Analysis of Threats to the Security of CPC Networks

J. G. Alfaro[†,‡], M. Barbeau[†], and E. Kranakis[†]

[†]Carleton University, School of Computer Science
5302 Herzberg Building, 1125 Colonel By Drive
Ottawa, Ontario, K1S 5B6, Canada

[‡] Open University of Catalonia,
Computer Science and Multimedia Studies
Rambla Poble Nou 156, 08018 Barcelona, Spain

E-mail: *joaquin.garcia-alfaro@acm.org,*
barbeau@scs.carleton.ca, kranakis@scs.carleton.ca

Abstract

Detecting and responding to security and privacy threats to Electronic Product Code (EPC) and Radio Frequency IDentification (RFID) technologies are becoming major concerns of information security researchers. However, and before going further in these activities, an evaluation of the threats in terms of importance must be done. We present such an evaluation. Our analysis of the threats is based on a methodology proposed by the European Telecommunications Standards Institute (ETSI). According to this methodology, we rank the threats to EPC networks in order of relevance. This assessment is intended to prioritize threats for future research on appropriate countermeasure mechanisms.

Key words: Network Security; Wireless Security; Electronic Product Code (EPC); Radio frequency identification (RFID); Threats analysis.

1 Introduction

Security and privacy issues on Radio Frequency IDentification (RFID) and Electronic Product Code (EPC) technologies are gaining great importance in information security research. Lots of analysis, studies, and solutions have recently appeared in the related literature [10]. Radio frequency technologies have been used to identify objects and individuals for more than 60 years (e.g., *Identification Friend or Foe Systems* in World War II). It is now that security and privacy concerns on modern applications (e.g., supply chain inventory, health care, animal identification, and electronic passports) are actively being debated and getting attention from consumers and industrial producers. We presented in [1] an evaluation of threats on the exchange of information between RFID interrogators and labels on EPC networks. The EPC network architecture is a pervasive infrastructure for the automatic identification of objects on supply and production applications (e.g., supply chain for medical or military applications). It relies on the use of RFID technologies to tag or label objects in motion, and distributed services to provide information about these objects via the Internet. We extend the evaluation presented in [1]. We review the set of threats on the ID service of EPC networks. We evaluate security and privacy threats on the lookup service of the EPC network architecture. The methodology used for our analysis is based on the evaluation of threats proposed by the *European Telecommunications Standards Institute* (ETSI). ETSI proposes in [7] the identification of threats according to their *likelihood* of occurrence, their possible *impact* upon targeted systems, and the *risk* that they represent for such systems. We slightly modify it in order to take into account the suggestions introduced in [4, 11] for identifying relevant threats and security flaws on current wireless network applications.

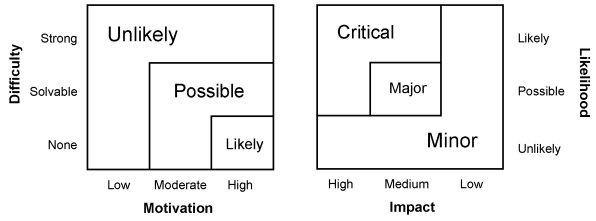
Section 2 outlines the methodology used to conduct our analysis of threats. Section 3 overviews the main properties of the EPC network architecture and presents our evaluation of the threats. Section 4 concludes the paper.

2 Analysis methodology

We define for our work a *threat* as the objective of an attacker in order to violate the security or privacy of a target

system. We define in turn an *attacker* as the specific agent or entity which is going to exploit a given vulnerability at the targeted system in order to manage the threat. The exploitation of such a *vulnerability* is defined in our work as the *attack* that establishes the threat upon the target system. Mitigation mechanisms, often referred in the literature as *countermeasures*, must be established by the security officer of the targeted system in order to reduce or, if possible, prevent, the illegal activity associated with each possible threat. Given the impossibility of applying countermeasures for every possible threat against a system, it is crucial for a security officer to identify those threats that might have a high impact upon the system they are in charge of and, then, guarantee the enforcement of countermeasures. This is indeed the objective of the methodology proposed for our analysis of threats. More specifically, the methodology used in this paper is based on an evaluation framework proposed by ETSI in [7]; but slightly modified in order to take into account the suggestions introduced in [4, 11] for identifying relevant threats and security flaws of current wireless network applications. We present in the sequel the key points of this methodology.

