RFID Security and Privacy: Threats and Countermeasures

Marco Spruit
Wouter Wester

Technical Report UU-CS- 2013-001
January 2013

Department of Information and Computing Sciences
Utrecht University, Utrecht, The Netherlands
www.cs.uu.nl

ISSN: 0924-3275

Department of Information and Computing Sciences
Utrecht University
P.O. Box 80.089
3508 TB Utrecht
The Netherlands

RFID SECURITY AND PRIVACY: THREATS AND COUNTERMEASURES

Marco Spruit, Utrecht University, Princetonplein 5, 3584 CC, The Netherlands, m.r.spruit@uu.nl

Wouter Wester, Utrecht University, Princetonplein 5, 3584 CC, The Netherlands

Abstract

The vulnerability of Radio Frequency Identification (RFID) and the objection of consumers to buy products that include non-protected RFID are holding organizations back from investing in this promising technology. Information security and privacy are therefore important academic research areas. This research presents the RFID Threat Countermeasure Framework (RTCF) to better understand the wide range of RFID threats and their corresponding protection countermeasures. We conclude that RFID security and privacy developments are very promising but do require more development iterations to become practically useful for organizations.

Keywords: Infrastructure protection, Wireless sensor networks, Logistics, Unauthorized access.

1 Introduction: from barcodes to radio waves

Physical object identification has become increasingly more important as trade and transport markets have grown. The first automatic identifier for products, which is still used on a large scale today, was the barcode. Barcodes however have their flaws, such as the need to align the barcode with the scanner and being able to only scan one product at a time. Better auto-ID systems have therefore been in continuous development. A well-known auto-ID system that lacks the before mentioned flaws is Radio Frequency Identification (RFID). RFID technology, which uses radio waves in order to identify or track a small chip (RFID tag) that is attached to a physical object, is envisioned as a replacement for its barcode counterpart and expected to be massively deployed in the coming years. Currently RFID is already being deployed in various applications and scenarios, such as automated payment and physical access control. Promising future and large scale RFID applications include asset tracking, monitoring supply chains, and inventory control.

Security and privacy aspects related to RFID are, however, gaining significant importance as the absence of good security and privacy is partially responsible for holding back the large scale implementations that are required for the previously mentioned RFID applications. Because RFID is a wireless system without any standard security controls, tags can be read, modified, manipulated, or disabled without physical, and therefore noticeable, contact. The privacy issues have been frequently hyped in the media by certain individuals and groups that are against the use of RFID, in particular in consumer products, as they expect it to violate their privacy. Their primary concern is that RFID tags are not disabled after purchase and can therefore still be scanned and read for unwanted purposes such as obtaining sensitive personal data or locating and tracking persons. Although the primary focus of RFID issues is on privacy, companies that use RFID have to be aware of security as well. Unprotected RFID tags can be scanned to obtain company sensitive information and locate valuable products, but can also be disabled to easily steal products or sabotage company supply chains.

Lately researchers have been trying to find ways to prevent these RFID security and privacy threats. Most of the published academic papers on protection capabilities for RFID are independent studies, each presenting new security and/or privacy techniques with unique abilities. These independent studies are, however, not very useful for organizations to determine which threats exist for their RFID implementation and how these threats need to be countered. We have therefore analyzed a large sample of academic papers from which we have selected the most common RFID threats. For each RFID threat we have identified all protection capabilities that are able to counter the threat in order to create a classification framework.

Although there have been other classifications of RFID threats, these classifications do not include the possible security and privacy measures that can counter these threats. Additionally there has been very limited research in how these threats relate to the risk management of organizations, which is required to determine which and how risks are to be countered. This paper provides an overview of the impacts of the well-known privacy and security threats in wireless RFID communication and how the latest developments in protection capability research can counter these threats.

2 Key concepts in security & privacy research

Information security and information privacy are, in relation to RFID, focused on protecting the data that is located on the tag or being transmitted from or to the tag. Valuable data from the RFID system needs to be protected from being read, modified, manipulated, or disabled. For over twenty years the *Confidentiality, Integrity and Availability (CIA)* triad has been the standard for information security and information privacy. These three principles are used in this paper to determine the impact of the RFID threats and are described in more detail below.

