AN ANALYSIS OF AUTHENTICATION FOR PASSIVE RFID TAGS

Gregory Stuart Smith[1] Marijke Coetzee[2]
Academy for Information Technology
University of Johannesburg
South Africa

[1]Hyperionza@gmail.com
[2]marijkec@uj.ac.za

ABSTRACT

RFID (Radio Frequency Identification) tags have become pervasive for identifying objects, people and pets, automated payment and theft-deterrents. However, assurance of tag identity has not been built into the RFID environment. Privacy by means of encryption can prevent the data from being human readable but cannot stop a clone being created. This paper considers recent approaches that have been proposed to breach this gap. These include PUF's (Physically Unclonable Functions), cryptography, digital signatures and radio fingerprints.

This paper contributes a critical analysis of current approaches in order to identify requirements for RFID tag authentication, focusing on passive RFID tags used for product authentication.

KEY WORDS

RFID tag authentication, Product authentication, PUF, RF Fingerprinting, Digital Signature, Cryptography.

AN ANALYSIS OF AUTHENTICATION FOR PASSIVE RFID TAGS

1. Introduction

A basic RFID system consists of small transponders, or tags, attached to physical objects and RFID tag readers. When wirelessly challenged by a reader, the tag responds with some identifying information that may be associated with arbitrary data records. Thus, RFID systems are a type of automatic identification system, similar to optical bar codes [1], but without the requirement for active human interaction.

Throughout its development, RFID technology was considered infallible as tags and readers could not easily be copied and reproduced, as the technology was not available. Today that technology does exist [2]. Criminals with little technical knowhow and accessible RFID kits can clone tags, thereby producing counterfeit goods with seemingly authentic identifiers. Criminals who are competent in technology can use freely available, open source software [3] to copy and modify tags and reveal tag information. A clone, as used in this context, refers to the creation of an exact replica of the original.

The aim of this paper is to outline the different approaches to RFID tag authentication, both traditional and new, and to objectively lay out the weaknesses in each approach. This paper then proceeds to propose a set of requirements needed to solve the problem of authenticating RFID tags for the purpose of product authentication.

The rest of this paper is structured as follows: Section 2 outlines a case study and explains RFID tags. Section 5 defines four broad authentication models and details several implementations. Section 4 outlines criteria for comparison, tabulates the results and Section 5 briefly summarizes the table. Section 6 gives the requirements. Finally Section 7 concludes the paper.

2. Background

A RFID tag may claim that it is Tag X representing Manufacturer Y, identifying Object Z. Figure 1 shows Tag X, attached to an object such as a passport, representing an organization such as Home Affairs. Currently the only method to verify Tag X, the RFID tag, is the unique ID embedded on Tag X itself. There is no secondary method of authenticating the tag, to support its claim to its identity and proving its authenticity.

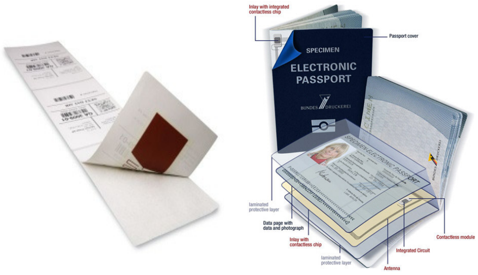

Inlay with integrated contactless chip
Passport cover
SPECIMEN
ELECTRONIC PASSPORT
BUNDESDRUCKEREI
laminated protective layer
Data page with data and photograph
Inlay with contactless chip
laminated protective layer
Antenna
Integrated Circuit
Contactless module

Figure 1: RFID tags embedded in a shipping label and a passport [4].

A passive RFID tag consists of an integrated circuit (IC) that receives its power from the reader via an induction loop aerial. The aerial is also used to send and receive data. Passive RFID tags either indicate their presence, i.e. on/off, or store data between 64-bits up to 64KB [5] in length. Active tags on the other hand have their own power source, are much more powerful and have a greater read range. They can typically store up to 128KB.

Without proper authentication in order to verify that the tag being read is not a clone, an attacker can easily write fraudulent data to a fake RFID enabled passport. In such a situation no-one would be the wiser because all available information about the passport would agree to its authenticity.

