RFID as an Enabler of the Internet of Things: Issues of Security and Privacy

Benjamin Khoo
School of Management, New York Institute of Technology
P.O. Box 8000, Old Westbury, NY 11568, U.S.A.
kkhoo@nyit.edu

***Abstract*—RFID is one of the enabling technologies of the Internet of Things. RFID has the potential to enable machines to identify objects, understand their status, and communicate and take action if necessary, to create "real time awareness." The pervasiveness of RFID technology has given rise to a number of serious issues including security and privacy concerns. This paper will discuss current RFID usage issues and conduct a threat analysis of the RFID system components then identify issues/risks and elucidate how these issues can be resolved or risks can be mitigated.**

I. INTRODUCTION

The term Internet of Things (IoT, also known as the Internet of Objects) refers to the networked interconnection of everyday objects. It is generally viewed as a self-configuring wireless network of sensors whose purpose would be to interconnect all things [1]. The individual technologies to make this possible are already available – Global Positioning System (GPS), Geographical Information System (GIS), Smart Objects and Radio Frequency Identification (RFID). RFID is a wireless Automatic Identification and Data Capture (AIDC) technology that operates without human intervention. The IoT concept is attributed to the original Auto-ID Center, founded in 1999 and based at the time in MIT [2]. The RFID development community at that time used the term Internet of Things to refer to the possibility of discovering information about a tagged object by browsing an Internet address or database entry that corresponds to a particular RFID tag. Business enterprises and even governments have looked upon the emerging Radio Frequency Identification (RFID) technology as a possible silver bullet in the application of pervasive and ubiquitous computing [3] [4].

The move from the Internet of Computers to the Internet of Things entails a paradigm shift from a physical world to one that is a fusion with the virtual world. Digital objects in a virtual world now represent physical things. Objects are now context-aware. They can sense, communicate and interact autonomously. The IoT will lead to new technology applications and services with higher productivity [5]. The key features of the IoT includes: options using the centralized or decentralized mechanism of the infrastructure depending on the applications; identity management of very large number of identifiers of people or objects or machines; context aware applications; mobility of people or things; different quality of service for different types of services and customized, personalized and user-friendly applications [6]. This new phase of the Internet will create opportunities for innovation in services relying on information related to the identity, status and location of the things (objects), and new societal services that will improve the quality of life [7].

There are four major enabling technologies for the IoT:
1. Identifying Objects: RFID,
2. Feeling Objects: Sensor technologies,
3. Thinking Objects: Smart technologies, and
4. Shrinking Objects: Nanotechnology.

RFID technology is considered a pivotal enabler of IoT.

The prominence that businesses and governments have placed on the IoT necessitates a closer examination of the security and privacy risks associated with this technology. The potential for anonymity, embedded tags in products that can reveal sensitive information, violations of location privacy with no-contact, non-line-of-sight through non-conducting material such as cardboard or paper, fast read rate at a distance of up to a few meters and invisible identification which can be done indiscriminately has raised privacy concerns [8][9].

There have been a number of published papers that surveyed IoT security and privacy issues. This paper will take a different approach while extending this body of published literature by conducting a risk analysis based on the RFID system components then elucidate how to mitigate these risks.

This paper is divided into 5 sections. Section I is the introduction. Section II provides a review of RFID's IoT enabling technologies. Section III will examine security and privacy issues in IoT applications. Section IV will conduct the risk analysis and discuss the various IoT security and privacy issues including mitigating the associated risks based on accepted secured RFID practices or guidelines. This paper will conclude in Section V by analysing current efforts and future roadmaps to resolve these outstanding issues.

II. REVIEW OF RFID'S IOT ENABLING TECHNOLOGIES

RFID is one of the technologies representing a new way of doing business brought about by convergence in which computing, communications, and interactivity are available through a world of wireless, sensors, and network computing [10][11]. RFID has the potential to enable machines to identify objects, understand their status, and communicate and

978-0-7695-4580-6/11 $26.00 © 2011 IEEE
DOI 10.1109/iThings/CPSCom.2011.83

take action if necessary, to create "real time awareness" [12][13]. As the 21st century gets more competitive, advances in sensor technologies, miniaturization and nanotechnology have created opportunities for embedding intelligence in objects. These technologies have contributed to the development of advanced information systems (IS) such as smart objects [14][15][16] that can autonomously communicate with each other. The 2009 Horizon Project reported that smart objects are one of the technologies to watch with a time-to-adoption horizon of four to five years [17]. Identification technologies such as RFID identifies each unique object, wireless sensor technologies allow objects to provide information about their environment and context, smart technologies allow everyday objects to "think and interact," nanotechnology and energy-scavenging technologies are packing more processing power into less space [7]. All these developments will create an "Internet of Things" (IoT) that connects and enables intelligent interaction between objects around the world [18][19]. In recent times, researchers have used the phrase "Internet of Things" to refer to the general idea of things, especially everyday objects that are readable, recognizable, locatable, addressable, and/or controllable via the Internet—whether via RFID, wireless LAN, wide-area network, or other means [20]. Today, developments are rapidly under way to take this phenomenon an important step further, by embedding short-range mobile transceivers into a wide array of additional gadgets and everyday items, enabling new forms of communication between people and things, and between things themselves.