Confidentiality: the state that information assets are accessible or usable by unauthorized individuals, entities, or processes. A breach of confidentiality will occur in case an unauthorized individual, entity or process is able to access the information assets. The results of a breach in confidentiality could result in a loss of public confidence, embarrassment, or legal action against an organization.

Integrity: the property of safeguarding the accuracy and completeness of information assets. Information assets should not be able to be changed by unauthorized individuals or entities. A loss of system or data integrity could lead to inaccuracy, fraud, or erroneous decisions. A violation of integrity may be the first step in a successful attack against system availability or confidentiality.

Availability: the property of information assets being accessible and usable by authorized individuals and entities. Unauthorized individuals or entities should not be able to prevent authorized individuals and entities from accessing the required information.

3 RFID Threats

Over the years researchers have identified many different types of threats that could affect RFID implementations. Through a systematic literature review we have identified the *Top 6* RFID-related threats based on a study of twenty-four academic papers that are focused on RFID threats and protection. Each different type of threat has been identified and the number of references in different papers has been counted. The results of this can be seen in Figure 1. The top five threats have been selected from the created list. The other threats are either not mentioned frequently enough or are too similar to one of the already selected threats. In the end the selected five threats form a representative mix of the different types of threats. In addition, we have split eavesdropping into two different types of threats to better differentiate between possible protection measures. The next sections elaborate on the selected threats: eavesdropping to read data, eavesdropping on the transmission, spoofing, tracking, and cloning.

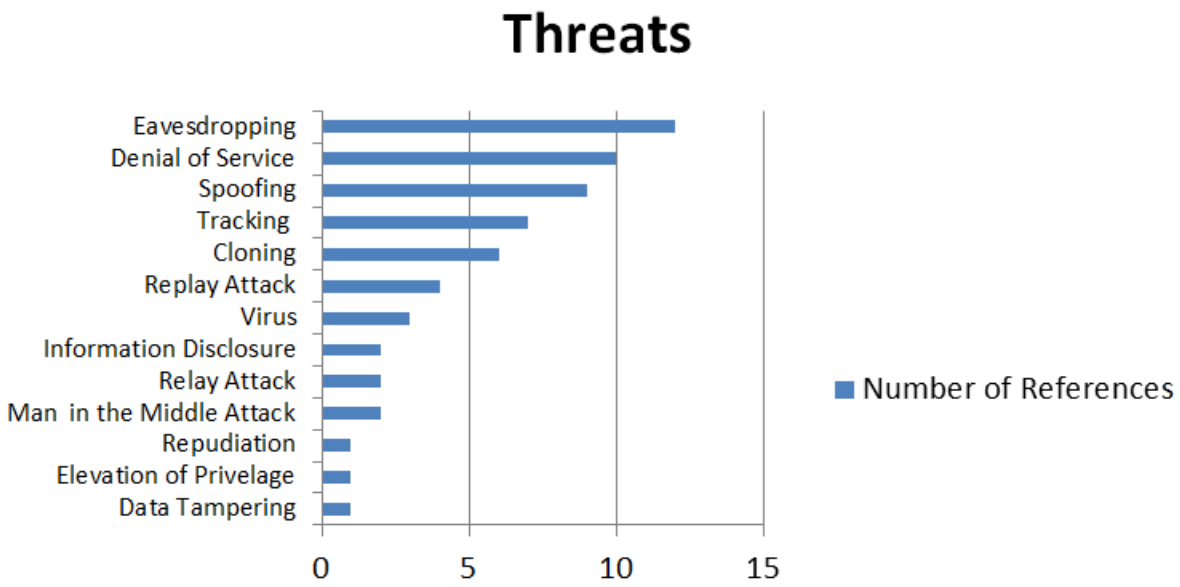

Figure 1: Number of appearances of each RFID threat in our selection of twenty-four academic papers.

