A Secure Architecture for the Use of RFID at Home

Shantanu Rao*

Department of Electrical and Computer Engineering, College of Engineering

Abstract. Radio Frequency Identification (RFID) tags are being adopted rapidly for item-level identification by retail giants such as Walmart. While this technology brings many benefits to consumers, it has also caused a lot of concerns about potential threats to consumers' privacy. This paper presents a secure architecture for the use of RFID in a home environment. This architecture defines a layered approach to RFID security. It is shown that the proposed architecture mitigates many threats relating to RFID use at home.

1. Introduction

RFID is a rapidly emerging technology that is anticipated to lead to great advances in areas as diverse as inventory management, health care, and animal farming, by enabling convenient item level tracking. Retailers such as Walmart and Tesco have started investing in RFID technology for supply-chain management. Consumer products labeled with RFID tags are appearing in the market. Consumers can already find RFID tags in some credit cards, car security devices, pet tracking applications and toll-booth payment devices.

A major retail application of RFID tags is to replace the current pervasive UPC bar codes. In a significant improvement over bar codes, new standards such the Electronic Product Code (EPC) [2] will enable every RFID tagged product to be uniquely identified worldwide. It is envisioned that in the near future consumers will wear RFID tags on their clothes, carry RFID tagged products in their pockets, and run RFID enabled smart-appliances in their homes.

2. RFID Security Challenges

Along with innumerable opportunities for new and improved services due to RFID come several security and privacy challenges. There has been much public concern about threats to personal privacy due to RFID use. This issue has also gained the attention of privacy rights activists [1].

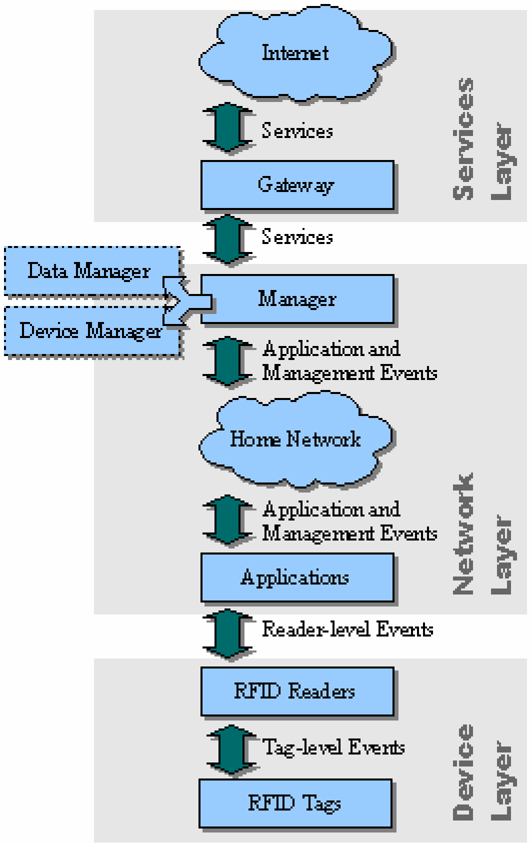
Such concerns are well founded in technical literature. Several possible security threats relating to privacy and authentication exist in an RFID environment. These are because RFID tags introduce the possibility of clandestine tracking and clandestine inventorying [3] that does not involve line-of-sight contact. Significant mitigation strategies also exist, including the Blocker Tag [4], RFID Guardian [5], and the employment of cryptography on RFID tags. However, threats to privacy due to the introduction of RFID tags exist not only between the RFID reader and the tag, but also in the network. The adoption of RFID and related technology is expected to result in an "Internet of Things" where humans are no longer the primary generators or receivers of information. RFID related technologies such as Object Naming Service (ONS) will result in increased traffic-flow on networks. Also, the information being exchanged will potentially be of a private nature. This suggests that new security models need to be created to deal with this new network paradigm. In the following section, the author proposes a secure architecture for the use of RFID by consumers in home environments.

3. Description of Proposed Architecture

This paper introduces a secure architecture for RFID use in a home environment. Figure 1 provides a diagrammatic representation of this architecture. The architecture is divided into three layers: device layer, network layer, and services layer. Each of these layers contains several components.

3.1 Device Layer

The device layer comprises RFID Tags and RFID Readers. The Tags carry globally unique tag IDs that are used to identify them. Readers power up and singulate the Tags within their range and obtain their tag IDs. They can also send certain commands to the Tags such as the "kill" command that disables the Tag. Readers are controlled by Applications that are described next.



[1] ***Figure 1. Secure Architecture for RFID***

3.2 Network Layer

The network layer comprises Applications, the Home Network, and the Manager. Applications (such as RFID-capable refrigerators, medicine cabinets, etc.) communicate with RFID Readers to obtain tag IDs. They can also send commands to Readers. Applications communicate with the Manager via a secure Home Network. This network can be wireless or wired.

The Manager consists of two sub-components. Device Manager provides network management capabilities including authentication of Applications and Readers, network encryption and synchronization. Data Manager aggregates RFID tag IDs received from the Applications, queries RFID information from the Services layer based on these IDs, maintains a database of such RFID information, and provides necessary information to the Applications.

3.3 Services Layer

The Services layer comprises of the Gateway and the Internet. The Gateway acts as a firewall and provides for access control and encryption of outgoing information. It also authenticates various RFID services such as ONS that will be accessed over the Internet.

The following section discusses the security aspects of this architecture.

4. Security of Proposed Architecture

The proposed architecture achieves overall security by ensuring that events between any two components are secure.

Tag-level security against active intruders is ensured by ensuring that RFID Readers read Tags only if they have been authorized by the Manager. Unauthorized Readers are detected by an RFID scanner that generates a jamming signal to block any attempts by such Readers to read Tag IDs. Passive monitoring of Reader-to-Tag communication is mitigated by ensuring that Readers use the minimum amount of power required to read tags. Additionally, redundant Tag reads are avoided by efficient Application protocols.

Reader-level Events are secured by authentication of Applications and Readers.

Application and Management Events on the Home Network are secured via data encryption on the network. The Manager maintains a list of authenticated home devices. All other devices that wish to access the Home Network either have to be authenticated, or need to gain entry via the Gateway.

Access to Services is secured by the Gateway. The Gateway controls access to the Manager or the Home Network by remote devices. It also authenticates the various Services on the Internet to ensure that RFID data is shared with trustworthy sources. All data received from external services is stored securely on local devices by the Manager.

5. Conclusion

In this paper, the author describes a secure architecture for the use of RFID in at home. The architecture is broken down into layers and components. Overall security is ensured by securing events that occur between the components in the architecture.

[1] Privacy Rights Clearinghouse. RFID Position Statement of Consumer Privacy and Civil Liberties Organizations. http://www.privacyrights.org/ar/RFIDposition.htm. Nov. 2003.
[2] EPCGlobal Inc. EPCGlobal Architecture Framework. July, 2005.
[3] Ari Juels. RFID Security and Privacy: A Research Survey. In IEEE *Journal on Selected Areas in Communications*, Vol. 24, No. 2, Pages 381-394, February 2006.
[4] Ari Juels, Ronald L. Rivest, Michael Szydl. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In *Proceedings of the 10th ACM Conference on Computer and Communications Security,* Pages 103–111, 2003.
[5] Melanie R. Rieback, Bruno Crispo, Andrew S. Tanenbaum. RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management. In *Proc. 10th ACISP*, Brisbane, Australia, Jul. 2005.