs and PS drugs in our discussion. Our goal is to secure both OTC drugs and PC drugs. But in practice the best approach maybe to develop two schemes one for OTC drugs and the other for PS drugs.

2.5 Lawful Tracing

Law enforcement is not interested in tracing individual consumers or recycling centers except in the case of controlled substances. If the drug is a controlled substance, the law enforcement may want to reserve the right for post-sale tracing. Usually, lawful inspection of individuals occurs at ports or security screens. Therefore, we do not view that lawful tracing of pharmaceutical products should be available when needed. Also observe that any law enforcement agency who wants to access drug information, optically or remotely, must be provided based on legal authority or a legal process completed. e.g. For example, the drugs of a party for which a legal warrant has been obtained should be investigated and tracked by law enforcement. Further governments may provide custom officers the authority to obtain such information at borders and ports of transit. Lastly, law enforcement may wish to trace products while in the supply chain.

3. Security Requirements

In this section we formalize the necessary security requirements needed for a pharmaceutical supply chain. First since the supply chain includes consumers, privacy will need to be supported. Secondly, it is extremely important that information and product is described in a valid matter. Consequently, a high-level of integrity is required.

3.1 Privacy Requirements

Important security requirements that are required include: privacy of communications, privacy of parties carrying the tagged items (privacy of bearers), and integrity of information. A formal model evaluating RFID security protocols was proposed in [6]. We will apply the model of indistinguishability of tag identity (INDI), indistinguishability of tag bearers (INDB) and perfect integrity of tag data (PID) within our security requirements. Here we provide a brief description of these models. For a complete discussion we refer the reader to [6].

Tag is the device, when queried it provides information about the item associated with it in form of remote signals. Identity is the remote identity for which the queried tag responds with. Reader is a device that receives some/none/all information transmitted from a tag. When a reader queries a tag, the information revealed is the identity but not the item. Authorized party is a group of people or organizations that are granted certain permissions to access the identity of an item from its tag. Since any individual in a party accesses a tag through a reader, the reader represents and implements the authorization of its user. For integrity, some data can only be modified by authorized parties, and parties authorized for some tags should be able to recognize the authenticity of this data. Channel is the source that a tag uses to send information. There are two information channels: public, secret. The two channels are designed to deliver data such that when both channels of information are collected by an authorized party, it provides the desired authenticated identity. The information that the

channels provide will vary depending which group (authorized or unauthorized) the reader belongs to. Informally, we characterize this as a "view'" of signals. Given the same channel of the tag at the same time, readers in different authorized groups may have different views of it. Consider the case where the data transmitted has been encrypted on the tag and suppose all authorized parties are provided the decryption key to this secret channel. Then, given the secret channel, an unauthorized reader will receive "no" information from the secret channel because they don't have the decryption key, but an authorized party can decrypt and view the plaintext from this signal.

Terminology is defined as follows.

I is a random variable of the identity of a tagged item. Φ is a random variable of the information received from an access to the tagged item. **I** is the set of all possible tagged items. η( )is a set representing the history information of a party. $\mathbf{AR}_i$ is the set of parties authorized to obtain the true identity of item $i \in \mathbf{I}$. $\mathbf{AW}_i$ is the set of parties authorized to modify some data of tagged item *i*. *O* is a random variable as the bearer of item *i*. **O** is a set of all bearers or owners. T_i is tag data of item i. $\mathbf{T}_i$ is the set of all possible tag data T_i. B_i is an operation on tag data T_i. $\mathbf{B}_i$ is set of operations on a tag data B_i. **AUTH** is set of all authenticated tag data. **Θ** is a random variable of the information received from an access to the tagged item. It is a tuple of information from three channels < U, V,W >. U is the variable representing the remote information received from a public channel. V represents remote information received from a secret channel. The environment channel W is usually omitted if it is not explicitly discussed. $\tau_{ta}( )$ is a tag's access limitation. τ_{ts} is a tag's resource: $\tau_{ts} = <P_T, C_T, M_T>$, where P_T is the physical condition ('0' means that it is physically unremoveable from the host item. '1' means removeable), C_T is the computational power limitation (number of gates), and M_T the memory limitation (number of bits). We define $\tau_r( )$ as the reader's access limitation.