3.1 Eavesdropping - Reading of Data

Eavesdropping, which is also known as *skimming*, is the unauthorized listening of the wireless communication between a RFID tag and reader (Soon & Tieyan, 2008). With radio receiving

equipment one can monitor or record the data that is being sent back and forth between that tag and reader. Eavesdropping in general is performed to read the data that is being transmitted. This means that what is being broadcasted by the RFID system can actually be translated by the eavesdroppers into understandable information. Eavesdropping is easy when the data is not protected and eventually allows for other threats to take place.

3.2 Eavesdropping - Reading of the Transmission

Unfortunately eavesdropping can still take place once data is actually protected. In order to avoid confusion we decided to split eavesdropping in reading of data as well as reading of the transmission. Reading of the transmission still allows for correlation of the tag to a particular person or object and thereby identifying or eventually even track that object or person. However tracking is considered as a separate threat.

3.3 Spoofing

Spoofing is an attack on the communication between tag and reader. In this type of attack an adversary impersonates a valid RFID tag to gain its privileges (Mitrokotsa, Rieback & Tanenbaum, 2008). To impersonate RFID tags the attackers use special emulating devices with increased functionality to spoof the RFID tags. To successfully perform a spoofing attack, knowledge about the used protocols and authentication secrets has to be known in advance. While impersonating a valid RFID tag, the impersonator can receive and read encrypted messages and also send out false information to the reader and tag if desired (Konidala, Kim & Kim, 2007).

3.4 Denial of Service

Denial of Service (DOS) attacks are aimed at disrupting the communication between tags and readers. One way to achieve a denial of service attack is by having multiple tags or specially designed tags overwhelming a reader's capacity with requests. This will result in the reader being unable to differentiate the different tags, rendering the system inoperative and the legitimate tags useless as they are unable to successfully communicate with the reader (Juels, Rivest & Szydlo, 2003).

3.5 Tracking

Products that are equipped with tags can, and most likely will, end up in the possession of a consumer. With the right encryption, tag data can be protected but still leave the possibility of tracking the tag itself. RFID tags contain an ID code that will enable readers, which have been strategically placed, to uniquely identify single tags or group of tags with personal identities (Rieback, Crispo & Tanenbaum, 2006a). Once a specific tag or a set of tags can be associated with a particular person, the mere presence of this tag in a particular reader field already implies a (most likely unwanted) location disclosure. Combining several such sightings across multiple logs can easily track a person over longer periods of time (Langheinrich, 2007).

3.6 Cloning

Cloning is a threat frequently categorized together with spoofing. However spoofing and cloning are not the same. Although both threats copy data from a legitimate tag, spoofing emulates the transmission of tag data while cloning means that the copied data is transferred onto a new tag owned by the attacker. Just as spoofing, the communication between legit RFID tags and readers will have to be read and stored, but a tag could also be stolen and then physically read. The data for the cloned tags

are then altered to suit to the needs of the desired attack and copied onto an empty tag. The cloned tag is then inserted into a RFID system to perform the planned attack (Soon & Tieyan, 2008).

4 RFID Protection Capabilities

In this section we present the protection capabilities for RFID threats. Similar to our overview of RFID threats above, we also created an overview of all the protection capabilities in the twenty-four academic papers. The result can be seen in Figure 2. We have included all protection capabilities. Next, the protection measures are divided in two groups: cryptographic algorithms and non-cryptographic schemes. The non-cryptographic schemes that have been selected are: tag killing, tag locking, faraday cage, blocker tag, and the RFID guardian. The cryptographic algorithms that are described are: rewritable memory, public key encryption, hash lock, randomized hash lock, hash-chain scheme, pseudonym throttling, and delegation tree authentication.

