An NFC Based Consumer-Level Counterfeit Detection Framework

Muhammad Qasim Saeed
Information Security Group
Royal Holloway University of London
Egham, UK
muhammad.saeed.2010@live.rhul.ac.uk

Zeeshan Bilal
Information Security Group
Royal Holloway University of London
Egham, UK
zeeshan.bilal.2010@live.rhul.ac.uk

Colin D.Walter
Information Security Group
Royal Holloway University of London
Egham, UK
Colin.Walter@rhul.ac.uk

***Abstract*—Counterfeit products have been a major concern in global market. There are many procedures for preventing the counterfeiting of goods, such as holograms, tamper-resistant packaging etc. However, there is still a rising trend in counterfeit goods. With the emergence of RFID systems, supply chain management is able to detect counterfeit products relatively easily. Existing techniques generally involve a centralized database and can only be implemented in an online scenario. This deprives the individual customers of using any authentication mechanism while making purchases due to the infeasibility of accessing a central database. In this paper, we analyze a recently published semi-offline scheme proposed by Alex *et al*. We identify limitations and weaknesses in this scheme and suggest solutions. We modify the framework to remove the main weakness and extend it to the consumer level so that a consumer can determine the legitimacy of a product. This involves Near Field Communication technology (NFC) which is now widely available in cell phones – the consumer's cell phone acts as an RFID reader and detects counterfeit products. Our solution is completely offline as it does not require a central database for product authentication. It is based on Public Key Cryptography *(PKC)* and a Public Key Infrastructure *(PKI)*. It offers dual layer authentication mechanisms to customers, *visual* and *cryptographic*, without accessing the supplier's database. The main beneficiary of the proposed framework is the consumer who uses the Internet for online shopping and can authenticate a product reliably after delivery. Our scheme is stand-alone and does not require the transfer of any secret values from a centralized authority.**

***Index Terms*—Anti-Counterfeit Products; EPC Tags; Off-line Authentication; Near Field Communication (NFC).**

I. Motivation

Counterfeit products are one of the major threats to modern commerce. According to estimates by the Counterfeiting Intelligence Bureau (CIB) of the International Chamber of Commerce (ICC), counterfeit goods make up 5 to 7% of world trade [1]. Counterfeits are available in a wide range of products, typically starting from high value small goods like watches, designer clothes, DVDs and electronic chips to high cost items such as cars, motorcycles and bicycles.

Counterfeit products are classified into four categories [2].

1) The first category consists of those products that are inexpensive, lower quality and may lack original packaging. This category is often called 'knockoff'. These products are being sold as counterfeits and the consumer is aware of it.
2) In the second category of counterfeit, a genuine product is reverse engineered and identical copies are sold as the genuine product. It is hard for a consumer to differentiate between a genuine and a counterfeit product. This category is meant to deceive the consumer.
3) These are the products that are produced by an outsourced manufacturer without intimation to the original owner. For example, an outsourced manufacturer manufactures further product after termination of its contract with the original owner without notifying the original owner.
4) These are genuine products that do not meet the manufacturer's standards but are not labeled as faulty.

One of the major outlets for counterfeit products is Internet e-commerce where the consumer has no means of authenticating a product before delivery. Even after delivery, the consumer has very limited resources to determine the legitimacy of a product. Auction websites, such as eBay, have further expanded the market of counterfeit products. For example, test purchases from 300,000 Dior products and 150,000 Vuitton items offered on eBay during 2006 found 90% conterfeits [3]. Tiffany & Co. purchased 186 random items from eBay and found only 5% to be genuine [4].

These circumstances call for mechanisms to fight counterfeiting. Analysis shows that the money spent in this way prevented a much greater loss from counterfeit goods. According to the U.S. Chamber of Commerce, $5 is gained for every $1 invested in this battle [5].

Radio Frequency Identification (RFID) tags attached to various goods provide a tool to remotely identify these goods. Among these, EPC tags are the most important. The Electronic Product Code (EPC) network is used for supply chain management and can be used as a tool for anti-counterfeiting [6]. Every item equipped with an EPC tag carries a 96-bit code to uniquely identify and manage the item in a supply chain. There are two main approaches to using the EPC as an anti-counterfeiting measure [7]. The first approach is tracking the physical location of a tag and updating the result in an online database. The EPC of a counterfeit product will appear twice (at least) in the database, assuming the counterfeit product is equipped with a cloned EPC tag. This is called the 'Track and Trace' approach. The main disadvantage of this approach

978-1-4673-5839-2/13/$31.00 ©2013 IEEE

is its significant communication and computation overheads. Every reader has to update records in the online server in real time. The online server has to track and trace each code received from the online reader and generate triggers in case of any abnormality. In addition to these overheads, there are also some privacy concerns associated with this approach: for example, tracking of individuals from the products they carry, or tracking medicines etc [8]. Moreover, there are some issues with updating the database. For example, suppose a retailer were to clone the EPC and attach the cloned tag to a counterfeit product. Assume he does not update the corresponding record in the database when it is sold. When he sells the counterfeit product, the consumer buying the counterfeit can check and find a valid record for the cloned EPC but will not be able to update its record to record its sale due to limited access and privacy concerns.