A new dimension has been added to the world of information and communication technologies (ICTs): from **anytime, anyplace** connectivity for **anyone,** there is an additional dimension - connectivity for **anything** (Figure 1). Connections will multiply and create an entirely new dynamic network of networks – an Internet of Things [21]. This new IoT will now integrate physical things into the information flows. The IoT includes the overall infrastructure (hardware, software and services) supporting this networking of objects that are active participants in business and information processes, exchanging data including their identities, their physical properties and information 'sensed' from their environment. Identification technologies like RFID allows each object to have a unique identifier that can be read at a distance allowing automatic, real time identification and tracking of individual objects [7].

GS1 is a not-for-profit organization that develops global standards for the identification of goods and services. GS1's standards foster cooperation and encourage information sharing worldwide. Businesses and organizations can improve efficiency by adding useful information to any exchange or interaction of goods or provision of services. The EPCglobal Network provides solutions for identification, data capture and data exchange. At the present time, scientists together with engineers are working to embed more memory on the RFID tag. The increase in memory will allow programmed intelligence to be embedded on the tag. This will transform a tagged common object into a smart object and as a consequence enhance inter-object interactions with intelligence. For such an information infrastructure there are four basic needs that must be fulfilled: the need for automatic/intelligent interactions, the need for identification, the need for data capture and the need for data exchange. The IoT will require the development of a global infrastructure and smart objects/tags that meets these needs.

III. SECURITY AND PRIVACY ISSUES

Despite its promises, RFID faces some challenges when used in the IoT. Most of the sources of security and privacy issues arise from the violation of the air interface between a tag and its reader.

A number of security researchers have published papers surveying the major threats and examined various approaches to protect privacy and ensure integrity in RFID technology[22][23][24][25]. Blocking is when attackers use a blocker tag to stimulate the existence of many tags and cause a denial of service as the reader tries to interrogate these non-existence tags. Jamming means paralysing the communication system by generating radio noise at the same frequency as that of the system. Blocking and jamming devices can be detected early and localize so that appropriate actions is taken. Relay attacks is done using a fake tag to communicate with the real reader and a fake reader to communicate with the real tag. The information obtained by the fake reader is passed to the fake tag, which then communicates with the real reader. Using short-range tags can mitigate this, by shielding the tag or implementing the distance bounding protocol. Eavesdropping happens when attackers secretly monitor the communication between the tag and the reader. Large read range has also opened up opportunities for eavesdropping by rogue readers. Authentication of distance is used to secure the tag by minimizing the read distance to a few millimetres. This can be mitigated by encrypting the data, shielding the tag or limit the tag-reader distance, however attacker can use a non-standard reader to extend the distance. Rogue readers can intercept and read tag information. Reader authentication can be used to allow only authorised readers to read the tag information. Replay attack happens when attackers eavesdrop on the communication between a tag and reader, and then use a cloned tag to repeat the authentication sequences. This can be mitigated using the same countermeasures for eavesdropping and tag cloning. When attackers make a duplicate tag based on a real tag after gaining unauthorised access to the real tag is called tag cloning. The duplicate tag can be used to gain unauthorised access to confidential information or make an electronic transaction. Tag cloning can be mitigated using tag authentication. Clandestine tracking and inventorying due to embedded tags in items that supports invisible identification, which can be done indiscriminately, can reveal sensitive information, and violates location privacy with no contact and is non-line-of-sight. Tags can also be used to track people who have in their possession a RFID tag by rogue readers and

eavesdropping devices. This can be mitigated by using low range tags or shielding tags, authenticating the readers or disabling the tags. Physical tag destruction is like microwaving a tag in an oven or hitting it with a hammer.