The methodology proposed by ETSI identifies the following categories of threats: *critical*, *major*, and *minor*. These categories depend in turn on the estimated values for the likelihood of occurrence of the threat and its impact upon a given user or system. The authors in [4] pointed out that through their experience with the ETSI methodology, many threats were over-classified. We agree with this observation, and adopt for our work the likelihood and risk functions introduced in [4, 11] in order to focus on truly critical threats.



(a) Likelihood function of a threat. (b) Risk evaluation function.

Figure 1. Likelihood and Risk functions.

We show in Figure 1(a) the likelihood function of a threat that we use in our evaluation. Let us notice that in such a figure the evaluation of the likelihood is based on the following parameters: the *motivation* for an attacker to carry out the attack path associated to the risk; and the *technical difficulties* that must be resolved by the attacker in order to apply such an attack. The three values associated with the likelihood function are the following ones: (1) *likely*, if the targeted user or system is almost assured of being victimized, given a high attacker motivation (e.g., financial gains as a result of selling private information or disrupting network services) and lack of technical difficulties (e.g., a precedent for the attack already exists); (2) *possible*, if the motivation for the attacker is moderate (e.g., limited financial gains) or high, and the technical difficulties are potentially solvable (e.g, the required theoretical and practical knowledge for implementing the attack is available) or there are no technical difficulties and the motivation is moderate; and (3) *unlikely*, in case that there is little motivation for perpetrating the attack (e.g., few or none financial gains for implementing the attack) or if strong technical difficulties must be overcome (e.g, theoretical or practical obstacles for perpetrating the attack). On the other hand, we show in Figure 1(b) the risk of a threat as a function of its likelihood and impact. The impact qualifies the consequences to the victim if a threat is successfully carried out. For our work, we assume that the victim is an EPC network infrastructure serving several users. We identify the following three categories: (1) *low* if the attack results in limited outages (e.g., short duration) and can quickly be repaired without suffering from financial losses; (2) *medium* if the outages are limited in time but might result in some financial losses; (3) *high* if the attack associated with the threat results in outages over a long period of time with a large number of users affected, and potentially accompanied by law violations or substantial financial losses. Taking into consideration these definitions, we establish the rules for managing the three aforementioned risk categories, i.e., critical, major, and minor. Except for the latter one, which typically requires no countermeasures, both major and critical threats need to be handled with appropriate countermeasures. Critical threats should be addressed with the highest priority.

3 EPC/RFID threat analysis

Acclaimed as the successors of today's omnipresent barcodes [10], RFID devices — often referred in the literature as RFID tags — are electronic devices that use radio waves to automatically identify objects or people. These devices may be mainly classified as either active (i.e., the transmission power comes from on-board batteries to respond to RFID readers and/or to broadcast signals) or passive[1] (i.e., the transmission power is directly derived from the signal of the RFID readers). Passive tags are the cheapest RFID devices we may find on the market for RFID supply chain item-level tagging (about 5 U.S. cents a piece in volumes of 100 million, and 7.9 U.S. cents in volumes of 1 million or

[1] A third category, often referred in the literature as semi-passive tags, uses a battery to power on-board microchips, but not to either broadcast signals or respond to RFID readers.

more[2] [13]) and, thus, the main kind of RFID tags used in today's RFID supply chain applications.

The main kind of passive RFID tags used for these applications are known as Electronic Product Code (EPC) tags. EPC tags were designed by the MIT's Auto-ID Center [3] and further developed by EPCglobal Inc. They represent the basis of a distributed architecture often referred in the literature as the EPC network architecture [6]. It is based on a *data-on-network* approach for the automatic identification of objects in motion on supply chain and industrial production applications (among others). By using this paradigm, a globally unique number is assigned to every EPC tag. This unique number is then used to identify objects in motion and get further information about them through Internet based technologies. Hence, the information about an object is not necessarily stored on the RFID tag. It is supplied by distributed servers on the Internet [6]. To do so, EPCglobal proposes a public lookup system for compliant EPC applications, called the Object Name Service (ONS) [6]. The ONS relies in fact on the use of Domain Name System (DNS) technologies.

