Security Threats in RFID

TTM4137 – November 8, 2009
Kim Joar Bekkelund – kimjoarr@stud.ntnu.no – Norwegian University of Science and Technology

Introduction

Radio-frequency identification (RFID) uses radio frequency signals to automatically identify objects. RFID tags are gradually being included into most objects on earth — From library books to passports to animals and all other things imaginable. An RFID tag is a small wireless device that react to electromagnetic fields generated by an RFID reader[2]. [1] calls RFID one of the most promising technologies in the scope of ubiquitous computing. And for every technology being deployed in such great numbers, security is essential.

In this essay I will try to identify RFID security threats and how they can be guarded against.

A basic understanding of RFID

RFID is a system for no-contact, non-line-of-sight and invisible identification[3], and is comprised of three main components[9] (as shown in Figure 1):

1. an RFID tag, which is located on the object to be identified.
2. an RFID reader, which is able to read and write to a tag.
3. a data processing subsystem, which is connected to an RFID reader.

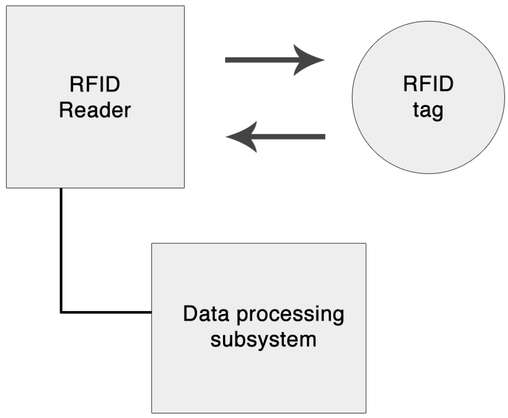

Figure 1: An illustration of an RFID system

There are basically three types of RFID tags[14]: Active, semi-passive and passive. The difference is that active tags have an on-tag power supply and actively send RF signals, while passive tags obtain all their power from an RFID reader. The semi-passive tag have both an on-tag power supply and rely on power from a reader.

Since passive tags rely on power from the RFID reader, they have very limited resources. They have a short communication range, a very small memory footprint — typically just hundreds of bits — and very limited computational power. With these limitations it is difficult to implement strong cryptographic functions[3].

Privacy and security issues should be addressed before RFID implementations will be accepted universally[4].

The primary focus of this essay is the RFID tag itself, and not the entire system. Specifically the focus will be on passive RFID tags since they are the most limited tags. Both semi-passive and active tags can handle far more resource intensive security protocols.

Threat Model

[5] defines a security threat as "*A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.*"

To get a grasp of the security threats in RFID the Microsoft developed threat model STRIDE is used[6]. STRIDE is an acronym for the following six categories of threats:

- **S**poofing — An attacker is successfully able to pose as an authorized user of a system.
- **T**ampering — An attacker is able to modify data.
- **R**epudiation — A user denies a situation and no proof exists to prove that the action was performed.

- **I**nformation Disclosure — Information is exposed to an unauthorized user.
- **D**enial of Service — Denying service to valid users.
- **E**levation of privilege — An unprivileged user gains higher privileges in the system than what they are authorized.

Categorizing the security threats with STRIDE identifies potential strategies for mitigating them[10].

Threats in RFID

An example of a spoofing attack is where an attacker is able to read an individual's tag without their specific authorization. To guard against the threat of spoofing, authentication is needed. There exists several strong authentication protocols, such as EAP and Kerberos, but as mentioned the problem with RFID tags, and especially passive tags, are that they are very resource limited. This severely limits the set of possible authentication protocols that can be used.

According to [1] a passive RFID tag roughly has between 5000 and 10000 logic gates. 250 to 3000 of these gates are available to security measures. A typical implementation of AES need in the order of 20000 logic gates. [7], [8] and several others have introduced lightweight authentication protocols specifically created for, or adapted to, RFID.

Tampering with data can for example be an attacker that is able to modify the tag in a passport to remove unwanted information. There are two kinds of protections against tampering[11]: Tamper-evidence, in which the system detects tampering, and tamper-resistance, in which the system is able to resist tampering.

In Electronic Product Codes (EPC), which are based on passive RFID tags, a 32 bit PIN is needed to get access to the internal memory of the tag[12]. Because of the difficulty of tampering with transmitted data, and the length of the PIN needed, [12] classifies integrity threats as unlikely. (But as a side-note, they don't seem to have considered the fact that this approach is vulnerable to eavesdropping.) [11] examines the most recent studies of tampering in RFID, and notes that data tampering is still in 2009 a critical threat in RFID based systems.

A repudiation threat can for example be that a retailer denies receiving a certain pallet. To ensure that neither sender nor receiver can deny an action a non-repudiation protocol is required[3].