Define ɣ be the maximal adversary advantage that an unauthorized party may obtain to identify a tag correctly. Here ɣ is a probability and κ is the size boundary of history for an adversary.

Definition [***(ɣ, κ)RFID INDI***] *An RFID protocol satisfies κ INDI provided that: whenever its access history η(α) satisfies that |η(α)| ≤ κ, an unauthorized party α of item i or any item i′ (i′ can be the same as i) cannot distinguish item i from i′*

$$\forall i' \in \mathbf{I}, Pr(I=i' \mid \Theta=\theta, \eta(\alpha), \tau_r(\alpha) \le \tau_{ta}(\alpha), \tau_{ts}, \alpha \notin \mathbf{AR}_i \cup \mathbf{AR}_{i'}) \le Pr(I=i' \mid \eta(\alpha), \alpha \notin \mathbf{AR}_i \cup \mathbf{AR}_{i'}) + \gamma.$$

Here $\theta = <u,v>$ is the RF signals transmitted.

Definition *[(ɣ, κ)RFID INDB] An RFID protocol satisfies κ INDB provided that: an unauthorized party of item i or any item i′ (i′ can be the same as i) cannot distinguish the bearers o of i from o′ of i′ with κ -history provided that whenever its access history η(α) satisfies that |η(α)| ≤ κ:*

$$\forall i' \in \mathbf{I}, Pr(\mathbf{O} = o' \mid \Theta=\theta, \eta(\alpha), \tau_r(\alpha) \le \tau_{ta}(\alpha), \tau_{ts}, \alpha \notin \mathbf{AR}_i \cup \mathbf{AR}_{i'}) \le \backslash Pr(\mathbf{O} = o' \mid \eta(\alpha), \alpha \notin \mathbf{AR}_i \cup \mathbf{AR}_{i'}) + \gamma.$$

Here $\theta = <u,v>$ is the RF signals transmitted.

We would suggest that the individual implementer choose appropriate γ and κ (these are their security parameters) in order to meet their security needs. We use these models in the following ways, in order to satisfy privacy of tag, a protocol needs to satisfy (γ,κ)RFID INDI,

in order to satisfy privacy of bearers, a protocol needs to satisfy (γ,κ)RFID INDB and the integrity requirements would requires the protocol to satisfy Perfect Integrity of tag Data (PID) (see the following section). These models represent security credentials that should be satisfied, parameters γ and κ need to be selected appropriately. Ideally γ should be zero, but in practice it will be a small percentage, κ is a positive integer. The larger κ is set, the more restrictive the model, in that the model requires a protocol to protect against a stronger adversary.

3.2 Formal Integrity Model

Tags used today are typically read-only but many advanced tags have already have write capabilities. We should consider the integrity when a protocol requires modifications. A modification on the tag is on the tag data. Tag data is the raw format of information stored at the physical tag memory. We should distinguish tag data from the identity and the channel. Identity is the item/data that the tag will responds with when it is queried. Channels provide the means for the communication. But tag data is the binary data stored in the tag memory cells.

In this section, we describe a mathematical model for integrity that was first introduced in [6]. The integrity model proposed in this section is quite restrictive compared with the typical security requirements for the resource limited RFID tags. Although RFID tags are low cost, it can still provide high integrity, for example this is the level of integrity that will be needed in anti-counterfeit applications. Before we set up the model, we formally define some terms used within our model.

Any protocol that modifies the data within the tag should be performed in an authorized manner by a modification function. It is a function that whenever is utilized guarantees that the data that maintains the integrity. Modification is a function that uses three inputs: current tag data, operation and authorization. Tag data is the data in tag before the modification. Operation defines how the tag data to be modified into a new one. Authorization is the authorized group the party belongs to.

Definition *The modification function f_m is defined as a mapping satisfying* f_m: $\boldsymbol{T}_i \times \boldsymbol{B}_i \times \boldsymbol{AR}_i \rightarrow \boldsymbol{T}_i$.

If the input data and authorization are valid for the requested operation, then the tag data can be modified in prescribed way. If it is not, then the modification function does not allow any change. Note that authorization here is whether a party has the write permission on this tag.