Another anti-counterfeiting approach is based on cryptography. In this approach, each tag contains a secret value, knowledge of which is established by the reader in an authentication proof. Generally, this uses an encrypted challenge-response protocol as it may be eavesdropped and the secret cloned if sent in the clear. This approach may be based on symmetric key or asymmetric key cryptography.

Anti-counterfeiting approach based on cryptography can be categorized into two main categories. In an *Off-line* approach, there is no shared secret between the tag attached to a product and the reader. Any reader can access the tag and verify its contents. In case the tag's contents are verified and the tag is authenticated, the product is assumed to be a legitimate one. In the *On-line* category, there is secret information shared between a tag and the reader. The reader needs an access to a server containing a database of secrets in order ascertain the legitimacy of a product. It is very unlikely that the login credentials to access the database are provided to a consumer. This makes former approach more suitable for product authentication at the consumer level.

If symmetric key cryptography is used, the reader must already know the secret value of the tag and match it against the secret value received from the tag. The secret value of each tag is chosen uniquely so that if a tag is compromised, it should not break the entire system. This results in a requirement for a secure and efficient key distribution mechanism to distribute the tags' secrets among the readers. One way is to deliver the secret values of all appropriate tags to readers in advance but this approach requires secure distribution of millions of such keys and is considered infeasible. Another way is to store the key database in an online server. This server is online at all times to provide the secret values of tags to readers. Assuming millions of tags are deployed in the supply chain with hundreds of compatible RFID readers, this approach incurs even higher communication and storage overheads than the track and trace approach [7]. In addition, the reader must always be trusted by the supplier since the reader stores the secret values of the tags in any framework employing symmetric key cryptography.

As observed earlier, one of the major factors in the upsurge in counterfeit products is online shopping. With the advancement in Internet technology, the volume of online shopping is growing rapidly. It is not feasible at present to tailor any symmetric key approach for product authentication to online shopping. The reason is obvious: a consumer receiving a product through online shopping does not possess an RFID reader to communicate with the tag attached to the product. Even in the very unlikely scenario where a consumer possesses an RFID compatible reader, the supplier will have to provide login credentials to access the database. This situation is far from practical. Thus, product authentication at the consumer level remains an open challenge, especially for the Internet shopping framework.

In contrast to the symmetric key approach, asymmetric key cryptography (or Public Key Cryptography (PKC)) can also be used to authenticate a product. Considering the limitations of the symmetric key approach described above, the case for PKC in product authentication is thus very strong. The main restriction in using PKC on RFID tags, such as EPC tags, is the limited computational and storage capabilities of these tags. Recently, Alex Arbit *et al.* presented a working implementation of a PKC-based anti-counterfeiting framework [8]. They selected WIPR, an ultra-low-power public key cryptosystem developed by Oren and Feldhofer [9]. WIPR is a lightweight version of 1024-bit Rabin encryption [10], with a minimal hardware footprint of under 4700 gates. The framework presented by Alex Arbit *et al.* is semi-offline, where the verification and decryption keys are dispatched to the reader using a smart card and the reader is considered as a secure module for storing these keys.

A. Our Contribution

We focus our work on detecting counterfeits that fall into the categories 2 and 3 mentioned in Section I. Category 1 counterfeits are not a major concern as the consumers are aware of the fact that the products they are buying are counterfeits. The loss in the sales of the original product owner is also negligible as very few genuine goods purchasers would purchase a knock off [2]. Category 4 counterfeits can be restricted by enforcing an efficient quality control measure by the genuine product owner. Categories 2 and 3 are most critical as not only is the consumer unaware of the illegitimacy of the product, but also the genuine owner has no or minimal control over the production, marketing and selling of such products. Our model helps in detecting counterfeits products at consumer level pertaining to category 2 and 3 products, thus providing an efficient tool to detect counterfeits.

In this paper we analyze the anti-counterfeiting model which Alex Arbit *et al.* proposed in [8] and highlight a few of its short-comings. The main drawback of their framework is its semi-offline structure, which renders it incapable of authenticating a product at consumer level despite using public key cryptography.