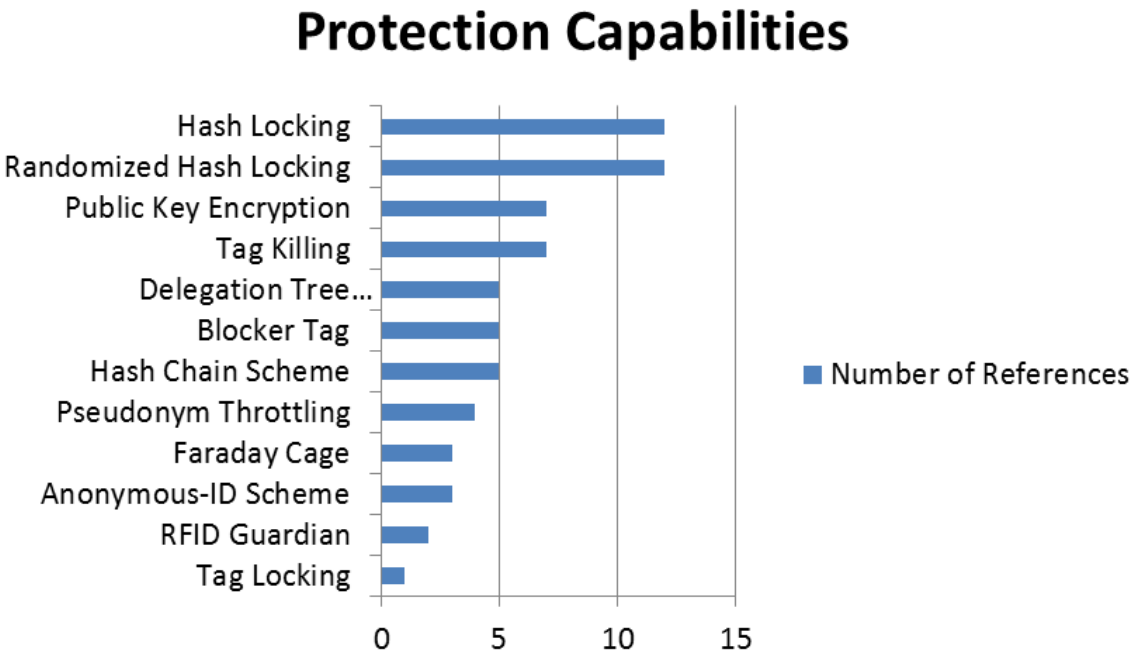

Figure 2: Number of appearances of each RFID protection capability in our selection of twenty-four academic papers.

4.1 Tag Killing

KILL is a feature designed to protect consumer privacy by allowing tags to be disabled at the point of sale in retail environments (Koscher, Juels, Brajkovic & Kohno, 2009). The KILL command, which is currently only available on the a few tag types, is initiated by entering a PIN number. When the PIN number is entered all information on the RFID tag is destroyed, ensuring that the privacy of the customer is protected. The tag will be permanently deactivated and rendered useless for post-purchase benefits for companies and consumers. The PIN code should however be well protected so it cannot be used by attackers to destroy the tags when they still need to be used.

4.2 Tag Locking

Tag locking needs to be activated by a PIN number, just like the KILL feature of the EPC tags (Rieback, Crispo & Tanenbaum, 2006b). Once this PIN number is entered the RFID tag enters a

locked mode where it will still reply by sending its ID number but not the data stored on the tag. However this does still enable a person to be tracked by correlating the locations where the particular ID is read. By entering the PIN number again the tag will be reactivated and able to send its data. The PIN code should be well protected just like the PIN number of the KILL command.

4.3 Faraday Cage

The principle of a faraday cage is to use a metal mesh (for example made of aluminum foil), that is impenetrable for incoming or outgoing radio waves, to prevent communication with RFID devices (Juels *et al.*, 2003). By placing metal meshes around tagged objects, the RFID tag, and thus the identity of the object, will be protected from reading by RFID readers. However RFID attackers could use the principle of the faraday cage to shield stolen items from being scanned by readers and therefore sneak out the products without setting off the alarm.