A tag may experience during the course of its life many modifications. We denote $M_i = <m_1, m_2, \ldots, m_n>$ as the sequence of modification history states of T_i. m_x is the state before the xth modification. A state $m_x=(t_x, b_x, \alpha_x)$ reflects the three inputs of the modification function where $t_x \in \mathbf{T}_i$ and $b_x \in \mathbf{B}_i$, and α_x is the party attempting to modify the tag. Modifying tag results in a transfer from the current tag state to the next one. One should interpret that modifying a tag by using the modification function is a valid modification and it will not lose integrity. Any physical modification of the tag, which is not supported by the modification function is interpreted as unauthentic, and characterize the tag as "dirty". But we allow operations that clean dirty tags, much like an accountant can rectify an arithmetic error in the books. Informally, a tag is authentic given that: there exists a sequence of states (tag data, operation and part authorization) starting from an authentic original state, such that the modification function, successively applied, results in an "clean" state.

Definition *[Authentic tag information] Given tag data T of modification history M_T, T is authentic if there exists a subsequence $<m_{x1},m_{x2},...,m_{xL}> \in M_i$ where $1 \leq x_1 < ... < x_L = n$, $f\_m(m_{xj})=t_{xj+1}$ is true. If this is true we say $T \in \boldsymbol{AUTH}$.*

We restrict our definition of integrity to whether the protocol supports that an authorized party α of a tagged item *i* will be able to distinguish an authentic tag given correct remote signals θ=<u, v>.

Definition *[Perfect integrity of tag information (PID)] A protocol that satisfies perfect integrity of tag information provided that:*

(i) an authorized party α is able to recognize an authentic tag,

$$Pr(\text{party } \alpha \text{ recognizes } T \text{ as authentic}\} \mid \boldsymbol{\Theta}=\theta, T \in \boldsymbol{AUTH}, \alpha \in \boldsymbol{AR}_T) = 1$$

(ii) an authorized party α is able to recognize a fake tag,

$$Pr(\text{party } \alpha \text{ recognizes } T \text{ as authentic}\} \mid \boldsymbol{\Theta}=\theta, T \notin \boldsymbol{AUTH}, \alpha \in \boldsymbol{AR}_T) = 0$$

The precise definition of what it means for a party to recognize a tag is authentic is dependent on the protocol. Our motivation for providing this definition is so that it can be applied to evaluate whether a protocol provides a suitable level of integrity. To evaluate a protocol, we will first model its modification function, this function is implicitly defined by the protocol. Since an RFID computing system may be a multi-party system where each party is provided some information, integrity must be evaluated from each party's view.

4. A protocol we use to ensure integrity while preserving privacy

In [7],[8] we introduced an anti-counterfeiting protocol that was used primarily to protect the integrity of currency. This protocol was developed by improving the integrity features of the protocol described in [5]. We apply it to pharmaceutical products. We assume that each pharmaceutical product will have a unique serial number S associated with the pharmaceutical product, of course there will be other information I associated with each drug. As the drug moves through the supply chain modification one would need to make changes to the information I. This modification would be limited to append only, and any modification would need to be signed, and the signing party would need to be identified. We denote that information that is written to the tag by the manufacturer by I0. Thus at different times the information available on the tag I is such that $I0 \subseteq I$. In this work we limit the discussion to the case that no other information besides the initial information I0 is written to the tag. In future work we describe the complete protocol of how third parties writing information to the tag, so that perfect integrity is still preserved.

We assume that law enforcement agencies L needs to periodically monitor pharmaceutical products as they flow through the supply chain as well as in the consumer environment. Information S and I needs to be provided to L. This information is signed by the manufacturer $\Sigma=Sig(SK_{MA}, [S \parallel I_0])$ where SK_{MA} is the signing key of the manufacturer. Observe that there exists only a small number of valid drug manufacturers. Law enforcement may wish to access S and I, further in order to determine that this information is valid, law enforcement needs Σ. This will be transmitted over the RF channel, but if transmitted as cleartext this would violate privacy. Then it is encrypted with the public-key of law enforcement. However if we encrypt S, I , Σ, then this would form a static ciphertext and could violate consumer's privacy. Thus, as recommended in [5], we use a random factor r and encrypt S, I, Σ and r, this is denoted by $C=Enc(PK_L , [\Sigma|S|I], r)$, where PK_L is the public-key of law enforcement. As the pharmaceutical product travels though the supply chain and consumer environment the

ciphertext can be refreshed by selecting a new r and re-encrypting it. (This process is described later).