To avoid ambiguity, this paper takes the term *privacy* to mean a transmission that is not in plain text. However, *privacy* cannot be taken to mean proof of *authenticity*.

How is the authenticity of a RFID tag ensured? The following section outlines four broad approaches answering this question.

3. State-of-the-Art Authentication Models for RFID

Authentication is defined as the process of verifying the authenticity of the RFID tag [6]. In the RFID environment there exists two main types of authentication: mutual- and product- authentication [7]. *Mutual* *authentication* is when the tag and reader need to prove the authenticity of each other. *Product authentication* is verifying the authenticity of an object. The focus of this paper is placed on product authentication. Typically authentication is proved through at least three factors: something you are, such as the passport; something you have, such as an RFID tag, and something you know, such as some form of secret [8]. The act of authentication must be performed such that it is reliable, accurate, discrete and secure from attack [7].

In this section, four general approaches used in authenticating RFID tags are discussed. The first two of these models are traditional forms of authentication, used amongst high end RFID tags. Here, *digital signatures* and *cryptography* are discussed. The last two approaches considered are new techniques. Here, *Physical Unclonable Functions* and *radio fingerprinting* are discussed in order to determine whether it is viable to use unique device characteristics in authentication.

3.1.Digital Signature

Traditionally, digital signatures [9] create a unique fingerprint of the data being transmitted. The fingerprint will differ between two users transmitting the exact same data. This provides evidence of user authenticity, guarantees data integrity and ensures non-repudiation of signed electronic data.

An approach taken [10] is to embed an immutable digital signature into the tag memory, which may be used to validate the RFID tag. The digital signature would be created using a public-key infrastructure (PKI) such as RSA [10]. The public key would be stored on the reader and the private key used to create the signature stored on the tag. The suggested minimum length of such a key is 1024-bit [11], which to the authors' knowledge, is not implemented in any RFID tag. A successful cloning attack against a digital signature transponder (DST), which does not employ an immutable digital signature, is described in [12]. The key length, which was said the vendor to be safe at the time, was 40-bits. A far cry from 1024 bits.

Analysis: Immutable digital signatures are vulnerable to cloning. An unchanging bit-stream is transferred between tag and reader. A bit-stream copy may be created and written to an RFID tag simulator or even a new

RFID tag. An immutable digital signature [11], fails to provide adequate security measures in authenticating RFID tags.

3.2.Cryptography

Traditional cryptography has some role in authentication, be it in use as part of a digital signature, as above, or merely by saying that only authorized parties have the keys necessary to decrypt the message. However, as far back as 1996 [13], 56-bit symmetric keys were being broken with regularity. In 2005 the 112-bit TrippleDES algorithm was labeled as inadequate by NIST [14]. AES, the currently recognized mainstream cryptographic standard, has a minimum key length of 128-bit [15]. However, this paper's focus is not on traditional cryptography on high-end devices, rather this section considers a selection of the cryptographic algorithms available for use in RFID tags. In this section the *One-Time-Pad* approach used by Electronic Product Code (EPC) tags is discussed. This is followed by the recently broken Mifare Classic's *Crypto-1* cipher. Lastly, a hardware implementation of the *VEST-4* stream cipher is discussed.

One-Time-Pad: EPC Class 1 Generation 2 tags [16] are passive RFID tags that make use of a one-time-pad for certain commands, these being Write, Kill and Access. Authentication data is generated by the one-time-pad and transmitted in the clear. It is recommended that tags use unique passwords and that memory operations be performed in a secure location, which is not always possible.

Crypto-1: Crypto-1 is a cipher using only a 48-bit key [17].The algorithm was kept private, thus enabling security through obscurity. In 2008, a research group in the Netherlands successfully reverse engineered a Mifare Classic RFID tag [17], and conducted fraudulent transactions. The successful attack on the Crypto-1 cipher is an indication that the key lengths possible within the constraints of RFID are not sufficient to provide adequate security for either privacy or authentication for a determined attacker.

VEST-4: Very Efficient Substitution-Transposition or VEST ciphers [18] are implemented in hardware with keys ranging from 80 bit and upward. VEST ciphers have, since publication in 2005 [19], till at least 2007 have had a clean security record, with the fastest method of attack being a serial brute force attack. Unfortunately, VEST ciphers exceed the specifications of more limited RFID tags.