Let us introduce the components, the flow of information, and the services of the EPC network architecture through the scenario shown in Figure 2. The EPC system of a company A is composed of the following elements: (1) a set T_A of RFID tags; (2) a set R_A of RFID readers; and (3) an EPC application composed of a set of EPC middleware instances (M_A), a set of address managers (A_A), and a set of EPC Information Services (IS_A). Every tag $t \in T_A$ has been assigned a globally unique number used to identify an object in motion within the supply chain of company A. Each reader $r \in R_A$ is strategically placed within the supply chain and reads each tagged object as it passes by its area. Then, it sends the identifier of each tag it reads, together with other additional information, such as timestamps and its location, to a middleware instance $m \in M_A$. This middleware instance controls and integrates the information sent by the different readers and other local infrastructure components, and then forwards it to the appropriate information service $is \in IS_A$ for sharing among authorized trading partners through the Internet. To do so, an address manager instance $a \in A_A$ has published the appropriate domain name to the lookup service associated with the application. Both the ONS and DNS are the components of the lookup service that allow the external application $e \in E$ to find data related to specific EPC tags in T_A, and to request access to the information services in IS_A.

Regarding the different stages of this process, let us split the complete group of threats that we are going to analyze into the following two groups: (1) *ID system threats* targeting the information transaction between RFID tags and readers via wireless connections; and (2) *lookup service threats* targeting the exchange of information during the name resolution process. We present in the sequel an evaluation for each one of these two groups, and rank the resulting list of threats by order of relevance.

[2]Including additional RFID features, especially for security purposes, may increase the total end-cost of these devices up to more than 15 cents.

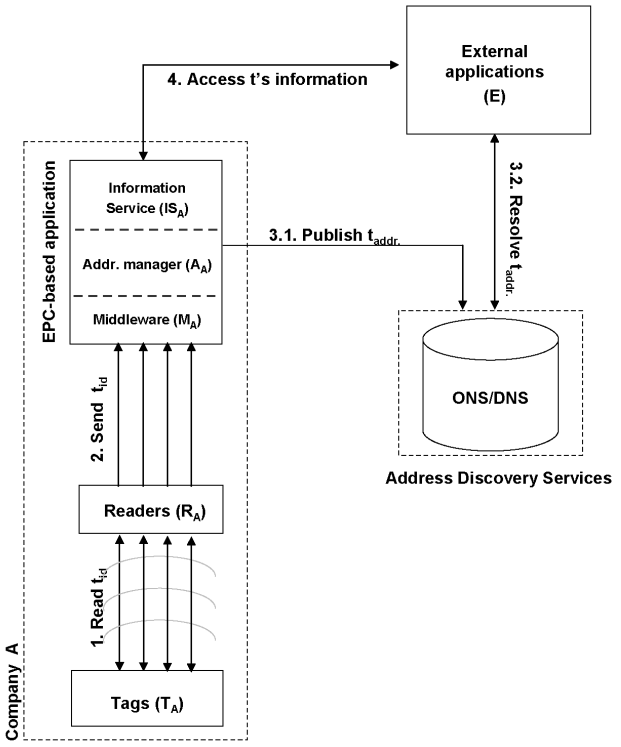


Figure 2. EPC network sample scenario.

3.1 ID system threats

The communication channel between the components of the ID system, i.e., RFID tags and readers, is a, potentially insecure, wireless channel. It is therefore fair to assume that most of the security and privacy threats on EPC based setups are going to target this level. As a result, most of recent publications regarding security and privacy concerns on RFID systems report threats on it. In [14], for example, the authors identify potential threats to commercial supply chains regarding attacks *to* and *by* the ID system of supply chain applications. Their categorization is built on the well-known STRIDE model [9], which is used for the design of secure software systems. The letters in the name STRIDE correspond to the first characters of the following six threat categories [14]: (S)poofing of identities, e.g., a reader $r' \notin R_A$ or a tag $t' \notin T_A$ are placed, respectively, as an authorized reader $r \in R_A$ or tag $t \in T_A$ in the ID system; (T)ampering with data, e.g., loss or corruption of the information stored within tag t, or its transmission to reader r; (R)epudiation, e.g., lack of proof in the ID system to demonstrate that the information stored in t has been transmitted to reader r; (I)nformation

Threat	Objectives			
	Confidentiality	**Integrity**	**Accountability**	**Availability**
Spoofing of identities	X	X	X	X
Tampering with data		X	X	X
Repudiation			X	
Information disclosure	X			
Denial of service				X
Elevation of privilege	X	X	X	X

Table 1. Threats to the security objectives of a system.

disclosure, e.g., illegal disclosure of the data stored within tag t during its transmission to reader r; (D)enial of service, e.g., tag t and/or reader r fail to perform the exchange of information; (E)levation of privilege, e.g., tag t and/or reader r gain higher privileges in the ID system.