4.4 Blocker Tag

The Blocker Tag scheme is intended for consumer privacy and uses a RFID tag to block the communication between other RFID tags and RFID readers. A consumer carrying a blocker tag induces a physical region where a reader would be incapable of communicating with the 'hidden' tags selected by the consumer. When a RFID reader would send a request, the blocker tag responds with a fake message by simulating the full spectrum of possible serial numbers for tags, thus preventing the reader from obtaining the true serial number of the tag (Juels *et al.*, 2003). This method can prevent consumers from being tracked and will block harmful attacks. The responsibility of the tag protection is however placed on the consumer. It is however possible to change the blocker tags so that it can be used maliciously (Mitrokotsa *et al.*, 2008).

4.5 RFID Guardian

The RFID Guardian is a battery powered device that looks for, records, and displays all RFID tags that it has scanned in the vicinity, manages RFID keys, authenticates nearby RFID readers, and blocks attempted accesses to the user's RFID tags from unauthorized readers (Rieback, Crispo & Tanenbaum, 2005). So unlike the blocker tag, the RFID Guardian allows for greater customization of the tag access by authorized readers. Just as the blocker tag the RFID guardian has to be carried around for personal use. Although it was initially designed for personal use, company use is possible as well. The device is however also usable to fool RFID systems (Mitrokotsa *et al.*, 2008).

4.6 Anonymous-ID Scheme

The anonymous-ID scheme uses an encrypted ID which is stored on the tag (Kinoshita, Hoshino, Komuro, Fujimura & Ookubo, 2003). This prevents an attacker from knowing the real tag ID. The encryption of the real ID of the tag could be a symmetric key encryption, which uses an encryption key to encrypt and decrypt a message, or a linked random value. This scheme alone will prevent the leaking of private consumer data, but not the tracking of a consumer. To prevent the tracking of a consumer the anonymous ID stored in the tag must be refreshed as frequently as possible by external re-encryption. The idea behind re-encryption is that a dedicated reader obtains the encrypted ID from the tag's memory and overwrites the old encrypted ID with a new encryption of the ID (Ohkubo, Suzuki & Kinoshita, 2005). Using this encryption scheme would however require the use of more expensive rewritable tags and consumer involvement.

4.7 Public Key Re-Encryption

In public key cryptography a device taking part in the communication has a pair of keys, a public key and a private key, and a set of operations associated with the keys to execute the cryptographic operations on the communication messages. RFID tags and readers are in this case the communication devices that are equipped with private and public keys, respectively. The encrypted messages would prevent the unauthorized reading of the RFID. Additionally this approach uses re-encryption, just as the anonymous-ID scheme, to improve consumer privacy by changing the public keys of the RFID tags so that the consumer cannot be tracked by the public key that is located on a particular tag (Golle, Jakobsson, Juels & Syverson, 2004).

4.8 Hash Lock

The Hash Lock encryption scheme is designed to fit on the tags that have only little memory available (Weis, 2003). Each of the hash-enabled tags will operate in a locked or unlocked stage and has a small amount of its memory reserved for a temporary hash encrypted ID. In the locked stage the broadcasted data is no longer readable to eavesdroppers. The advantage of using the hash lock scheme is the ability to allow multiple users assume control or change the tag functionality. This is especially useful in supply chains where the tags are passed on between companies. Unfortunately the tags still transmit their ID's while in the locked state meaning that the ID's could be used as a tag identifier and therefore be tracked.

4.9 Randomized Hash Lock

The randomized hash lock scheme has the same functionality as the hash lock scheme but it also has an added pseudo-random number generator function that helps prevent the tag from being tracked. The pseudo-random number generator adds an additional random encrypted factor into the mix that allows for a variation in the transmission of the ID of a single tag. The random ID's are brute force checked in the database which stores all the random numbers. Once a match is found, the reader can unlock the tag by sending the ID value (Golle *et al.*, 2004). Owners of huge number of tags, who require read rates of 100 to 200 tags per second, might be better of employing a regular hash lock. This is because the brute force searches of the randomized hash lock scheme costs a lot of time and will significantly lower the efficiency of the RFID processes.