We revise and extend their work in two main ways. Firstly, we restore the EPC tag to the original standard rather than using the modified EPC tag in the Alex Arbit *et al.* model. This resolves any modification-related problems in the existing

EPC framework. Secondly, we supplement the EPC tag with an NFC tag which can perform the necessary computations that were not within the capability of the EPC tag. The main advantage of being offline is that a consumer can authenticate a product without any online communication with the supplier's database. We believe that our offline product authentication at consumer level can prove to be an efficient anti-counterfeiting tool. Although our framework is applicable to all levels of supply chain management, the main beneficiary are customers using the Internet for online shopping. This framework not only helps the customers to authenticate a product, but any verifier such as a law enforcement agency can also use this model to detect counterfeit products.

We resolve the problem of provisioning of an RFID reader for product authentication to every consumer by also using a Near Field Communication (NFC) tag for the EPC. The NFC tags are RFID tags based on ISO/IEC 14443 operating in the 13.56 MHz frequency band. NFC technology is now available on cell phones and so a consumer's cell phone can act like an RFID reader to read the EPC. Since our framework is totally offline, the consumer is able to distinguish between a legitimate and a counterfeit product by using his cell phone without accessing the supplier's database.

We also resolve the issue of trust in the reader for an offline framework. In the work of Alex Arbit *et al*, the reader is a secure module storing a verification key and a decryption key, as noted earlier in this section. These keys cannot be stored on any reader that is not trusted by the supplier. Although the consumer's cell phone is not trusted by the supplier, this issue can be addressed by using a Public Key Infrastructure (PKI), thereby all but eliminating any key storage requirement on the reader side. In many cases, the NFC tag can also be accessed and authenticated during product distribution without having to resort to the greater reading range of the EPC tag.

The first part of the paper introduces NFC technology and the different types of NFC tags available in the industry. This is followed by an overview of the EPC network and its application in supply chain management. Next, related work in this area is described with a detailed description of the framework proposed by Alex Arbit *et al* in [8] and discussion of some of its shortcomings. This is followed by our main contribution, which is to modify and extend that work. Finally, we present a detailed analysis of our proposals which also highlights some unresolved issues.

II. RFID Technologies

In this section, we introduce the two different classes of RFID technology that are related to our framework.

A. Near Field Communication

Near Field Communication (NFC) is a wireless technology that operates at a distance of less than about 4 cm. This technology is compatible with contactless smart cards based on the ISO/IEC 14443 standard. The frequency of operation falls in the HF band operating at 13.56 MHz [11]. The limited 4cm range means that their use in supply chain management can be problematic. Access to tags embedded in products which are packaged in rigid expanded polystyrene foam requires precise location markers printed on the boxes, and the ability to place a reader on that location. This may not be possible in a warehouse.

An NFC link is established between a tag and a reader on a single touch. This makes it a user friendly technology where no input is required from a user apart from touching the tag to the reader. NFC has three modes of operation enabling a variety of applications: peer-to-peer mode, read/write mode and emulation mode [12]. The latest mobile phones are equipped with the NFC technology [13] enhancing the number of its users. We only focus on its read/write mode of operation as only this mode is applicable to our proposed framework. In read/write mode, an NFC device (or NFC equipped cell phone) acts as an RFID reader/writer to read or write an NFC tag. NFC tags are, in fact, RFID tags operating at 13.56 MHz and based on ISO/IEC 14443 standard.

In order to maintain the interoperability of NFC devices and tags, the NFC Forum (a forum to standardize the applications related to NFC [14]) has specified four different types of tags [15]: Type-1, Type-2, Type-3 and Type4. Type-1 has the least resources in terms of computational power and memory whereas Type-4 is much more powerful and contains a cryptographic processor.

B. EPC in the Supply Chain

The EPCglobal Class-1 Gen-2 (*EPC C1G2*) standard [16] specifies low-cost UHF tags which operate in the frequency range of 860-960 MHz and have a read range of 2-10 metres. This longer range makes UHF tags more easily read in containers and warehouses than is the case with NFC tags. Electronic Product Code (EPC) tags are typically deployed in supply chain management systems for automated inventory checks. The EPC is a 96-bit identifier stored in the EPC tag which helps to identify each tagged product uniquely. EPC has various advantages over existing product identification techniques, e.g. barcodes, as the former does not require line of sight compared to the latter. Moreover, the EPC tag may store additional information about the product which cannot be achieved using a barcode. Because of these advantages, barcodes are often being replaced by EPC tags in the supply chain.

III. Related Work

The EPC network as an anti-counterfeiting tool was proposed by Staake *et al.* [6]. The proposal is based on a central database server and does not explicitly cover the use of cryptography. The BRIDGE project [7] analyzed various anti-counterfeiting approaches based on RFID tags. This work analyzed the secure distribution and management of secret keys in a symmetric key anti-counterfeiting framework, and showed that it results in ten times more communication and computational overheads than in a track-and-trace anti-counterfeiting system.