Our protocol will need to provide a cryptographic link between the serial number printed on the pharmaceutical product and its RF ciphertext. We assume that the adversary is not be able to remove/replace, clone, tamper or block a tag. The tool we developed creates a cryptographic binding between the RF signal and the Serial Number (optical key). This provides a way for the law enforcement to verify the serial number remotely. In order to protect privacy we use re-encryption where the static signature that is available to law-enforcement L (encrypted with law-enforcement's public key) is re-encrypted by parties who encounter the drug via the supply chain or by consumers who wish to protect privacy.

Cell γ and δ, as described in [5] are used. In [5], one cell (γ) is write protected and the other cell (δ) is read/write protected. Both of the cells are protected by the same key (D=h(Σ)), where h is a collision-free hash value computed from the digital signature Σ. We utilize optical information in a similar manner as how it is used in [5]. We place S, I_0 and Σ optically on the tagged pharmaceutical product. Thus if one has physical possession, the can compute the read/write protected key D=h(Σ). Using the organization we created in [7], [8] we add three more memory cells. One is a no-access internal memory. It stores the authentic value or its hashed format. After it is manufactured, the hash of the serial number is stored by the manufacturer and is not allowed to be modified. The second memory cell is an RF keyed-write-only memory. It stores a mask value that is used to mask the authentic value to protect the privacy of pharmaceutical product bearers. The third memory cell is an RF read-only memory. The value is computed by the internal hardware to be the exclusive-or of the authentic value and mask value. Only the third cell is remotely accessible. Our design allows law enforcement to verify the serial number obtained remotely through the verification value stored in the third cell. But additional memory cells will not provide any information to an unauthorized party to remotely track pharmaceutical products nor the bearers. This cryptographic binding enhances the integrity but does not reduce privacy. And the tag does not need to perform any expensive cryptographic computing although a slight increase in RF memory is needed. The RFID data on a pharmaceutical product is illustrated in Table 1. The added memory cells are:

ω no RF read or write internal memory. It is set by the manufacturer. This non RF memory can be accessed only by internal circuitry and is never modified. The hash value of serial number h(S) is permanently encoded inside.

ϕ *RFID write and compare only (no read) memory cell under key D.* It stores the hash value of encryption factor h(r).

ε RF read (non-keyed read). This contains the verification value V which is the XOR of cells ω and ϕ.

The RFID data is illustrated in Table 1

Table 1: Organization of Data associated with drug

Internal		
Hash of Serial Number	$h(S)$	
Optical		
Serial Number	S	
Manufacturer Information	I_0	
Signatures	$\Sigma=\boldsymbol{Sig}(SK_{MA}, [S \| I_0])$	
RFID Tag		
Ciphertext	$C=\boldsymbol{Enc}(PK_L, [\Sigma\|S\|I], r)$	Cell ɣ: r**w**
Encryption factor	R	Cell δ: **rw**
Hash of Encryption factor	W	Cell ϕ: **w**c
Exclusive-or[b]	$h(S) \oplus W$	Cell ε: r
Hash of serial number	$h(S)$	Cell ω:r**w**

There are five kinds of access control for each memory cell: Normal read r, keyed read **r**, normal write w, keyed write **w**, compare c. Access Key is D=h(Σ).

[b] this value is not ``stored in memory", merely computed from cells ϕ and ω

The tag will respond with $V = h(S) \oplus W$ whenever a reader requests ε, here W is the value stored in cell ϕ. $h(S)$ is pre-computed and stored in memory cell ω during manufacturing. After a tag for a pharmaceutical product is created, the data in ω is neither RF readable nor writable. W will be recomputed and refreshed whenever a new r is selected during the re-encryption. Whenever **L** decrypts the ciphertext of a pharmaceutical product successfully, both its serial number S_i and encryption factor r_i will be hashed and exclusive-ored to compare with the verification value V_i in cell ε. Since nobody is able to forge $h(S)$ without damaging the tag, the verification value is computed from the genuine serial number printed on the tag of the pharmaceutical product. At the same time, the integrity of cell ϕ is ensured by the use of a "compare operation". The motivation is as follows. We cannot allow cell ϕ to have read access, otherwise all would be able to trace the tag using the static value $h(S)$, by combining cells ϕ and ε. Thus ϕ does not have read access, but **L** needs to be assured that the value W which is placed in cell ϕ is really $h(r)$. The reasoning is that there exists an attack. Suppose an adversary inserts W into cell ϕ such that $W \neq h(r)$ then when law enforcement queries cell ε what is returned will not be $h(r) \oplus h(S)$.