4.10 Hash-Chain Scheme

The goals of the hash-chain scheme are to keep complete user privacy, eliminate the need for extraneous rewrites of the tag information, minimize the tag cost, eliminate the need for high power of computing units, and provide forward security (Yao, Qi, Han, Zhao, Li & Liu, 2009). The idea behind the hash-chain scheme is that it enables key-updating by using two hash functions. After each authentication the tag computes the old key's hash value as the new key (Yao *et al.*, 2009). Due to the one-way property of hash function, attackers cannot recover the old keys even if obtaining the current key. Locating two hash encryptions on a tag can however be difficult as it will slow down the tag read rate and require double the amount of the on tag storage capacity.

4.11 Pseudonym Throttling

Pseudonym throttling is a pseudonym authentication scheme where an RFID tag only stores a short list of pseudonyms (Juels, 2004). Each time the tag is queried the RFID tag will broadcast the next pseudonym in the list. Once the list of pseudonyms is exhausted the tag switches to the beginning of the list. The reader receives a pseudonym and checks it with the list of all known pseudonyms that are

linked to tags until it finds the right tag ID associated with received pseudonym. The tag is authenticated once the ID is found. Pseudonym throttling is a practical and simple approach for RFID-tag authentication, but has a shortcoming: The small list of pseudonyms due to the small storage capacity will limit the privacy protection. An extension of this scheme allows the pseudonyms to be refreshed by authorized verifiers and therefore make the tag untraceable. These tags will however need to be rewritable to allow this extra function.

4.12 Delegation Tree Authentication

Delegation Tree authentication is an improved algorithm based on a shared secret and a pseudo-random function (Molnar, Soppera & Wagner, 2005). The main idea is to use a RFID pseudonym scheme and to use a Trusted Center which is connected with the RFID readers. The Trusted Center controls the desired privacy policy and limit which readers may read which tag. When a new tag is enrolled in the system it is provided with a secret key by the Trusted Center. The Trusted Center keeps a tree structure of the secret keys, tag information and the tag privacy policy listed in a database.

5 Evaluating RFID Threat Impacts and Countermeasures

In order to implement certain security or privacy measures, organizations use risk management to calculate the risk before determining which security and privacy measures will be required. Calculating the risk involves the activities of assessing the threats and the impact of these threats to the organization, the vulnerability of the organization and the likelihood that the threat will occur. Organizational vulnerability and the likelihood of a threat are both dependable on the organization and the type of RFID system that is being used. Impacts of a threat can however be related to the three principles of the CIA triad, as the impacts will remain the same for each organization and RFID implementation. In this section we will present the impact of each threat and which countermeasure can be used for a threat.

We have interviewed eight experts, with relevant knowledge in the field of security and privacy and RFID, to validate our results. Our goal was to validate the selected threats and protection capabilities, the relationships made between them, and the threats linked to the CIA principles. From the interviews we could conclude that the first results were very accurate. With some minor adjustments to our findings we are able to present the final validated results as shown in Figures 3 and 4. A description of the interviewed experts is given in Table 1.

Expert #	*Function*	*Affiliation*	*Knowledge/Experience*
Expert #1	Security Manager	Consultancy Multinational	Theoretical background of RFID. Security expert.
Expert #2	Senior Architect	Consultancy Multinational	Eight years working experience with RFID.
Expert #3	Security Manager	Consultancy Multinational	Extensive experience with the security concepts of CIA, threat, vulnerability and risk assessments.
Expert #4	Security Consultant	Consultancy Multinational	Basic knowledge on RFID. Several years of work experience with cryptography.
Expert #5	Security Manager	Supply Chain Consulting	Extensive knowledge on RFID and security.
Expert #6	Manager Information Security	Consultancy Multinational	Experience and knowledge on cryptography and risk management.
Expert #7	Manager Information Security	Consultancy Multinational	Specialization in cryptography. Several IS security certifications.
Expert #8	Principle Consultant	Software Multinational	RFID blogger.

Table 1: Eight experts validated the selection of threats and protection capabilities and their relationships.