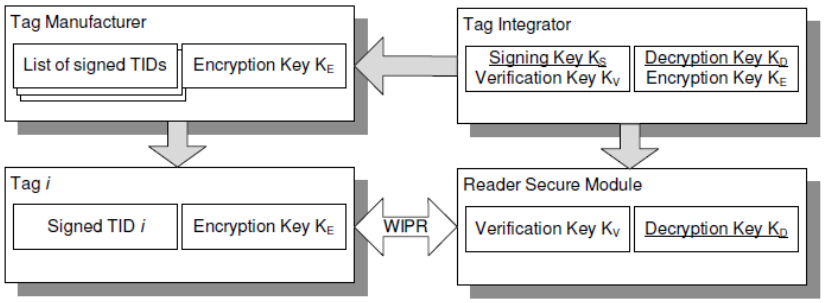

Fig. 1. Alex *et al* anti-counterfeiting framework([8], fig. 2)

An NFC based tag authentication framework is proposed by Saeed and Walter in [11]. They proposed a framework that can distinguish between a legitimate NFC tag and a cloned NFC tag without relying on a central database server. Their proposal is based on public key certificates and a PKI.

Work to reduce the computational overheads in public key cryptography is also in progress and various lightweight public key cryptosystems are being designed. The CRYPTOGPS is a light-weight public-key cryptosystem mainly suitable for UHF RFID tag. It can be implemented in around 2800 GE (Gate Equivalent) with a processing time of around 720 cycles [17], [18]. The Rabin Cryptosystem was the first to be implemented in a wireless sensor network in [10]. It took about 16,700 GEs to implement 512-bit encryption. This led them to declare that this cryptosystem was unsuitable for resource-constrained RFID tags. A lower version of this scheme, WIPR, was introduced in [9]. It is well suited to RFIDs because it has the smallest hardware footprint and largest payload capacity of all published high-security public key schemes [8]. Alex Arbit *et al* proposed an anti-counterfeiting framework based on WIPR that uses 1024 bit keys with a hardware footprint of just 4700 GEs.

A. The Alex Arbit et al Anti-Counterfeiting Model

Alex Arbit *et al* proposed an anti-counterfeit model based on EPC tags and Public Key Cryptography [8]. Their framework is described in Figure1. The figure represents the various entities involved in the anti-counterfeiting framework. The framework consists of the following sequence of operations.

- **Step 1:** The framework is initiated by the Tag Integrator, who wishes to deploy anti-counterfeiting technology in EPC tags. He creates two public-private key pairs: a Private Signing Key K_S together with its Pubic Verification Key K_V, and a Private Decryption Key K_D with its Public Encryption Key K_E. The signing key K_S is never disclosed to any entity of the framework. The Tag Integrator generates a list of Tag Identifiers (TIDs) and signs each TID with the key K_S. He then sends the list of signed TIDs to the tag manufacturer along with the encryption key K_E. Since the tag manufacturer lacks K_S, he is unable to generate arbitrary signed TIDs, thus ensuring the integrity of the TIDs.
- **Step 2:** The tag manufacturer produces and deploys the tags, each with an individually signed TID from the list along with the public key K_E.
- **Step 3:** The reader receives K_D and K_V from the tag integrator. Once these keys are delivered to the reader, the system can operate in an offline framework. The reader then carries out a challenge-response protocol to determine that the tag possesses a valid, signed TID.

This is a semi-offline model as it requires an initial key distribution mechanism to distribute keys to readers through some secure channel. The authors suggests distributing keys through a secure module such as a smart card.

B. Weaknesses

There are several weaknesses in this model.

- The framework is semi-offline where the reader stores K_V and K_D. This puts a limit on its utility for product authentication at consumer level, as K_D cannot be communicated to the consumer.
- K_V and K_D have to be delivered to a reader through some secure channel such as a smart card. Since the same set of keys are distributed to each reader, this results in a single point of failure where the loss of a single smart card will compromise the entire system. Moreover, if a single retailer is dishonest, he can break the entire system as all the readers use the same set of keys K_V and K_D.
- The authors have not discussed the storage location and accessibility of K_E inside an EPC tag. If K_E is stored at an accessible location, an attacker can make a successful counterfeit tag by simply copying all the content of the EPC tag, including K_E, to a counterfeit tag. If K_E is stored at some inaccessible location inside the EPC tag, it can prevent tag cloning, but still the framework is prone to single point of failure. Since K_E is identical in each tag, it only needs an adversary to attack a single tag to compromise the entire system.
- **Bypass Attack.** The framework is prone to a "Bypass" attack where the anti-counterfeiting protocol is circumvented in a counterfeit tag in the following way. The framework is designed to handle both WIPR-modified and standard EPC tags. During the handshake protocol between a reader and an EPC tag, the tag responds with an indication of being WIPR modified or not. This is achieved by the modified tag sending a special WIPR