The increased integration of RFID technology in businesses and in the day-to-day life of consumers has raised privacy concerns [8][9]. There are two main privacy issues – personal and location privacy. Solutions that had been proposed includes: temporarily disabling a tag (putting a tag to sleep) then transmitting a PIN to awoken it, changing the tag identifier over time, killing a tag (which can be executed with a 32-bit PIN), relabeling tags, the active jamming approach where the RF channels are jammed with radio signals to isolate the tag from any electromagnetic waves, minimalist cryptography where tags contain a small collection of pseudonyms and releasing a different pseudonym on each reader query, re-encryption of tags in banknotes and universal re-encryption where the cipher-text is re-encrypted without knowledge of the corresponding public key, the Faraday Cage Approach where the tag is isolated from any electromagnetic waves, the blocker tag, and the use of cryptography, hash functions and authentication schemes to secure the data [24].

RFID devices are used for tracking and transfer of data at different stages or locations to different "owners" in an open system for later processing. RFID technology needs to support data sharing and transfer between different objects that are interacting. They are different from the traditional assets in a threat analysis scenario because they are "carriers" of the information assets that are useful in the case of tracking. For this reason, RFID have to support two important features: transfer of ownership and multiple authorisations [26].

IV. IOT SECURITY RISK ANALYSIS

This paper will approach the analysis process from the perspective of the RFID system components. In general, the RFID system components are: tag, air-interface, reader, network and back-end. A threat can attack one or more of these components. As a result of the proliferation of threats to the RFID data, it is important to protect the confidentiality (C), integrity (I) and availability (A) of the data. Threats to RFID data can have three types of effect on the data. The analysis will identify the threat, affected RFID component/s, its effect on the data and then mitigate the risks based on accepted practices (such as NIST800-98) [27] and ISO27001/2 (available for purchase at http://www.standards-online.net/InformationSecurityStandard.htm). ISO27001 provides guidelines on the structure and controls required to implement an Information Security Management System (ISMS). ISO27002 provides the Code of Practice for Information Security Management.

The threat analysis matrix of the RFID system can be summarized as illustrated in Table 1.

Threats	Affected RFID Component	Effect on the data	Risk Mitigation
Rogue Reader	Tag, Air-Interface, Reader	C	Reader authentication
Eavesdropping	Tag, Air-Interface	C	Encrypting the data, shielding the tag or limit the tag-reader distance
Relay Attack	Air-Interface	C, I	Using short range tags, shielding the tag or implementing the distance bounding protocol
Replay Attack	Tag, Air-Interface	C, I	Encrypting the data, shielding the tag or limit the tag-reader distance, tag authentication
Tag Cloning	Tag, Air-Interface	C, I	Tag authentication
Tracking People	Tag, Air-Interface	C	Low range tags or shielding tags, authenticating the readers or disabling the tags.
Blocking	Air-Interface	A	Detect early and localize, take appropriate action.
Jamming	Air-Interface	A	
Physical Tag Damage	Tag	A	Use protective material

Table 1. Threat Analysis Matrix of a RFID System.
The effects are: C = View confidential data, I = Manipulate data, A = Data not available.

V. CONCLUSION

As the IoT is a new paradigm (from the Internet) that includes dimensions from anytime, anyplace connectivity for anyone and connectivity for anything, the issues with the RFID infrastructure needs to be resolved. As RFID becomes more pervasive, it is the ideal technology to enable a unique identifier for each object that can be read at a distance allowing automatic, real time identification and tracking of individual objects. However, threats to the RFID system from the air interface needs to be conclusively mitigated. RFID technology is great for tracking and keeping stock of items or animals but if this is applied to humans there have to be laws and regulation to govern its operation and strong enforcement or audit to ensure compliance as it can be so easily abused. It is important to eliminate people's fears and concern before the RFID technology is wholly accepted. Thus, for RFID technology to enable the IoT and meet the pervasive and ubiquitous computing expectations, issues with the technological and social problems will have to be resolved.

REFERENCES

[1] Conner, Margery (May 27 2010). Sensors empower the "Internet of Things" pp. 32–38. ISSN 0012-7515.

[2] Sean Dodson (2003-10-09). "The internet of things". The Guardian. The Auto-ID Labs replaced the Auto-ID Center in October 2003. More precisely, EPCglobal was formed as the successor organization to the Auto-ID Center, while its sister organization Auto-ID Labs manages and funds research on the EPC technology.

[3] C. M. Roberts, "Radio Frequency Identification (RFID)," *Computers & Security*, vol.25, no.1, pp. 18-26, 2006.

[4] H. Y. Smith and B. Konsynki, "Developments in Practice X: Radio Frequency Identification (RFID) – an Internet for Physical Objects," *Communications of the Association for Information Systems*, vol. 12, pp. 301-311, 2003.

[5] http://www.iot-visitthefuture.eu/fileadmin/documents/whatisrfid/Futint-3-Internet-Of-Things_En.pdf Retrieved on July 2, 2010.

[6] Presentation "Beyond RFID – The Internet of Things" at Joint EC/EPoSS Expert Workshop 2008, 11-12 February 2008.