5.1 Impacts of RFID Threats

By comparing the effects of RFID threats with the three principles of the CIA triad we are able to create an overview that allows an organization to quickly determine which threats will need to be countered. This can be done once an organization has decided which of the CIA principles are of importance to the RFID system that it has in use, and will need to be protected. Figure 3 shows the results of the comparison we performed.

Eavesdropping will only breach a entity's Confidentiality, as it will only read the information or senses that communication is taking place. It will not alter or block access to that information. Spoofing and cloning both are able to read the information as well as alter the information, which will lead to a breach of the confidentiality and integrity of the RFID data. Denial of service is a threat that will try to block any communication between tag and reader and thus hamper the availability of the data. Tracking is, in short, performed by continuously performing eavesdropping attacks. The location of the tag, which is supposed to be confidential and private, is thereby revealed. Confidentiality is therefore lost by tracking.

	CIA principles		
RFID Threats	Confidentiality	Integrity	Availability
Eavesdropping Data	X		
Eavesdropping Transmission	X		
Spoofing	X	X	
Cloning	X	X	
Denial of Service			X
Tracking	X		

Table 2: Impact of the Top 6 RFID threats on the CIA principles. Each relation indicates a negative influence.

5.2 Selecting Countermeasures: The RFID Threat Countermeasure Framework

Once an organization has determined which threats need to be countered it is important to analyze the countermeasures that are available that can actually counter that particular threat. By assessing the academic research on the protection capabilities we were able to create an overview that shows which cryptographic or non-cryptographic protection capabilities can counter which threats. This overview is presented as the RFID Threat Countermeasure Framework (RTCF) in Figure 4.

What instantly becomes clear from observing Figure 4 is that non-cryptographic protection capabilities are much more efficient against RFID threats. However, these non-cryptographic protection capabilities are limited in the way in which they can be applied. Cryptographic protection on the tags would allow for greater flexibility of security and privacy while the tag is passed on between different owners. Finally, note that none of the selected cryptographic protocols is, unfortunately, able to counter all threats in itself.

	Countermeasures											
	Cryptographic							Non-cryptographic				
RFID Threats	Anonymous-ID Scheme	Public Key (Re-) Encryption	Hash Lock	Randomized Hash Lock	Hash-Chain Scheme	Pseudonym Throttling	Delegation Tree Authentication	Tag Killing	Tag Locking	Faraday Cage	Blocker Tag	RFID Guardian
Eavesdropping Data	X	X	X	X	X	X	X	X	X	X	X	X
Eavesdropping Transmission								X		X	X	X
Spoofing	X	X	X	X	X	X	X	X	X	X	X	X
Cloning	X	X			X	X	X	X	X	X	X	X
Denial of Service								X		X	X	X
Tracking	X	X		X	X	X		X		X	X	X

Table 3: The RFID Threat Countermeasure Framework (RTCF) maps RFID threats to their corresponding protection countermeasures.

6 Conclusions and Discussion

Due to the increasing number of RFID implementations, RFID security and privacy are increasingly gaining more importance. Unfortunately the wireless RFID communication is vulnerable for attacks, which contributes to the delay of mass RFID adoption. Although RFID is becoming more standardized, the current protection capabilities still lack in their abilities to counter or prevent RFID threats and therefore gain acceptance in the commercial sector. But as RFID technology keeps improving, security and privacy effectiveness will also grow. In the end it will take time for protection capabilities to become more standardized and be implemented as part of a RFID system. The progress that academics like us are making made today will assure that, once RFID is being implemented on a large scale, we all can trust the security and privacy of the RFID tags that are embedded in the products we buy. This research contributes the RFID Threat Countermeasure Framework (RTCF) to help achieve this strategic goal.