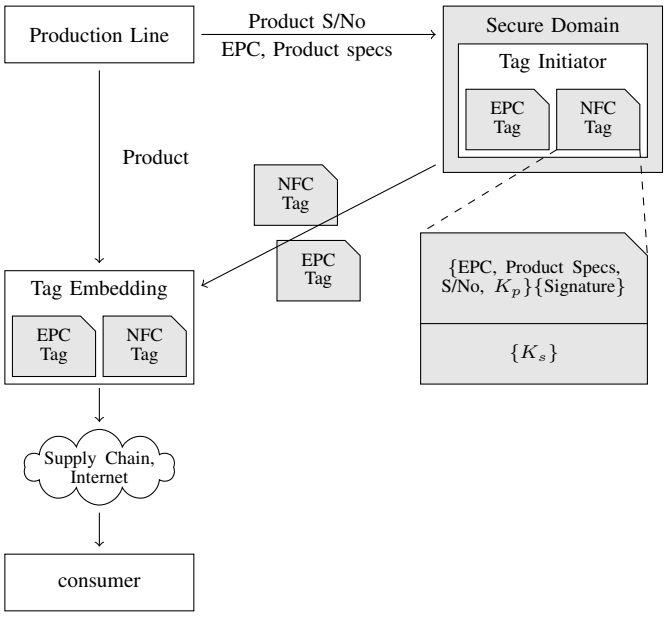

Fig. 2. Initialization phase of proposed scheme.

EPC message to the reader instead of the actual EPC value according to the standard (see Figure 4 in [8]). The special WIPR message acts as a flag to the reader to execute the anti-counterfeit protocol.

The framework does not provide integrity protection to the special WIPR EPC message contents and so alterations to this message may not be detected. An attacker just needs to replace the message with the actual EPC value in the counterfeit tag, thereby making the tag claim to follow standard EPC protocol. On receipt of the actual EPC value from a counterfeit tag, the reader does not execute the anti-counterfeiting protocol, instead assuming the tag to be unmodified as the flag (the special WIPR message) is not received from the tag. Thus, the anti-counterfeit protocol is bypassed and the counterfeit tag remains undetected. Of course, if the reader knows the TID belongs to a tag which follows the WIPR modified protocol, then the counterfeit should be detected.

IV. Proposed Anti-Counterfeit Offline Model

In this section, we propose a different anti-counterfeiting model that uses RFID technology to detect counterfeit products. This model is a modified version of the Alex Arbit *et al.* [8] model. We add an NFC chip to the EPC tag, thereby providing a product authentication mechanism to the consumer level. NFC technology is used mainly for two reasons. Firstly, this technology can support public key cryptography on tags and, secondly, it is available on cell phones enabling them to act as RFID readers. The former supports our framework in an offline mode where a connection to the supplier's database is no longer required. The latter helps extend the authentication model to the consumer level, where a consumer uses his cell phone to authenticate a product.

A. Initialization Phase

Our new anti-counterfeit model is executed in two phases, the first, namely initialization, being illustrated in Fig. 2. This phase is initiated from the production line where a serial number and an EPC are allocated to the product. The serial number, EPC and the product specification are communicated to Tag Initiator *(TI)*. Meanwhile, the product is dispatched to the Tag Embedding department.

On receipt of the information from the production line, the *TI* generates a public/private key pair (K_p, K_s). This pair is unique for each tagged product item. The *TI* must be a secure platform as it is responsible for the generation of anti-counterfeit keys. It stores the EPC in an EPC tag and forms a string S_1 defined by

$$S_1\text{=EPC}\|\text{Product S/N}\|\text{Product Specification}\|K_p$$

The *TI* digitally signs this string S_1 with his signing key K_{sign} and stores the string along with its signature on the NFC tag. The signature on the tag is stored as a 'Signature Record' according to NFC Forum's Signature Record Type Definition [19]. According to this specification, the signature record consists of a digital signature along with a digital certificate containing the corresponding verification key K_{ver}. S_1 and its signature are stored at a memory location accessible to any NFC reader. However, the *TI* also stores the secret key K_s inside the tag but at a secure location. This location of K_s is only accessible to the tag's processor and therefore inaccessible to a reader. The corresponding public key K_p is a part of S_1, and therefore accessible to any NFC reader. After storing the relevant information on both tags, the *TI* configures both tags as write protected and dispatches them to the Tag Embedding department.

On receipt of the tags from the *TI*, the Tag Embedding department embeds both tags on the product. Since the tags are physically embedded we shall assume that any attempt to remove the tags will destroy them. After embedding the tags, the products are shipped to the supply line, from whence they may be delivered to a department store or direct to a consumer through online shopping.