Analysis: Cryptographic techniques available to RFID technology are severely limited in nature and strength. This is primarily due to cost constraints [20].It must be pointed out that a key length of 48 bits, such as that used in Crypto-1, is less than 20% of the bits currently used in online encryption. As such cryptography should not be used in RFID for the purpose of authentication because of weak encryption (short keys), but used for weak information hiding (privacy).

The discussion to this point has been of well established models used in authentication in the electronic world. This paper now moves away from these models, changing focus to new and emergent models that focus on the inherent characteristics of devices that make them unique. Next this paper discusses *Physical Unclonable Functions* and *Radio Frequency Fingerprinting.*

3.3. Physical Unclonable Functions

The Integrated Circuit (IC) that contains the logic of an RFID tag has physical and electrical characteristics that exist as a result of the manufacturing process. These characteristics can ideally be used for authentication. Such characteristics are unique and it is impossible to intentionally create a duplicate. This is not to say that a duplicate may not exist as there is no control over these characteristics during the manufacturing process [21]. Characteristics are a result of material imperfections and irregularities in the doping and etching process. Recent research attempts to harness, measure, and extract these characteristics. A Physical Unclonable Function (PUF) is an implementation specific circuit that has been designed to extract these features [22] and is added into the IC of the RFID tag whose characteristics are to be measured and used in authentication. A particular drawback of this method is that each RFID tag that is manufactured would have to be tested repeatedly. This is to accommodate any electronic noise that may be present, and build a database of challenges and responses to be used for authentication. The result of the PUF is a set of fingerprints, or *challenge-response pairs* (CRP’s), that are stored in the database of some relevant authority. Next the *Vera X512H* RFID tag and the *FERNS* algorithm, as a means of using PUF's to determine authenticity are discussed.

Vera X512H: Released late 2008, it is claimed to be unclonable [23]. The RFID tag uses PUF technology in a challenge – response environment, where recorded challenges must be matched with their recorded responses generated by the PUF circuit by processing the challenge. Each challenge – response pair may only be used once to avoid man-in-the-middle and replay attacks. The match need only be above 75% for the tag to be taken as authentic [24]. The challenge is sent through the PUF circuitry, which uses delay characteristics of various components. Verayo claims a failure rate of less than one in billion [25]. Vera X512H is based on preliminary work with delay based arbiter PUF's presented in [26], [27] and [28]

FERNS: uses a different kind of PUF than Vera RFID tags. FERNS [29], is based on the transient power-on state of Static Random Access Memory (SRAM). This state, measured before the SRAM is initialized, can produce a unique set of values. However, the transient power-on states of SRAM can be affected by environmental noise. Thus, before releasing to market, the manufacturer would have to accurately map the set of values by aggregating many readings in different environmental conditions. A major flaw for use in authentication is that its output is a static digital response, and as such is susceptible to replay attacks. There is no dynamically generated challenge to prevent such an attack.

Analysis: As Karsten Nohl points out in [22] the designers of PUF's cannot anticipate the output, given an arbitrary input, merely by looking at the design. As he terms it, it is security-by-obscurity par excellence. There is no guarantee that the characteristics of the electronics will be unique Transmitting the PUF results insecurely open the approach up to man-in-the-middle as well as replay attacks, as only a limited number of challenge-response pairs are recorded and used. Whilst PUF's are secure from creating intentional clones on other tags, it is not secure from a device capable of simulating a RFID tag, assuming the attacker has unlimited contact time with the tag.

3.4. Radio Frequency Fingerprinting

Using unique characteristics to identify electronics is an area undergoing staunch research. Some success [30], [31] in measuring, and subsequently using the characteristics of wireless and wired network cards and their transmissions over their respective mediums, for device identification has been observed. This shows that, for a small environment, devices that transmit data over wires or radio frequency, have a unique way of doing it. Applying this to authentication is trivial. If each device, such as an RFID tag, that transmits data has a unique way of doing so, then it is logical to assume that two transmissions would then come from the same RFID tag if their transmission characteristics match.

