Security threats on EPC based RFID systems

Joaquin Garcia-Alfaro[*,†], Michel Barbeau[*], and Evangelos Kranakis[*]

Abstract: *We present an evaluation of threats on the Radio Frequency IDentification (RFID) system of the Electronic Product Code (EPC) Network architecture. We analyze attacks on the communication channel between RFID components due to the use of an insecure wireless channel. We analyze the threats according to the methodology proposed by the European Telecommunications Standards Institute (ETSI), and we rank them in order of relevance.*

Keywords: Radio frequency identification (RFID); Electronic Product Code (EPC); Threats analysis; Information systems security; Network security; Wireless security.

1 Introduction

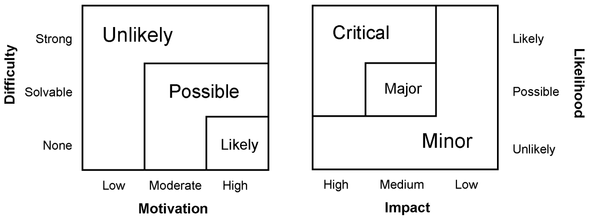
The Electronic Product Code (EPC) is a low-cost technology, based on passive Radio Frequency IDentification (RFID) devices. It is acclaimed as the successor of today's omnipresent bar codes. The EPC is the basis of a distributed architecture, called the EPC Network [1], for the automatic identification of objects in motion on supply chain and industrial production applications. A globally unique number is assigned to the RFID device assigned to every tagged object. This number is then used to identify the object and get further information about it through Internet based applications (e.g., using Web services). The information about an object is not stored on a tag, but instead supplied by distributed servers on the Internet. Security and privacy threats can target the different services of the EPC network, if weaknesses are not handled properly. The exchange of information between EPC tags and readers, for example, are carried via insecure wireless connections and without authentication and authorization processes. This situation may allow an attacker to misuse the front-end service of an EPC setup, in order to steal information or track the location of objects and/or their carrier. Mitigation mechanisms must be applied in order to reduce those risks, ranked as major or critical —according to our evaluation. We present an analysis of threats on the RFID level of the EPC network.

Section 2 outlines the methodology used for our analysis of threats. Section 3 presents the results of our evaluation. Section 4 concludes the paper.

2 Analysis methodology

The methodology used for our evaluation relies on the identification of threats depending on their *likelihood* of occurrence, their possible *impact* upon the targeted system, and the *risk* that they may represent to the victim. It is based on an evaluation framework proposed by the *European Telecommunications Standards Institute* (ETSI) in [2]; but slightly modified in order to take into account the suggestions introduced in [3] for identifying relevant threats and security flaws on current wireless network applications.

The likelihood of a threat (cf. Figure 1(a)) is determined by the *motivation* for an attacker to carry out an attack associated to the threat vs. the *technical difficulties* that must be resolved by the attacker in order to conduct such an attack. In turn, the risk associated to a threat (cf. Figure 1(b)) is a function of its likelihood vs. the consequences on the system if the threat successfully achieves its objective. A threat is ranked as *minor* when it is unlikely to happen or when its impact is low. A threat is ranked as *major* when its likelihood is possible and its impact is medium. A threat is assessed as *critical* when it is likely to happen and its impact either medium or high; or when its likelihood is possible and its impact is high.



(a) Likelihood of a threat.

(b) Risk evaluation function.

Figure 1. Likelihood and risk functions.

[*] School of Computer Science, Carleton University, Ottawa, Canada.

[†] Open University of Catalonia, Barcelona, Spain.

3 RFID threats

The communication channel between the components of an RFID system of an EPC network [1], i.e., the EPC tags and RFID readers is a potentially insecure wireless channel. It is therefore fair to assume that most of the threats on EPC setups are going to target this first level. Let S be an EPC based supply chain associated to an organization O. Let T_S be the set of RFID tags in S. Let R_S be the set of RFID readers in S. We analyze in this section threats targeting basic security features such as *authenticity*, *integrity*, *confidentiality*, and *availability* during the exchange of data between a tag $t \in T_S$ and a reader $r \in R_S$. We assume that attackers may only act from the outside if they want to exploit the insecure communication channel between r and t, or the lack of authentication between these elements. We therefore assume that attackers do not have physical access neither to the components of the system nor to the organization itself. The reason why we do not consider direct physical access is because we assume the presence of other security mechanism in the organization, such as physical access control and surveillance of workers. Attackers, however, may have access to information about the system and its components or services. We summarize in Table 1 the results of our evaluation.