B. Verification Phase

This phase is executed by the verifier on receipt of the product. Since this is an offline framework, the verifier does not require any connection to the supplier's database. Therefore the verifier may be a consumer, a warehouse employee, a member of law enforcement or indeed, any individual wishing to authenticate the product. The verification phase is executed in two phases. The first is visual and the second is cryptographic. The visual verification process is executed as follows:

- The consumer checks the claimed identity of the product itself and the integrity of the tag which should be bound to the product item in a tamper-evident manner.
- The verifier places his cell phone on the NFC tag to read its contents. The accessible data on the NFC tag (string

S_1 and corresponding signature) is communicated to the cell phone.
- The cell phone verifies the signature. A successful verification is an indication that the string S_1 is legitimate.
- The cell phone displays the product specification and its serial number to the consumer.
- The consumer checks the two product descriptions match each other.

In the case of a successful visual verification, the consumer should initiate the second phase of product verification, which is a cryptographic challenge-response protocol:

- The cell phone sends a random challenge r to the NFC tag.
- The tag signs r with the secret key K_s and returns the result $sign(r)$ to the cell phone.
- The cell phone verifies the signature using the corresponding verification key K_p which it knows from S_1.

A successful verification is a strong indication of a genuine product, as a counterfeit tag lacks the signing key K_s and so cannot compute a valid signature on r.

V. Analysis

In this section, we analyze the proposed framework from various angles. Our model addresses category 2 and 3 of counterfeits as mentioned in I-A. Categories 1 and 4 are not a focus of our work since, in the former case, the products are being identified by the consumers as counterfeits and, in the latter, can be countered with an appropriate quality control. Categories 2 and 3 are critical as the consumer is not aware of the illegitimacy of the product. Since our model is designed to detect counterfeits at the consumer level, it provides a tool for consumers to determine the legitimacy of a product.

In the case of category 2 counterfeits where the original product is reverse engineered, the NFC tag attached to the original product cannot be reverse engineered – the secret data on the NFC tag cannot be copied as explained in Section V-B. A consumer can therefore determine the illegitimacy of a reverse-engineered product by the unsuccessful verification of the data on the NFC tag.

In our model, the Tag Initiator (*TI*) is responsible for generating and storing the secret keys on the NFC tags. The tags are then embedded on the product by another department termed the 'Tag Embedding Department'. In the case of out-sourced manufacturers, the product manufacturing and tag embedding are done by the out-sourced manufacturer. The *TI* remains a part of the genuine owner. The genuine owner provides NFC and EPC tags to the out-sourced manufacturer only in same quantity as specified in the contract. If an out-sourced manufacturer is dishonest and produces more than the quantity mentioned in the contract (category 3 counterfeits), he will have to produce the product either without the NFC tag or with a fake NFC tag. This counterfeit product is then detected by the consumer because making a fake NFC tag is too difficult (explained in Section V-B). Thus, our model helps in the detection of category 3 counterfeits at consumer level.

A. Justification for Two RFID Tags

We use two types of tags in our framework, an EPC tag and an NFC tag. Although both are RFID tags, they have very different characteristics. The main difference is the operating frequency: EPC tags operate at 860-960 MHz whereas NFC tags operate at 13.56 MHz frequency band. The range is consequently different in the two tags. EPC tags can be read from 2 to 8 metres whereas NFC tags have a very short communication range of no more than about 4 cms. This property makes only the EPC tag suitable for supply chain management in order to remotely identify the products. Since EPC tags are already deployed in the market for supply chain management, we use EPC tags in our framework in order to maintain the backward compatibility and normal supply chain needs.

NFC tags are used because two main requirements cannot be fulfilled by EPC tags. Firstly, EPC tags are very resource constrained when compared to NFC tags: EPC tags have very limited computational power and much less memory, whereas NFC tags, specially NFC Type-4 tags, are much more powerful. Since our framework is based on PKC and PKI, where the tag has to perform PKC, we need a reasonably resourced tag. Secondly, our framework needs to provide authentication down to the consumer level. Without an NFC tag, this would require every consumer to be equipped with an EPC tag reader, which is far from practical. The issue is resolved with the inclusion of the NFC tag, as the consumer's cell phone can act as a reader for the tag.

B. Security Analysis

In this section, we analyze our framework from the security point of view. The goal of an attacker is to develop a clone tag or a tag with a valid signature. To develop a clone tag, the attacker must know the private key K_s of the original tag. This key is stored at an inaccessible location in the tag's memory and so it is normally secure from the attacker. The alternative solution open to an attacker with a cloned tag is to replace the legitimate public key K_p with the attacker's public key K'_p in S_1 and store the corresponding private key K'_s in the tag. However, this is not possible as the legitimate K_p is digitally signed (it is in a digital certificate) so that any alteration will invalidate the signature. Of course, the verifier must have a trusted source for the certificate's public key in order not to be duped.