As with PUF's, this model uses the unintentional characteristics created in a circuit during manufacture in an attempt to uniquely identify the circuit and prove its authenticity. However, as opposed to measuring these characteristics on the tag itself, the reader measures the effect they have on the transmissions and radio spectrum [32]. A patent exists [33] to match this approach. However further details, of its implementation regarding RFID tags, is not available. There is very little literature regarding this approach.

Analysis: Each radio transponder has different characteristics associated with it, also called transients. These transmission characteristics can sometimes be used to identify a particular transmitter. Unfortunately it is not reliable [34] as not all the fingerprints created by the transmission characteristics will be unique enough to prove an identity.

Having completed a discussion on each of the four different models available to the task of authenticating RFID tags, this paper now draws a comparison of the approaches discussed to determine the best approach for RFID product authentication.

4. Comparison of Authentication Models

The resource constrained nature of the RFID environment, used for product authentication, is the focus of the comparison. This paper addresses a RFID system, both tag and reader, with no form of authentication or privacy built into it. The purpose is to show the change required from such a system using both traditional and new approaches, to have a common point of comparison. The terms of comparison used in Table 1 are:

4.1.Implementation

Broken up into several criteria, this section focuses on the characteristics of the various implementations of the four models.

- Privacy or Authentication: is the model better suited to hiding of information (privacy), as opposed to proving a products authenticity?
- Cost Effectiveness: this shows how cost effective an implementation would be were it to be implemented.
- Resource Consumption: will the approach use a “High”, “Average”, “Low” or “None” amount of resources available to the tag to complete its function?
- Reliability: how reliable is the implementation regarding read errors and mismatches? Unfortunately not all models have data regarding this.
- Strength: how much difficulty must an attacker go to, to create a duplicate RFID tag or RFID simulation device?
- Speed: how many RFID tags may be read per second?

4.2.Compatibility

Compatibility refers to two possible states, either forwards compatibility or backwards compatibility.

- Forwards: given a vendor who has implemented a RFID solution prior to the authentication model being implemented, would the old implemented system be capable of reading the new model RFID tags without unreasonable modification.
- Backwards: given a vendor who implements a RFID solution after the implementation of the authentication model, would it still be capable of reading old RFID tags that have not implemented the new authentication model.

Under either circumstance of compatibility, authentication is not possible. The hardware or firmware required to perform authentication activities would not be present. The implemented system would only be able to identify the RFID tag being queried and not authenticate it.

4.3. Stage most affected by change

This refers to the stage of production, design or manufacture, which would be most affected, in terms of time, should the authentication model become standard.

4.4. Change required from base technology

This refers to the change that is required by the new model with respect to the reader / writer devices and the RFID tag itself. The categories by which these will be laid out are as follows. “Significant” - a major change would be incurred. “Some” - a degree of change is necessary. “Minor” - a small addition either of a circuit or programming would be incurred. And finally “None” - no change to the tag or reader would be incurred at all.