We group in Table 1 the security objectives targeted by the threats of STRIDE. Some threats are only targeting a single security objective — the denial of service threat, for example, is only targeting availability — while other threats (e.g., tampering with data) can target more than one objective or even all of them (e.g., spoofing of identities).

We consider threats on the ID system of an EPC network like the one shown in Figure 1. We are interested in threats targeting the main transaction of information at this level, i.e., the exchange of the EPC code assigned to a given tag $t \in T_A$ and read by a given reader $r \in R_A$. We assume moreover that the attacker acts from the outside in order to exploit the insecure communication channel between reader r and tag t, as well as the lack of authentication and/or negotiation between both components. We assume that the attacker does not have physical access neither to the components of the ID system nor to the infrastructure itself. The reason why we do not consider such a physical access is because we presume that other security and privacy mechanism in the company, such as physical access control and surveillance of workers, must apply at this level. The attacker, however, may have access to information about both the ID system infrastructure and its components. Taking into account these assumptions, we summarize in Table 2 the results of our evaluation.

Let us start our evaluation by ranking the motivation and difficulties of the spoofing threat. While the spoofing of a legal tag t into the system may only represent a disruption into the system rather than an opportunity for gain, the spoofing of a legal reader r might result in a gain for an attacker if later he or she may offer the malicious service to a competitor or thief who looks to perform an unauthorized inventory of the supply chain. The vulnerability that an attacker would try to exploit to manage the final objective of scanning EPC tags from company A with an unauthorized reader is the absence of secure authentication between readers in R_A and tags in T_A. Since we assume that the attacker does not have physical access to the ID system, he or she may find some difficulties for exploiting such lack of secure authentication. In fact, current EPC Gen-2 tags [6] support for example 16-bit Pseudo-Random Number Generator (PRNG) and Cyclic Redundancy Code (CRC) on chip, that might be used to improve the reader-to-tag link characteristics. They also include a 32-bit Personal Identification Number (PIN) for reading/writing the internal memory of the tag, as well as a 32-bit PIN for executing an internal auto-killing routine in order to destroy the information stored in the tag. However, the absence of stronger cryptographic functionalities (e.g., hash functions like MD5 and SHA-1) limits the execution of secure authentication mechanisms between reader and tags and leaves open the possibility of malicious readers from impersonating legal readers. Then, we can conclude that an attacker from the outside equipped with an EPC Gen-2 compatible reader can theoretically scan objects in motion from the supply chain, if he or she successfully manages to place the reader at the appropriate distance from the tags.

According to [6], the information stored on an EPC tag is an identification number for a specific object in motion in the supply chain. No additional information beyond the number itself is conveyed in the EPC. Any additional information must be retrieved by an EPC Information Service (EPCIS). Without access to this information, the EPC number itself is meaningless. We believe that if an attacker may access the data stored into a legal EPC tag (i.e., the EPC code), the attacker may successfully determine types and quantities of items in the supply chain, and properly sell the information to competitors of thieves. First, the attacker can obtain information from an EPC code, like the manufacturer and the product class. This information may be used for corporate espionage purposes by competitors or attacks against the rest of the infrastructure. Using the EPC codes scanned with the unauthorized reader, an attacker may clone tags through a skimming attack, by spoofing legal tags in T_A without physical access to the ID system infrastructure. We therefore consider that the *motivation* of an attacker for the spoofing threat should be considered as *high* and the difficulties as *solvable*. Hence the motivation and difficulties associated to this threat leads to a *likelihood* ranked as *possible*. Regarding the *impact* associated to this threat, we consider it as *high*, since it may have serious consequences for the company if either the attacker offers the malicious

Threat	Motivation	Difficulty	Likelihood	Impact	Risk
Spoofing of identities	*High*	*Solvable*	*Possible*	*High*	*Critical*
Tampering with data	*Moderate*	*Strong*	*Unlikely*	*Low*	*Minor*
Repudiation	*Moderate*	*Solvable*	*Possible*	*Medium*	*Major*
Information disclosure	*High*	*Solvable*	*Possible*	*High*	*Critical*
Denial of service	*Low*	*Strong*	*Unlikely*	*Low*	*Minor*
Elevation of privilege	*Low*	*Strong*	*Unlikely*	*Low*	*Minor*

Table 2. ID system threats analysis.

service to a competitor or to a thief. The threat is assessed as *critical* and needs to be handled with proper countermeasures.