In case an attacker spends time and money to reverse engineer a single tag and recover its private key K_s, it will not affect the entire system as the pair K_s, K_p is unique to each tag. The tags, being cheap, will have few counter-measures to side channel analysis, which will be a significant threat in some markets. However, this will avoid a single point of failure as experienced in Alex *et al* model.

Our framework is resistant to the bypass attack. The existence of K_p in S_1 is an indication that the tag is equipped with the anti-cloning feature. This key can neither be removed nor altered as it is digitally signed. The user's application on

the cell phone, once it has detected K_p, will execute the anti-counterfeiting protocol, thereby resisting the bypass attack.

In addition to cryptographic authentication, our framework also provides visual product authentication. After scanning the NFC tag, the product specification and product serial number is visually displayed on the user's cell phone display. The user can visually check and verify the information from the product or product packaging. Needless to say, there are many other sources of compromise. For example, the NFC tag could just return a QR code which connects the consumer's phone to the attacker's website and displays the expected protocol output and the verification data for the counterfeit product. Alternatively, the merchant may direct customers who lack the verification app to the attacker's website to download a compromised app that confirms the authenticity of any product.

The tags have to be tamper-evident. This is to ensure that they cannot be re-used on counterfeit products. If the tag were to contain the URL for registering the product under the manufacturere's guarantee, customers could be encouraged by their app to register, the manufacturer could check its database for duplicate registrations that would flag a clone, and the manufacturer could advise the consumer if there were such a problem.

One critical factor in securing the system is the physical location of the NFC tag in the product. This is an industry specific decision and requires careful consideration. It is assumed that the tags are physically embedded on the main assembly of the product and not on casing/packing or on any easily replaceable component of the product, very much in the same way as a watermark or hologram is an integral part of the item it is protecting. As in the latter case, an attacker just needs to place the tag embedded component from a legitimate product into the counterfeit product.

C. Economic Analysis

This section analyzes economic aspects of the proposed scheme at a broader level.

The inclusion of NFC tags in addition to EPC tags for product identification requires some additional investment by the supplier. For simplicity, we assume the additional costs associated with generating keys, signing certificates, writing to the tags, embedding the tags, etc. is already included in the cost of the NFC tag. We also assume that the cost of an item is independent of the number of such items made, which is plainly rather naïve.

We only consider loss in the sales revenue because of counterfeit products. The true loss is much higher and not just financial. There are various other important aspects such as loss in distinctiveness of brand image, gradual decline in sales, unemployment etc, but inclusion of these factors complicates the analysis too much – our goal is merely to justify the cost of our anti-counterfeiting scheme.

Let x be the production cost/unit and y the selling price/unit, $\Delta = y - x$ the profit/unit, n the market demand over some fixed period and p the percentage of counterfeits in the market. Suppose, by observing his sales, the original manufacturer is able to make exactly the number of products he can sell, namely $n(1-p)$. The remaining market share of np consists of counterfeits from other suppliers. The profit P_r by the original manufacturer is $n \cdot \Delta \cdot (1-p)$ compared with an ideal profit of $n \cdot \Delta$ if he were to supply the whole market.

Let c be the unit cost of implementing RFID tags on a product. This cost includes all associated costs regarding RFID implementation as mentioned earlier. If no price increase is allowed and the RFID tags eliminate all counterfeits, the profit P_r' generated under these conditions is:

$$P_r' = n \cdot (\Delta - c)$$

This represents an increase providing $P_r' > P_r$, i.e.

$$n \cdot (\Delta - c) > n \cdot \Delta \cdot (1-p)$$

which is equivalent to $c < \Delta \cdot p$.

The percentage p of counterfeit products depends on various factors like brand, geographical location, in-store or on-line etc. It is difficult to find an exact value of p for a specific brand as the counterfeit products of categories 2, 3 and 4 are indistinguishable. Fortunately, the surveys mentioned in Section I regarding counterfeit products on eBay are only measuring a fraction of the total market for the goods in question – although this may change. Assuming the price of implementing RFID tags with the required infrastructure is \$2/unit, and assuming p as 7% (which is an estimate by the Counterfeiting Intelligence Bureau (CIB) of the International Chamber of Commerce (ICC)) [1]), our model is suitable for those businesses where the profit/unit Δ is greater than \$28.50, i.e. around \$30. This is a very rough estimate as it is based on very simple assumptions. Of course, with higher values of p, the profit/unit threshold at which the NFC RFID scheme becomes cost effective decreases. This means that it becomes suitable for more businesses.