Mitigation techniques for repudiation include digital signatures, timestamps and audit trails [10], but because of the limited computational power of RFID tags this is a challenge. The tag itself does not have enough memory to save an audit trail, so this must be done externally. This puts a much higher demand on the *data processing subsystem*.

An information disclosure threat is for example a thief querying the tags on a potential victim to determine what they are carrying. To guard against this, it should not be possible for the thief to determine the object they are trying to identify. Authentication will make it significantly more difficult to determine the identity, but it is still possible to track the specific tag, since it always will have the same identification. For example a thief queries a tag on an expensive watch in a store, and thereby learns its unique identification. He then waits outside the shop, querying all the tags that passes. When someone buys the watch, the thief will know who. To remedy this [15] suggests that RFID tags should be relabeled on checkout. [14] names other possible solutions, including *killing* the RFID tag or rotating between a collection of pseudonyms to identify it.

Since RFID if based on radio communication, an example of a denial of service threat is an attacker shielding a tag with a Faraday Cage, and thereby making it impossible to read.

Another possibility is sending radio signals that collide with the authorized user's, making it impossible for them to communicate with the tag. Since all wireless devices are subject to *radio jamming*, this is not an issue that is specific to RFID[14]. [9] suggests a method requiring physical contact for critical functionality, which help defend against denial of service attacks.

Since RFID is such a limited system, most passive tags only have two types of access: No access and access to everything. [16] classifies this as two states: locked and unlocked, and where the tag only enters the unlocked stage when it receives an appropriate command. Elevation of privilege is then basically getting the tag into the unlocked stage, and will be dependent of choice of anti-tampering approaches[11]. The threat of elevation of privilege is far more important when considering the entire RFID system.

Conclusion

By using the STRIDE model, we have been able to get a better understanding of the security threats in RFID — and because of the space constraints with a focus on only the passive RFID tags — and as we can see there exist several major and critical security threats. According to [13] a major challenge with RFID is the immaturity of the industry, and that the standards are being developed while RFID is being globally deployed.

RFID is already widely used, and will be globally deployed into more and more areas of life if the coming years, and it is therefore important to know that there are security threats related to the use of RFID, and that many of them are major.

References

[1] Peris-Lopez, P. et al. *RFID systems: A survey on security threats and proposed solutions.* Lecture Notes in Computer Science. 2006.

[2] Damgard, I. and Pedersen, M.O. *RFID security: Tradeoffs between security and efficiency*. Lecture Notes in Computer Science. 2008.

[3] Thompson, D.R. and Chaudhry, N. and Thompson, C.W. *RFID Security Threat Model*. Conf. on Applied Research in Information Technology. 2006.

[4] Chaudhry, N. and Thompson, D.R. and Thompson, C. *RFID Technical Tutorial and Threat Modeling*. 2005.

[5] RFC 2828 — Internet Security Glossary

[6] Hernan, S. and Lambert, S. and Ostwald, T. and Shostack, A. *Uncover Security Design Flaws Using The STRIDE Approach*. 2006.

[7] Lee, Y. and Verbauwhede, I. *Secure and low-cost RFID authentication protocols.* 2nd IEEE Workshop on Adaptive Wireless Networks (AWiN). 2005.

[8] Vajda, I. and Buttyán, L. *Lightweight authentication protocols for low-cost RFID tags*. Second Workshop on Security in Ubiquitous Computing. 2003.

[9] Sarma, S.E. and Weis, S.A. and Engels, D.W. *RFID systems and security and privacy implications*. Lecture notes in computer science. 2003.

[10] Thompson, D.R. and Di, J. and Sunkara, H. and Thompson, C. *Categorizing RFID privacy threats with STRIDE*. Proc. ACM Symposium on Usable Privacy and Security. 2006.

[11] Gandino, F. and Montrucchio, B. and Rebaudengo, M. *Tampering in RFID: A Survey on Risks and Defenses*. Mobile Networks and Applications. 2009.

[12] Garcia-Alfaro, J. and Barbeau, M. and Kranakis, E. *Security threats on EPC based RFID systems*. International Conference on Information Technology: New Generations (ITNG 2008), IEEE Computer Society, Las Vegas, Nevada, USA. 2008.

[13] Rathinasabapathy, G. and Rajendran, L. *RFID Technology and Library Security: Emerging Challenges*. Journal of Lib. Inf. & Comm. Technology Vol 1. 2009.

[14] Juels, A. *RFID Security and Privacy: A Research Survey*. 2005.

[15] Good, N. et al. *Radio frequency identification and privacy with information goods*. Workshop on Privacy in the Electric Society. 2004.

[16] Weis, S. et al. *Security and privacy aspects of low-cost radio frequency identification systems*. In Proceedings of the 1st International Conference on Security in Pervasive Computing, 2003.