Let us now move to the threat tampering with data. We consider the possibility of an attacker of adding, deleting, or modifying the information stored into a tag $t \in T_A$, or being transmitted from tag t to a reader $r \in R_A$. The motivation of the attacker is disrupting business operations and causing a loss of revenue to company A. Since this threat represents for the attacker a disruption rather than a clear opportunity for gain, we rate the *motivation* for this threat as *moderate*. Regarding the difficulties for performing an attack leading to the objective of this threat we rate them as *strong*. The difficulty is strong because the attacker should successfully bypass the difficulties presented before for spoofing threats and moreover: (1) the attacker should successfully bypass the necessary 32-bit PIN to access the internal memory of the tag (e.g., by performing a power analysis attack as the one presented in [12]), in case the tampering with data targets the tag t itself; or (2) in case it targets the information that is going to be transmitted from t to r, the attacker must re-inject the data once tampered at the precise instant that the reader is requesting it and, moreover, to bypass any possible collision with the information sent from the legal tag. We therefore consider that there are strong technical difficulties in conducting a proper attack for this threat. We rank its *likelihood* as *unlikely*. Since the impact results into temporary disruption rather than great financial losses, we rate the *impact* as *low*. We rank the threat as *minor*.

We analyze the repudiation threat. Each reader $r \in R_A$ sends to the corresponding middleware $m \in M_A$ a timestamp and its location. This is only an evidence, but not a proof of the transaction. The motivation of a retailer denying that it has received a certain pallet or case, due to the lack of non-repudiation protocols on the EPC network infrastructure, may clearly address financial gains. We rate the motivation as *moderate*. On the other hand, the difficulties, if any, are related to existing laws and legislations, and are clearly *solvable*. The impact to the company may constitute some financial losses, and we rate it as *medium*. Given the likelihood (i.e., *possible*) and impact associated to this threat, it is ranked as *major*. It therefore needs to be properly handled.

We continue our analysis evaluating the information disclosure threat. We recall that the communication channel between a reader $r \in R_A$ and a tag $t \in T_A$ are accessible over the air via an insecure wireless channel. Thus, illegitimate collection of this exchange of information, although might be slightly protected by reducing the reception range or by sheltering the area, is theoretically possible by means of eavesdropping attacks. Clearly the motivation for this threat must be rated as *high*, since the disclosure of the information related with the ID system may be used by a potential attacker for offering such malicious services to competitors, thieves, or any other individual looking for the objects tagged in the supply chains. The uniqueness of the information stored within an EPC tag, moreover, can also result in the tracking of individuals carrying such tags. We rank the information disclosure threat at the critical level.

Let us evaluate now the likelihood and impact of a denial of service threat against an EPC based RFID scenario as the one shown in Figure 2. Although the motivation for the attacker may be moderate if he or she expects financial gains, we consider that only a temporary disruption and limited outages apply at this level (e.g., ID system). Two kind of attacks may be used in order to manage the objective of this threat. On the one hand, the attacker may use a compatible reader from the outside and try to kill the set of tags in T_A by sending them the *kill* command. Current EPC Gen-2 tags support on-board, for privacy purposes, an auto-killing routine that destroys all the information stored in the tags. The routine is protected by a 32-bit PIN. Although there are strong difficulties to retrieve such a PIN, it is theoretically possible. In [12], for example, the authors present a proof-of-concept attack that does not require physical contact to the targeted tags, and that can retrieve the 8-bit PIN that protects the EPC Gen-1 tags. This proof-of-concept is only available for EPC Gen-1 tags. The authors in [12] state that EPC Gen-2 tags are however equally vulnerable. We therefore rate the technical difficulties for such an attack as *strong*. On the other hand, attackers may manage a similar disruption by performing RFID jamming attacks, i.e., by using powerful transmitters from the outside that generate noise on the frequency of the targeted readers. Although these attacks are possible, and obviously *solvable*, the signal is illegal and it is very easy, using direction finding tech-

nologies, to discover where a transmitter is located in order to stop it. We rate the motivation as *low*. We consider that in both cases, the likelihood of availability threats must be rated as *unlikely*. Given that it only represents to the organization temporal disruption of its operations rather than financial losses, we rate the impact as *medium*, and so the threat as *minor*.