For example, suppose a malicious party places $W=h(r) \oplus h(S_i) \oplus h(S_{i'})$ into cell ϕ. Then the verification value would be $V_i=h(r) \oplus h(S_{i'})$. Thus this party could use $C=\boldsymbol{Enc}(PK_L, [\Sigma'|S'|I], r)$ and law enforcement would be unable to detect it. The compare function for cell ϕ is important so that law enforcement can check if W in cell ϕ equals $h(r)$, where r is decrypted from the ciphertext C. Any inconsistency to the verification value in ε or ϕ indicates that the ciphertext of the pharmaceutical product has been tampered. Further cell ε ensures privacy to the pharmaceutical product bearer since r is refreshed after every transaction and $h(r)$ is also refreshed. In addition, since r is random and h is a cryptographic hash function, $h(r)$ will statistically appear random. Therefore $h(S) \oplus h(r)$ will statistically appear random. The improved protocol is outlined below.

1. The manufacturer **MA** creates anti-forgery tags for the pharmaceutical product

1. **FORALL** RFID tag for pharmaceutical product *i* to be created
2. choose and print a unique S_i optically on the drug (label)
3. define and print I_{0i} optically on the drug (label)
4. print $\Sigma_i \leftarrow \textbf{\textit{Sig}}(SK_{MA}, [S_i \,||\, I_{0i}])$
5. $D_i \leftarrow h(\Sigma_i)$
6. compute $h(S_i)$ and burn into ω
7. randomly select and write r_i into δ_i
8. compute $h(r_i)$ and write $h(r_i)$ into ϕ_i
9. compute and write $C_i \leftarrow \textbf{\textit{Enc}}(PK_L, [\Sigma_i|S_i|I_{0i}], r_i)$ into γ_i

2. Parties who encounter the drug **P** detect counterfeit drugs and re-encrypt authentic drugs

1. **FORALL** RFID tagged drug i to be verified
2. optically read S_i, Σi
3. **IF** signature verification $\textbf{\textit{Ver}}(PK_{MA}, \Sigma_i, [S_i|I_i])$ is *false*
4. *abort.*
5. **IF** RF read C_i or RF read V_i or RF keyed read r_i fails
6. *abort*.
7. **IF** $V_i \neq h(S_i) \oplus h(r_i)$
8. *abort.*
9. **IF** C_i $\neq \textbf{\textit{Enc}}(PK_L, [\Sigma_i|S_i|I_{0i}], r_i)$
10. *abort.*
11. randomly select and RF keyed write a new $r_{i'}$ into δ_i
12. compute $h(r_{i'})$ and RF keyed write $h(r_{i'})$ into ϕ_i
13. compute and RF keyed write $C_i' \leftarrow \textbf{\textit{Enc}}(PK_L, [\Sigma_i|S_i|I_{0i}], r_i')$ into γ_i

3. Law enforcement agencies **L** trace wanted RFID tagged drug

1. **FORALL** RFID tagged drug i to be traced
2. **IF** RF read C_i or RF read V_i fails
3. *abort*.
4. $[\Sigma_i|S_i|I_i] \leftarrow \textbf{\textit{Dec}}(SK_L, C_i)$
5. **IF** signature verification $\textbf{\textit{Ver}}(PK_{MA}, \Sigma_i, [S_i|I_{0i}])$ is *false*
6. *abort*. COMMENT{Here $I_{0i} \subseteq I_i$}
7. **IF** $V_i \neq h(_{Si}) \oplus h(r_i)$
8. *abort.*
9. **IF** *compare* W to $h(r_i)$ returns *false*
10. *abort.*

In [7],[8] we established that the building block of our RFID secure pharmaceutical chain protocol satisfies perfect integrity for the law enforcement. Thus we have.