5. Analysis

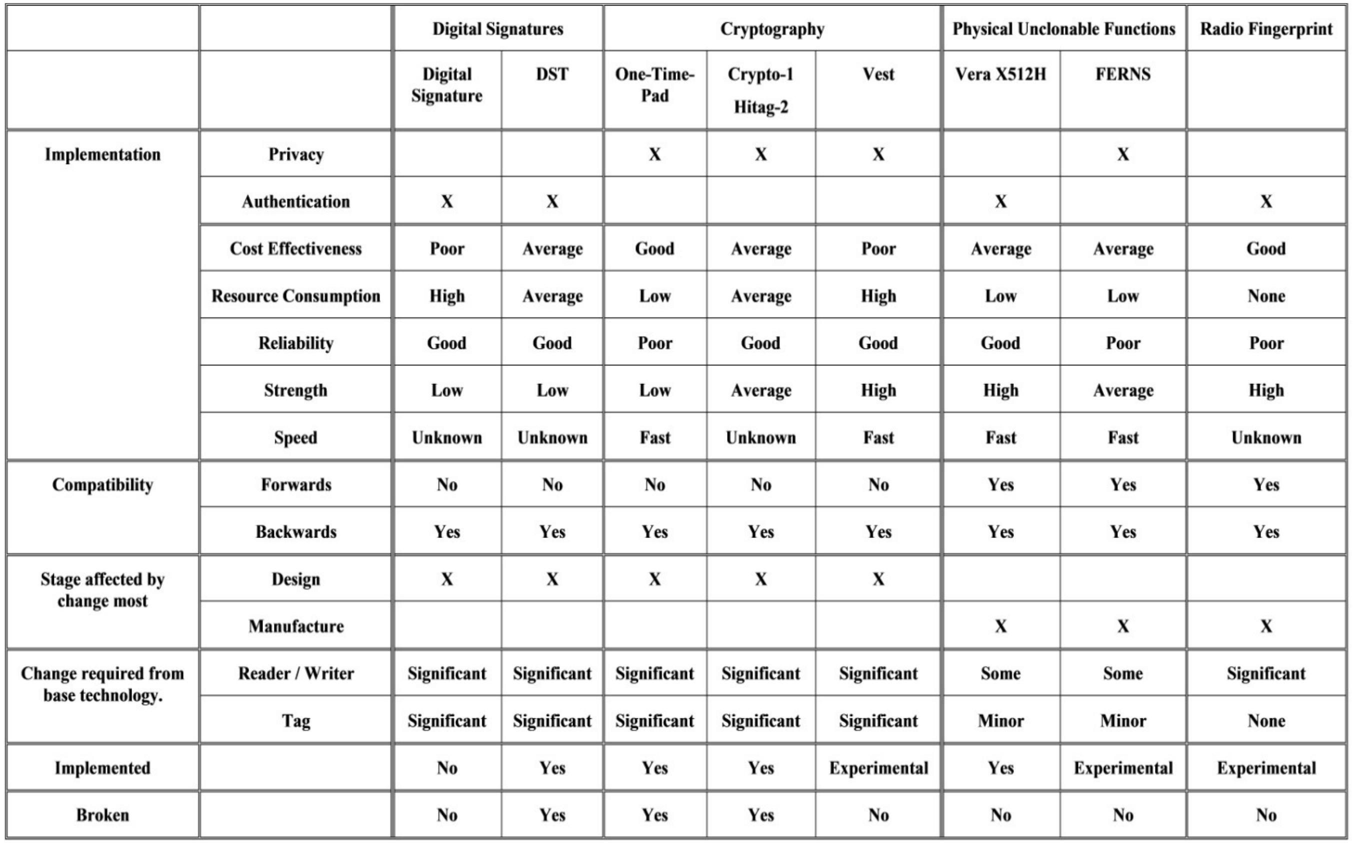
The analysis of Table 1 briefly highlights issues that stem from the traditional and recent approaches to authentication in passive RFID tags.

Traditional: Both *digital signatures* and *cryptography*, save for the *one-time-pad*, have a fairly high cost in terms of resources within the RFID tag. The lack of resources available in passive RFID tags has lead to all the traditional forms of authenticating RFID tags having been broken. To add the necessary resources would increase the cost of the tags beyond the reasonable point. These approaches are clearly not suited to authentication of passive RFID tags.

Next, a critical analysis is performed of more recent approaches.

Recent: *PUF*’s and *Radio Fingerprinting* (RFF) are both the result of inherent, unintentional characteristics within the circuitry caused as a result of the manufacturing process. PUF’s rely on a digital state to generate their fingerprints and would require a small additional circuit built into the RFID tag to monitor and measure these functions. RFF would require no additional circuitry on the RFID tag itself, but requires a greater addition to the reader, neither of which affects the current operation of a RFID tag, rather extending it. This ensures both *forwards-* and *backwards- compatibility.* Neither PUF’s nor RFF are reported to have been broken, which would indicate a high level of resilience against

Table 1. Comparison of discussed authentication models.