We finally evaluate the elevation of privilege threat. Although we assume for our evaluation that there is a lack of authentication and/or negotiation between reader r and tag t, we assume however that an attacker could try to modify the configuration of reader r (by using configuration or programming flaws in this device) in order to read tags that is not meant to read and cause service disruption. The motivation of the attacker is thus rated as *low*, and the impact to the system is also rated as *low*. The technical difficulties are however rated as *strong*, due to the difficulty of modifying readers' configuration without physical access. The resulting likelihood is hence rated as *unlikely*, and the threat ranked as *minor*.

3.2 Lookup service threats

The Object Name Service (ONS) relies on a subset of functions of the Domain Names Service (DNS). Hence, it is fair to assume that deficiencies on security and privacy reported for the DNS are also going to affect the use of the ONS service. According to [8], although the complete discovery service for EPC applications (EPCDS) is not yet specified in [6], we can envision some early threats by studying the lookup service provided by the ONS.

The ONS behaves as follows. A reader r receives the identifier of an EPC tag. The reader forwards the identifier to a local middleware instance $m \in M_A$ of an EPC application. The middleware, or the corresponding address manager of the application, publishes an associated domain name into the local ONS service. This allows trading partners to query information about the tagged object. To perform such an operation, a given Uniform Resource Identifier (URI) is associated to the object in the form of an encoded concatenation of the attribute field values of the tag identifier. An external application $e \in E$ can then use this URI, together with the domain name `onsepc.com` (which is reserved for the ONS resolution process) to construct a FQDN (Fully Qualified Domain Name) (e.g., `ObjectClass.ManufacturerID.Header.onsepc.com`). Using the name, the application obtains URLs of associated information services. The ONS recycles existing DNS procedures and tools for the resolution of EPC based domain names. The main drawback of this scheme, from a security point of view, is that the underlying DNS protocol is potentially harmful. It introduces new threats to the EPC infrastructure. We may find in [2] a list of existing DNS vulnerabilities such as (1) interception of packets; (2) ID guessing and query prediction; (3) betrayal of trusted services; and (4) denial of service. It is reasonable to assume that threats against the availability of ONS resources, as well as confidentiality and accountability threats to the exchange of data between companies and ONS servers, and further integrity issues, are going to appear. We evaluate in the sequel the set of threats identified in Section 3.1 on the lookup service of the EPC network sample scenario shown in Figure 2. We take into consideration the assumptions that an attacker acts from outside the infrastructure and does not have physical access to components or services of the company. We summarize in Table 3 the results of our an evaluation.

Let us start by evaluating the spoofing of identities threat. We assume two different scenarios: (1) the attacker impersonates an external application and executes a dictionary attack in order to generate random queries that target the ONS/DNS instances associated to the lookup service utilized by company A; (2) the attacker impersonates the ONS/DNS server associated to company A, by using a man-in-the-middle attack for example, in order to intercept queries addressing products associated to company A. In both cases, the final objective of the attacker is the gathering of URLs to determine which products are actually located in company A. To do so, the attacker may try to isolate, for example, the manufacturers and/or the product numbers associated to the URLs. This information may be sold by the attacker to competitors or thieves. We therefore rate the *motivation* as *high*. Regarding the technical difficulties, and according to [2], they are perfectly possible and therefore *solvable*. These motivation and difficulties allows us to rate the *likelihood* associated to this threat as *possible*. On the other hand, the *impact* for the company should be considered as *high*, since it may lead to financial losses if such information is delivered to a competitor or to a thief. The threat is assessed as *critical*.