Authenticity Threats – We start ranking the motivation and difficulties of authenticity threats using spoofing attacks. While the spoofing of a legal tag $t \in T_S$ into the system may only result in a disruption rather than an opportunity for gain, the spoofing of a legal reader r might result in a gain for attackers if they offer this malicious service to a competitor or thief who looks to perform an unauthorized inventory of the supply chain. The vulnerability that the attacker would exploit to manage the final objective of scanning EPCs from organization O with an unauthorized reader is the absence of secure authentication between readers in R_S and tags in T_S. Since we assume that attackers do not have physical access to the system, they face difficulties for exploiting the lack of secure authentication. In fact, current EPC Gen-2 tags [1] support 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 that destroys the information stored in the tag. However, the absence of strong cryptographic functionalities (e.g., hash functions like MD5 and SHA-1) limits the execution of secure authentication mechanisms between readers and tags and leaves open the possibility of malicious readers from impersonating legal readers. We conclude that outside attackers equipped with EPC Gen-2 compatible readers can theoretically scan objects in motion from S if they successfully manage to place a reader at the appropriate distance from the tagged objects. According to EPCglobal [1], the information stored on an EPC is an identification number for a specific object in motion in the supply chain, and no additional data beyond the number itself is conveyed in the EPC. Any additional information associated with such a number must be retrieved by an EPC Information Service (EPCIS) [1]. We believe that if an attacker may access the data stored into EPC tags, and if such data is the EPC codes, an attacker may successfully determine types and quantities of items in the supply chain, and sell the information to competitors or thieves. First, the attacker can obtain information from an EPC code, like the manufacturer and product number. This information may be used for corporate espionage purposes by competitors, or other attacks against other services of the EPC infrastructure. Even more, by using the EPC codes scanned with an unauthorized reader, attackers may clone those tags through a skimming attack, by spoofing legal tags in T_S, without physical access to the organization. We therefore consider that the motivation for attackers for conducting spoofing attacks is *high*, and that the associated difficulties are *solvable*. This motivation and difficulty lead to a likelihood that is *possible*. Regarding the impact associated to this threat, we consider it as *high*, since it may have serious consequences for the company either the attacker may offer the malicious service to competitors or to thieves. According to the methodology presented in Section 2, the threat is assessed as *critical* and needs to be handled by appropriate countermeasures.

Integrity Threats – We consider here the possibility of an attacker to add, delete, or modify the information stored in a tag $t \in T_S$, or being transmitted from tag t to a reader $r \in R_S$. The motivation of an attacker is disrupting business operations and causing a loss of revenue to organization O. Since the attack creates a disruption rather than a clear opportunity for gain, we rate the motivation for the threat as *moderate*. We consider that the difficulties for performing the attack are *strong*. The reason why we rate the difficulty of this threat as strong is because the attacker should successfully bypass the same difficulties presented before and moreover: (1) the attacker should successfully bypass the necessary 32-bit PIN to finally access the internal memory of the tag (e.g., by performing a power analysis attack as the one presented in [4]), in case an attack based on tampering of 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 tampered data at the precise instant that the reader is requesting it and avoid any collision with the information sent by the legitimate tag. We therefore consider that there are strong technical difficulties in conducting a proper attack for this threat, and we rate its likelihood as *unlikely*. The impact consists of temporary

Objective	**Motivation**	**Difficulty**	**Likelihood**	**Impact**	**Risk**
Authenticity	*High*	*Solvable*	*Possible*	*High*	*Critical*
Integrity	*Moderate*	*Strong*	*Unlikely*	*Medium*	*Minor*
Availability	*Low*	*Strong*	*Unlikely*	*Medium*	*Minor*
Confidentiality	*High*	*Solvable*	*Possible*	*High*	*Critical*

Table 1. Evaluation of threats.

disruptions rather than great financial losses. We hence rate the impact as *medium*, and the threat as *minor*.

Availability Threats – Although the motivation for attackers for performing Denial of Service (DoS) attacks may be moderate if they expect financial gaining, we consider that only a temporary disruption and limited outages apply at the ID service of an EPC network. Two kind of mechanisms may be used by attackers to manage the objective of a DoS attack. On the one hand, attackers may use a compatible reader from the outside and try to kill the set of tags in T_S by sending them *kill* commands. 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 [4], for example, the authors presented a proof-of-concept attack that does not require physical contact with the targeted tags, and that can retrieve the 8-bit PIN which protects the routine on EPC Gen-1 tags. Although this proof-of-concept is only available for EPC Gen-1 tags, the authors in [4] state that EPC Gen-2 tags are equally vulnerable. We therefore rate the technical difficulties for such attacks 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 on the frequency of the targeted readers. Although these attacks are possible, and obviously *solvable*, the signal is illegal and it is very easy to discover locations of transmitters. 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*.

Confidentiality Threats – The traffic between a reader $r \in R_S$ and a tag $t \in T_S$ flows through an insecure wireless channel. Thus, illegitimate collection of this traffic, 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 RFID system of an EPC network, as we pointed out for authenticity threats, may be used by potential attackers for offering their services to competitors, thieves, or any other individual looking for the objects tagged in S. The uniqueness of the information stored within an EPC, moreover, can also result in the unique tracking of individuals carrying such tags. We rank the confidentiality threats at the critical level. Confidentiality threats must therefore be handled by appropriate countermeasures.

4 Conclusion

We presented in this paper an analysis of threats on the RFID system of the EPC network architecture. We identified and ranked four threats that we consider relevant for further research. We ranked authenticity and confidentiality threats as critical and claimed that they must be handled by appropriate countermeasures. Our future work is heading in this direction.

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 (TSI2007-65406-C03-03 “E-AEGIS” and CONSOLIDER CSD2007-00004 “ARES” grants), and *La Caixa* (Canada awards).

References

[1] EPCglobal Inc. http://www.epcglobalinc.org/

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

[3] 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.

[4] 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/