		Digital Signatures		Cryptography			Physical Unclonable Functions		Radio Fingerprint
		Digital Signature	DST	One-Time-Pad	Crypto-1 Hitag-2	Vest	Vera X512H	FERNS	
Implementation	Privacy			X	X	X		X	
	Authentication	X	X				X		X
	Cost Effectiveness	Poor	Average	Good	Average	Poor	Average	Average	Good
	Resource Consumption	High	Average	Low	Average	High	Low	Low	None
	Reliability	Good	Good	Poor	Good	Good	Good	Poor	Poor
	Strength	Low	Low	Low	Average	High	High	Average	High
	Speed	Unknown	Unknown	Fast	Unknown	Fast	Fast	Fast	Unknown
Compatibility	Forwards	No	No	No	No	No	Yes	Yes	Yes
	Backwards	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Stage affected by change most	Design	X	X	X	X	X			
	Manufacture						X	X	X
Change required from base technology.	Reader / Writer	Significant	Significant	Significant	Significant	Significant	Some	Some	Significant
	Tag	Significant	Significant	Significant	Significant	Significant	Minor	Minor	None
Implemented		No	Yes	Yes	Yes	Experimental	Yes	Experimental	Experimental
Broken		No	Yes	Yes	Yes	No	No	No	No

attack. Evidence of this resilience lies in that there is no published report about current implementations, of these technologies being broken. This makes them good candidates for authenticating resource constrained passive RFID tags. To refer back to the definitions differentiating *privacy* from *authentication*, it becomes obvious as to why PUF and RFF technology is better suited to authentication as opposed to privacy. At no point in time do these technologies perform any cryptographic or other data obscuring operations, except, as in the case of PUF, on the authentication data itself.

Next, the proposed requirements for an authentication model for passive RFID tags are laid out.

6. Requirements for Passive RFID Authentication

To supply the definition of authentication again: Authentication is defined as the process of verifying the authenticity of the RFID tag [6]. The focus of this paper has been specifically on *product authentication* with regards to passive RFID tags.The following requirements are now proposed, which match and extend the definition of authentication as given in Section 3:

- Resource consumption: the approach should not rely overly much on the resources provided by the passive RFID tag, these are few and costly.
- Strength: should be such that the attacker needs put a substantial amount of effort towards breaking the approach, making it not worth their while. The approach should also consider that an attacker may not have limited time with a captured passive RFID tag.
- Speed: in today’s fast paced lifestyle, seconds matter, anything too slow, becomes cumbersome to use, and oft times finds itself discarded on the wayside.
- Reliability: read errors, false negatives and false positives breed frustration for the end user and should be limited.
- Cost effectiveness: the approach should be such that RFID remains a feasible solution, especially for product authentication in which the number of passive RFID tags is no longer trivial.

- Compatibility: the aim of a new approach should be of maintaining functional compatibility with existing systems. Instead of changing technology, the new approach should extend current technology. Thereby including markets with previous systems without forcing a change.
- Stage of production: to minimize cost and contact time with the manufacturers, the stage affected most by implementing an approach should ideally be the design stage.

The authors believe that PUF's are a viable model for use in authenticating passive RFID tags. PUF's meet most of the requirements as laid out above. However, the very nature of the unpredictability of a PUF should be cause for concern. The entire set of possible CRP's cannot possibly be stored and the single-use policy of a CRP indicates that a periodic update would be necessary to avoid re-using a CRP. Future research would need to discover a way of avoiding this inconvenience. Next, the conclusion of this paper.

7. Conclusion

This paper introduces the problem of authentication in a resource constrained environment, such as passive RFID tags, providing background and examples. It then discusses four broad models and several implementations of these models in order to uncover issues involved with authenticating passive RFID tags. After this discussion this paper performs a critical analysis of the implementations, the results of which are tabulated and highlighted. The main contribution of this paper is that it identifies a set of requirements that a passive RFID tag should implement when considering authentication.

Future research will be performed in order to identify an approach to passive RFID authentication whose nature is predictable and controllable, without the need to be measured, that meets the requirements set out in this paper.

Bibliography

[1] Weis, S. A. (2006). RFID (Radio Frequency Identification): Principles and Applications.

[2] Trossen Robotics. (Accessed 16/04/2009). RFID Catalogue Home. http://www.trossenrobotics.com/store/c/2784-RFID.aspx.

[3] RFIDIOt. (2008). http://rfididiot.org/.

[4] www.gadgettastic.com. (2008). rfid_passport. http://www.gadgettastic.com/wp-content/2008/08/rfid_passport.jpg.

[5] Williams, D. H. (2004). RFID - Hot Technology with wide ranging applications.

[6] Office of Information Dissemination Program Development Service. (2005). Authentication. Washington, D.C.: U.S. Government Printing Office.