For the threat tampering with data, we assume the possibility of intercepting queries sent from an external application $e \in E$ to the ONS/DNS instance associated to company A and responding with false URLs. The final objective is leading e to conduct exchange of information with a malicious information service. If this attack is successfully executed, the attacker can deliver false information to the partners associated to company A and hence, leads to a loss of reputation or trust to the information of such company. We rate the motivation of an attacker as *moderate* since it can disrupt the operations of company A and can produce some kind of gain if the partners are redirected to a malicious information service. The attacker may successfully apply this threat using session hijacking and/or manipulation of queries, for example. We therefore assume that the exploitation of these vulnerabilities is theoretically possible and we rate the difficulties of this threat as *solvable*. These two parameters derive a likelihood rated as *possible*. Concerning the impact, we consider that this threat may cause to the company a loss of reputation and even some kind of

Threat	Motivation	Difficulty	Likelihood	Impact	Risk
Spoofing of identities	*High*	*Solvable*	*Possible*	*High*	*Critical*
Tampering with data	*Moderate*	*Solvable*	*Possible*	*Medium*	*Major*
Repudiation	*Moderate*	*Solvable*	*Possible*	*Medium*	*Major*
Information disclosure	*High*	*Solvable*	*Possible*	*High*	*Critical*
Denial of service	*Moderate*	*Solvable*	*Possible*	*Medium*	*Major*
Elevation of privilege	*High*	*Strong*	*Unlikely*	*High*	*Critical*

Table 3. Lookup service threats analysis.

economical consequences if, as an addition of the poisoning of URLs, the trading partner finally exchanges information with a non legitimate server. We thus rate the impact as *medium* and, as a consequence, we rank the threat as *major*. That means that the threat must be properly handled.

Let us evaluate the risk of the repudiation threat. Here, we assume either the possibility of an external application $e \in E$ or an address manager $a \in A_A$ performing illegal operations against the ONS/DNS component of the lookup service associated to company A. This is possible given the lack of tracing or auditing of such operations. Although it is fair to conceive the possibility of adding audit trails at this level, it seems that no repudiation protocol at both the ONS and DNS are actually going to present strong difficulties for an attacker from applying such a threat [2, 8]. We hence rate the motivation for the attacker as *moderate*, since he or she may offer the service to trading partners or customers of company A for denying the proper service during the publishing and/or resolution of addresses; and we rate the difficulties associated to this threat as *solvable*. These parameters lead to a likelihood rated as *possible*. The impact to the company for evading responsibilities when demanding a proof of the operations performed at the ONS instance of the lookup service level might result in some kind of economical repercussions. It thus leads to an impact rated as *medium*. The threat is finally ranked as *major*, which means that it must be properly handled in order to add, for example, appropriate audit trails associated to the infrastructure and hence, reduce its likelihood.

We move to the threat information disclosure. As we have assumed till now, and since the complete discovery service for an EPC based application has not publicly been yet specified in [6], we only analyze the possibility of leakage at the lookup service based on the DNS. We recall that such operations are based on a clear text protocol which uses domain names constructed using some field values of corresponging EPCs. It means that, by definition, the use of these domain names without additional countermeasures leads to a leakage of data such as manufacturers and product classes. The motivation of an attacker for looking for an attack path for this threat is clearly *high*, since such information can potentially be sold to competitors and thieves. The difficulties for executing the attack are *solvable* [2], which directly leads to rate the likelihood of this threat as *possible*. Given this likelihood and the repercussions for the company related with the illegal disclosure of information, i.e., *high* impact, we assess the information disclosure threat as *critical*; and we emphasize the necessity for handling it with the appropriate countermeasures.

Regarding the threat denial of service, since the service offered by the ONS can be seen as a critical component of an EPC based RFID application of company A (cf. Figure 2), we assume that the impact for the company in case that such a service fails is *medium*, since it is not going to be able to offer to the trading partners the on-line service that is meant to offer, i.e., information about the objects in its supply chain. DNS-like services have traditionally suffered from vulnerabilities that might be exploited to target availability [2]. The dependency between the ONS and DNS leads us to conclude that the lack of resistance against denial of service threats is also present in the ONS. This fact leads to rate the difficulties of an attacker for performing such threat as *solvable*. The motivation for the attacker, given such weak difficulties, is fairly rated as *moderate*. We thus consider the likelihood of this threat as *possible* and, then, its risk is assessed as *major*. Similarly to the previous threats, it must be handled by appropriate countermeasures.

We finally evaluate the elevation of privilege threat. DNS-based systems have no authentication procedures for the exchange of information. We assume that configuration deficiencies or programming flaws (e.g., buffer overflow vulnerabilities) on such systems can be exploited by attackers to elevate their privileges (e.g., beyond the proper reception of URLs, retrieving, for example, further information from company's resources). Since there are not yet precedents of these deficiencies on current ONS implementations, we assume that the technical difficulties associated to this threat, although theoretically possible, are sufficiently high and we rated them as *strong*. Since the motivation for the attacker is going to be equally high, due to the wide range of objectives that this threat can target (cf. Table 1), we rate both motivation and impact as *high*. The resulting likelihood is hence rated as *unlikely*. However, given the high impact to the company if the threat is successfully applied, we rate this later threat as *critical*, which means that it has to be handled by appropriate countermeasures.