This research opens many new opportunities for further research. In closing this paper we would like to point out three promising venues to pursue in a follow-up investigation. First, the RFID Threat Countermeasure Framework (RTCF) could easily be expanded with additional threats and protection capabilities to allow for a greater overview that might be needed in the daily practice of a security department. Some examples given by Expert #5 during the validation phase are elevation of privilege, repudiation, and the RFID virus or worm. Second, a more technical research could be performed to test the actual protection capabilities against the threats and thereby determining how effective each protection capability is in daily practice. Third, Expert #6 commented that it would be very interesting to find out what exactly could be done about the downsides of the non-cryptographic protection capabilities. If these cons could be prevented, the applicability of the non-cryptographic options would be greatly increased.

References

Golle, P., Jakobsson, M., Juels, A., Syverson, P. (2004). Universal Re-encryption for Mixnets**.** In Okamoto, T. (Ed.), RSA Conference Cryptographers' Track '04 (pp. 163-178). Springer-Verlag.

Juels, A. (2004). Minimalist Cryptography for Low-Cost RFID Tags. In Blundo, C. & Cimato, S. (Eds.), The Fourth International Conference on Security in Communication Networks (pp. 149-164). Istanbul: Springer-Verlag.

Juels, A., Rivest, R. L., & Szydlo, M. (2003). The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. Proceedings of the 8th ACM Conference on Computer and Communications Security, ACM Press, 103-111.

Kinoshita, S., Hoshino, F., Komuro, T., Fujimura, A., & Ookubo, M. (2003). Nonidentifiable Anonymous-ID Scheme for RFID Privacy Protection. Joho Shori Gakkai Shinpojiumu Ronbunshu, 2003(15), 497-502.

Konidala, D. M., Kim, W.-S., & Kim, K. (2007). Security Assessment of EPCglobal Architecture Framework. Auto-ID Labs. Retrieved Oktobor 6, 2010, from http://www.autoidlabs.org/uploads/media/AUTOIDLABS-WP-SWNET-017.pdf

Koscher, K., Juels, A., Brajkovic, V., & Kohno, T. (2009). EPC RFID Tag Security Weaknesses and Defenses: Passport Cards, Enhanced Drivers Licenses, and Beyond. Proceedings of the 16th ACM conference on Computer and communications security. ACM Press, 33-42.

Langheinrich, M. (2007). RFID and Privacy. In M. Petkovic, & W. Jonker (Eds.), Security, Privacy, and Trust in Modern Data Management. (pp. 433-450). Berlin: Springer.

Mitrokotsa, A., Rieback, M. R., & Tanenbaum, A. S. (2008). Classification of RFID Attacks. Proceedings of the 2nd International Workshop on RFID Technology, Citeseer, 73-86.

Molnar, D., Soppera, A., & Wagner, D. (2005). A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags. Lecture Notes in Computer Science, 3897(1), 276-290**.**

Ohkubo, M., Suzuki, K., & Kinoshita, S. (2005). RFID Privacy Issues and Technical Challenges. Communications of the ACM, 48(9), 66-71.

Rieback, M. R., Crispo, B., & Tanenbaum, A. S. (2005). RFID Guardian: A battery-powered mobile device for RFID privacy management. Proceedings of the 10th Australasian Conference on Information Security and Privacy. (ACISP 2005), Springer, 184-194

Rieback, M. R., Crispo, B., & Tanenbaum, A. S. (2006a). Is Your Cat Infected with a Computer Virus? Proceedings of the Fourth Annual IEEE International Conference on Pervasive. IEEE, 169–179.

Rieback, M. R., Crispo, B., & Tanenbaum, A. S. (2006b). The Evolution of RFID Security. Pervasive Computing, 5(1), 62-69.

Soon, T. J., & Tieyan, L. (2008). RFID Security. Synthesis Journal, 33-38.

Weis, S. A. (2003). Security and Privacy in Radio-Frequency Identification Devices. Massachusetts Instute of Technology, Retrieved October 6, 2010, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.2.4785&rep=rep1&type=pdf

Yao, Q., Qi, Y., Han, J., Zhao, J., Li, X., & Liu, Y. (2009). Randomizing RFID Private Authentication. Proceedings of the IEEE International Conference on Pervasive Computing and Communications, IEEE, 1-10.