VI. Conclusion

This paper presents an RFID based anti-counterfeiting framework at the consumer level. There are two main constraints related to this authentication level. Firstly, the individual consumer cannot afford to keep an RFID reader to authenticate a product; and secondly, customers cannot be provided with access to the supplier's database because of intellectual property rights and communication overheads. We addressed both these constraints by using NFC technology: an NFC tag is used along with an EPC tag for consumer level authentication on the reasonable assumption that most individuals will carry an NFC-enabled mobile phone in the near future. We provided a dual layer verification mechanism to a consumer. In the first phase of verification, the product specifications are displayed to the consumer on his cell phone for visual verification against the actual product. After successful verification, a cryptographic challenge-response protocol is executed to authenticate the product. Our proposal is based in PKC and PKI and successfully detects the counterfeit products. Analysis shows that the proposed framework is

suitable for products with a profit/unit above about $30 under some straightforward assumptions, with about 7% of market lost to counterfeits, and an approximate cost of $2 per item for implementing NFC chips in the products. This threshold makes us conclude that our proposed framework is suitable for many products for which counterfeiting is a major concern.

REFERENCES

[1] P. Avery, F. Cerri, L. H. Fayle, K. Olsen, D. Scorpeci, and P. Stryzowski, "The Economic Impact of Counterfeiting and Piracy." Organisation for Economic Co-operation and Development (OECD), 2008.

[2] B. Berman, "Strategies to Detect and Reduce Counterfeiting Activity," in *Business Horizons*, vol. 51, no. 3. ELSEVIER, 2008, pp. 191 – 199.

[3] C. Matlack and T. Mullaney, "Fed Up With Fakes," in *Bloomberg Businessweek*, October 2006. [Online]. Available: http://www.businessweek.com/stories/2006-10-08/fed-up-with-fakes

[4] L. Chao, "What Happens When an eBay Steal Is a Fake," in *The Wall Street Journal*, June 2006. [Online]. Available: http://online.wsj.com/article/SB115154214225593742.html

[5] The Economist, "The spread of counterfeiting: Knock-offs catch on," 2010. [Online]. Available: http://www.economist.com/node/15610089

[6] T. Staake, F. Thiesse, and E. Fleisch, "Extending the EPC network: the potential of RFID in anti-counterfeiting," in *Proceedings of the 2005 ACM Symposium on Applied Computing*, ser. SAC '05. New York, NY, USA: ACM, 2005, pp. 1607–1612. [Online]. Available: http://doi.acm.org/10.1145/1066677.1067041

[7] M. Lehtonen, J. Al-Kassab, F. Michahelles, and O. Kasten, "Anti-counterfeiting business case report," in *Technical report, BRIDGE Project*, December 2007.

[8] A. Arbit, Y. Oren, and A. Wool, "Toward Practical Public Key Anti-Counterfeiting for Low-Cost EPC Tags," in *International IEEE Conference on RFID*. Orlando, USA: IEEE, 2011, pp. 184–191.

[9] Y. Oren and M. Feldhofer, "A low-resource public-key identification scheme for RFID tags and sensor nodes," in *Proceedings of the Second ACM Conference on Wireless Network Security, WISEC*, March 2009, pp. 59–68.

[10] G. Gaubatz, J.-P. Kaps, E. Öztürk, and B. Sunar, "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks," in *The 3rd IEEE Conference on Pervasive Computing and Communications Workshops*. Kauai Island, USA: IEEE, March 2005, pp. 146–150.

[11] M. Q. Saeed and C. D. Walter, "Off-line NFC Tag Authentication," in *The 7^{th} International Conference for Internet Technology and Secured Transactions (ICITST-2012)*. IEEE, December 2012.

[12] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger, "NFC Devices: Security and Privacy," in *The Third International Conference on Availability, Reliability and Security, ARES*. Technical University of Catalonia, Barcelona: IEEE, March 2008, pp. 642–647.

[13] NFC World, "A definitive list of NFC phones," 2012. [Online]. Available: http://www.nfcworld.com/nfc-phones-list/

[14] NFC Forum, "The NFC Forum," 2004. [Online]. Available: http://www.nfc-forum.org/home/

[15] ——, "NFC Forum Tag Type Technical Specifications," 2010. [Online]. Available: http://www.nfc-forum.org/specs/spec_list/#tagtypes

[16] *EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz-960 MHz*, GS1 EPC-Global Standards Std. Version 1.2.0, 2008.

[17] A. Poschmann, M. J. B. Robshaw, F. Vater, and C. Paar, "Lightweight Cryptography and RFID: Tackling the Hidden Overhead," in *Information, Security and Cryptology (ICISC)*. Springer, 2009, pp. 129–145.

[18] S. Canard, L. Ferreira, and M. Robshaw, "Improved (and Practical) Public-Key Authentication for UHF RFID Tags," in *The 11th international conference on Smart Card Research and Advanced Application (CARDIS)*, ser. Lecture Notes in Computer Science, vol. 7771. Springer, 2012, pp. 46–61.

[19] *Signature Record Type Definition: Technical Specification*, NFC Forum Std. SIGNATURE 1.0, November 2010. [Online]. Available: http://www.nfc-forum.org/specs/spec_list/