Theorem: *The secure pharmaceutical chain protocol using RFID satisfies perfect integrity for law enforcement.*

Proof: The proof is provided in [8].

5. Future work: modification to tag information I by third parties.

As the pharmaceutical product moves through the supply chain many parties will interact with the product. These may include: internal distributors, external distributors, pharmacy, and recycling center. As the parties interact with the pharmaceutical product, in their official

capacity they should modify information *I*. Recall we denoted the information that the manufacturer generated by I_0. We assume that the information can be modified in an append-only manner. Because the number of legitimate third parties will be small and known, elaborate information concerning the identification of these parties is not needed, but rather one can encode this identification is a small field. Further, we will utilize small signatures in this process. The precise data structure of *I,* as well as the modification protocol is not provided here. Suffice to say that current RFID technology does not support this amount of available memory, but modifications can be made. We have analyzed the data structure and have estimated its size as: Maximal memory requirements (full functionality with 10 entries of pedigree): 2890 bits.

6. Conclusion

In this paper we have described the necessary requirements to secure the pharmaceutical supply chain. We have described those parties that interact in the chain, and their roles. We have also described a privacy preserving protocol to demonstrate the integrity of the pharmaceutical products and how to allow law enforcement agencies to remotely check this information. Future work will describe the entire protocol as well as the data structure that will be used to store this information.

7. References

[1] Davey, M.: Illinois to help residents buy drugs from Canada, and afar. The New York Times (2004)

[2] Koh, R., Schuster, E.W., Chackrabarti, I., Bellman, A. Securing the pharmaceutical supply chain. Technical Report MIT-AUTOID-WH-021, AUTO-ID Center (2003)

[3] Harris, G. Tiny antennas to keep tabs on U.S. drugs. The New York Times (2004)

[4] Brock, D.L. Smart medicine: The application of Auto-ID technology to healthcare. Technical Report MIT-AUTOID-WH-010, AUTO-ID Center (2002)

[5] Juels, A., Pappu., R.: Squealing euros: Privacy-protection in RFID-enabled banknotes. In: Financial Cryptography, Springer-Verlag (2003) pp. 103-121

[6] X. Zhang and B. King. Modeling RFID Security, CISC 2005, Information Security and Cryptology, First SKLOIS Conference, CISC 2005, Beijing, China, December 15-17, 2005. Lecture Notes in Computer Science 3822 Springer 2005, pp. 75-90.

[7] X. Zhang and B. King. Integrity Improvements to an RFID Privacy Protection Protocol for Anti-counterfeiting, ISC 2005. Information Security, 8th International Conference, ISC 2005, Singapore, September 20-23, 2005, Proceedings. Lecture Notes in Computer Science 3650 Springer 2005, pp.474-481.

[8] X. Zhang and B. King An Anti-counterfeiting RFID Privacy Protection Protocol, *Journal of Computer Science and Technology,* Vol. 22,No. 3,May 2007, pp.438-448.

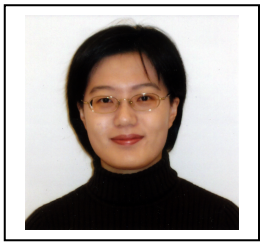
[9] SupplyScape Company, Electronic Pedigree using RFID and EPC.

Authors

Brian King

Brian King received a Ph.D. in mathematics (1990) and a Ph.D. in Computer Science (2000). He is currently an assistant professor of Electrical and Computer Engineering at Indiana Univ. Purdue Univ. Indianapolis (IUPUI). Prior to joining IUPUI he worked in the Security Technologies La at Motorola Research Labs. His research interests include: wireless security, cryptography, threshold cryptography and low-complexity cryptosystems.

Xiaolan Zhang



Xiaolan Zhang received the B.S. degree in information engineering from Shanghai Jiao Tong University in 2003 and the M.S. degree in computer engineering from Purdue University at Indianapolis in 2005. Now she is a Ph.D. candidate in electrical and computer engineering at the University of Illinois at Urbana-Champaign. She is currently a Research Assistant in the Coordinated Science Laboratory at the University of Illinois at Urbana-Champaign.