4 Conclusions and future work

Security and privacy threats on RFID technologies are becoming one of the major concerns of information security researchers. The pervasiveness of these technologies and the power limitations of some of their components pose a great challenge when dealing with the problem of detecting and responding to threats on current and future EPC based RFID applications. We have presented an analysis of threats in order to identify and rank security issues that we consider relevant for further research. At the ID service, we ranked spoofing and disclodure threats as critical; and repudiation threats as major. At the lookup service, we ranked spoofing, disclosure, and elevation of privilege threats at the critical level; and tampering, repudiation, and denial of service threats as major. Threats ranked as either critical or major must be handled by proper countermeasures.

We have not covered existing countermeasures that may be applied for those threats. We refer the reader to [10] for a complete review on recent literature and scientific solutions that could be studied in order to handle both critical and major threats at the ID system level. The reader may find some mechanisms, such as lightweight authentication protocols and anti-forgery procedures, that could be considered for inclusion in current EPC based scenarios in order to countermeasure threats reported in Section 3.1. Existing countermeasures, such as DNSSEC, TLS/SSL, VPNs, and anonymizers may be used to address the critical and major threats analyzed in Section 3.2 [8]. We are actually studying and analyzing the cost and impact of these countermeasures, as well as their benefits.

Acknowledgments — The authors graciously acknowledge the financial support received from the following organizations: Natural Sciences and Engineering Research Council of Canada (NSERC), Mathematics of Information Technology and Complex Systems (MITACS), Spanish Ministry of Science and Education (CONSOLIDER CSD2007-00004 "ARES" grant), and *La Caixa* (Canada awards).

References

[1] Alfaro, J. G., Barbeau, M., and Kranakis. E. Security threats on EPC based RFID systems. In: *5th International Conference on Information Technology: New Generations. Information Security and Privacy track*, IEEE Computer Society, 2008.

[2] Atkins, D. and Austein, R. Threats analysis of the domain name system (DNS). *RFC 3833*, 2004.

[3] Auto-ID Labs. Available from: http://www.autoidlabs.org/.

[4] Barbeau, M. and Laurendeau, C. Tilting Giants: Avoiding Quixotic Pursuits in Undestanding the Threats to Wireless Network Security. In: *MITACS e-newsletter, Connections*, September 2007.

[5] EPCglobal Inc. Available from: http://www.epcglobalinc.org/.

[6] —. EPCglobal Standards Overview.. Available from: http://www.epcglobalinc.org/standards/.

[7] ETSI, Methods and protocols for security; part 1: Threat analysis. Technical Specification ETSI TS 102 165-1 V4.1.1, 2003.

[8] Fabian, B., Gunther, O., and Spiekermann, S. Security Analysis of the Object Name Service (ONS). In: *1st Int'l Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing* , pp. 71–76, 2005.

[9] Howard, M. and LeBlanc, D. Writing Secure Code. Microsoft Press Redmond, 2003.

[10] Juels, A. RFID security and privacy: a research survey. In: *IEEE Journal on Selected Areas in Communications*, 24(2):381–394, 2006.

[11] Laurendeau, C. and Barbeau, M. Threats to Security in DSRC/WAVE. In: *5th International Conference on Ad-hoc Networks (ADHOC-NOW)*, Lecture Notes in Computer Science, Springer Berlin / Heidelberg, Volume 4104, 2006, pp. 266-279.

[12] Oren, Y. and Shamir, A. Power analysis of RFID tags. In: *Rump session of Advances in Cryptology, CRYPTO'2006*, 2006. Available from: http://www.wisdom.weizmann.ac.il/∼yossio/rfid/.

[13] Roberti, M. 5-Cent Breakthrough. RFID journal Available from: http://www.rfid-journal.com/article/articleview/2295/1/128/.

[14] Thompson, D.R., Di, J., Sunkara, H., and Thompson, C. RFID security threat model. In: *Conf. on Applied Research in Information Technology*, 2006.