[7] Soon, T. J., & Tieyan, L. (2008). RFID Security. Information Technology Standards Committee.

[8] Brainard, J., Juels, A., Rivest, R. L., Szydlo, M., & Yung, M. (2007). Fourth-Factor Authentication: Somebody You Know.

[9] Arx. (2009). Digital Signatures FAQ. http://www.arx.com/digital-signatures-faq.php.

[10] Texas Instruments Incorporated. (2006). Increasing Security in the Supply Chain with Electronic Security Markers.

[11] Texas Instruments Incorporated. (2005). Securing the Pharmacutical Supply Chain with RFID and Public-key infrastructure (PKI) Technologies.

[12] Bono, S. C., Green, M., Stubblefield, A., Juels, A., Rubin, A. D., & Szydlo, M. (2005). Security Analysis of a Cryptographically-Enabled.

[13] Blaze, M., Diffie, W., Rivest, R. L., Schneier, B., Shimomura, T., Thompson, E., et al. (1996). Minimal Key Lengths for Symetric Ciphers to Provide Adequate Commercial Security. http://www.crypto.com/papers/keylength.txt.

[14] Department of Commerce. (2005). Announcing Approval of the Withdrawal of Federal Information Processing Standard (FIPS)46-3, Data Encryption Standard (DES); FIPS 74, Guidlines for Implementing and Using the NBS Data Encryption Standard and FIPS 81, DES Modes of Operation. In N. I. Technology, Fedeal Register (Vol. 70).

[15] National Institute of Standards and Technology. (2001). Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards.

[16] EPCglobal Inc. (2008). EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz Version 1.2.0.

[17] Garcia, F. D., de Koning Gans, G., Muijrers, R., van Rossum, P., Verdult, R., Wichers Schreur, R., et al. (2008). Dismantling MIFARE Classic. Nijmegen: Radboud Universiteit Nijmegen.

[18] O'Neil, S., Gittins, B., & Landman, H. A. (2006). VEST Ciphers (eStream Phase 2). www.vestciphers.com.

[19] Synaptic Laboritories Limited. (2007). VEST Enhanced Smart Cards. www.vestciphers.com.

[20] Jain, V. (2006). Radio Frrequency Identification: The Current and Future Solutions for Privacy and Authentication.

[21] Radio Comms. (2008). Electronic DNA enables unclonable RFID chips. http://www.radiocomms.com.au/articles/27871-Electronic-DNA-enables-unclonable-RFID-chips.

[22] Nohl, K. (2008). Bold Security Claims about PUFs on RFID.

[23] Verayo. (2008). Vera X512H Unclonable RFID IC.

[24] RFID Journal. (2008). PUF Technology Catches Clones.

[25] Verayo. (2009). Physical Unclonable Functions: Performance and reliability. http://www.verayo.com/technology/technology.html.

[26] Gassend, B., Clarke, D., van Dijk, M., & Devadas, S. (2002). Silicon Physical Random Functions. Computer and Communication Security Conference.

[27] Gassend, B., Lim, D., Clarke, D., van Dijk, M., & Devadas, S. (2004). Identification and authentication of integrated circuits.

[28] Suh, G. E., & Devadas, S. (2007). Physical Unclonable Functions for Device Authentications and Secret Key Generation.

[29] Holcomb, D. E., Bureson, W. P., & Fu, K. (2007). Initial SRAM state as a Fingerprint and Source of True Random Numbers for RFID tags.

[30] Franklin, J. e. (2006). Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting.

[31] Gerdes, R. M., Daniels, T. E., & Russell, S. F. (2006). Device Identification via Analog Signal Fingerprinting.

[32] Hall, J., Barbeau, M., & Kranakis, E. (2003). Detection of Transient in Radio Frequency Fingerprinting Using Signal Phase.

[33] Clarke, J. B. (2006). RADIO FREQUENCY FINGERPRINTING TO DETECT FRAUDULENT RADIO FREQUENCY IDENTIFICATION TAGS. http://www.wipo.int/pctdb/images4/PCT-PAGES/2006/322006/06083468/06083468.pdf.

[34] Ellis, K. J., & Serinken, N. (2001). Characteristics of radio transmitter fingerprints.