[7] Future networks and the internet: Early Challenges regarding the "Internet of Things," Commission Staff Working Document, Brussels, 29 September 2008, SEC (2008)2516.

[8] StephenWeis, Sanjay Sarma, Ronald Rivest, and Daniel Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems." In Dieter Hutter, G¨unter M¨uller, Werner Stephan, and Markus Ullmann, editors, *International Conference on Security in Pervasive Computing – SPC 2003*, volume 2802 of *Lecture Notes in Computer Science*, pages 454–469, Boppard, Germany, March 2003.

[9] Dirk Henrici and Paul M¨uller. Tackling Security and Privacy Issues in Radio Frequency Identification Devices. In Alois Ferscha and Friedemann Mattern, editors, *Pervasive Computing*, volume 3001 of *Lecture Notes in Computer Science*, pages 219–224, Vienna, Austria, April 2004.

[10] Rolf Clauberg. RFID and Sensor Networks: From Sensor/Actuator to Business Application, RFID Workshop, University of St. Gallen, Switzerland, September 27, 2004.

[11] Buettner, M., Prasad, R., Sample, A., Yeager, D., Greenstein, B., Smith, J. R., and Wetherall, D. RFID sensor networks with the Intel WISP. In *Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems* (Raleigh, NC, USA, November 05 - 07, 2008), pp 393-394.

[12] Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., Balazinska, M., and Borriello, G. Building the Internet of Things Using RFID: The RFID Ecosystem Experience. *IEEE Internet Computing*, Volume 13, Number 3, (May. 2009), pp 48-55.

[13] The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems. Edited by Lu Yan, Yan Zhang, Laurence T. Yang, and Huansheng Ning. Auerbach Publications 2008. Print ISBN: 978-1-4200-5281-7. eBook ISBN: 978-1-4200-5282-4.

[14] Gerd Kortuem, Fahim Kawsar, Vasughi Sundramoorthy, Daniel Fitton, Smart Objects as Building Blocks for the Internet of Things, *IEEE Internet Computing*, vol. 14, no. 1, pp. 44-51, Jan./Feb. 2010.

[15] Frank Siegemund. A Context-Aware Communication Platform for Smart Objects. In Alois Ferscha and Friedemann Mattern, editors, *Pervasive Computing*, Volume 3001 of *Lecture Notes in Computer Science*, pages 69-86, Vienna, Austria, April 2004.

[16] Friedemann Mattern. From Smart Devices to Smart Everyday Objects (Extended Abstract). *Proceedings of sOc'2003 (Smart Objects Conference)*. pp. 15-16, Grenoble, France, May 2003.

[17] 2009 Horizon Project (http://www.nmc.org/horizon)

[18] awareIT: Internet of Things & Smart Objects (http://awareit.blogspot.com/) Retrieved on July 8, 2010.

[19] First International Workshop on the Web of Things (WoT 2010) Online papers at http://www.webofthings.com/wot/2010/program.php

[20] "APPENDIX F: THE INTERNET OF THINGS (BACKGROUND)". Disruptive Technologies: Global Trends 2025. SRI Consulting Business Intelligence. Retrieved 30 May 2010

[21] Internet Reports 2005: The Internet of Things – Executive Summary, International Telecommunication Union (http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf) Retrieved June 30, 2010

[22] Ari Juels. RFID Security and Privacy: A Research Survey. *IEEE Journal on Selected Areas in Communications*, 24(2):381–394, February 2006.

[23] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan Estevez-Tapiador, and Arturo Ribagorda. RFID Systems: A Survey on Security Threats and Proposed Solutions. In *11th IFIP International Conference on Personal Wireless Communications – PWC'06*, volume 4217 of *Lecture Notes in Computer Science*, pages 159–170, September 2006.

[24] Pattabhiraman Krishna and David Husak, "RFID Infrastructure," *IEEE Applications & Practice*, June 2008.

[25] Gustavo H. P. Florentino , Heitor U. Bezerra , Hélio B. De A. Júnior , Marcelo X. Araújo , Ricardo A , De M. Valentim , Antônio H. F. Morais , Ana M. G. Guerreiro , Gláucio B. Br , Carlos A. Paz De Araújo. 2008. Hospital Automation RFID-Based: Technology Stored In Smart Cards, *Proceedings of the World Congress on Engineering 2008,* Volume II, WCE 2008, July 2 - 4, 2008, London, U.K.

[26] Wang, Fusheng and Liu, Peiya. Temporal Management of RFID Data, *Proceedings of the VLDB Conference, Trondheim, Norway, 2005.*

[27] Tom Karygiannis, Bernard Eydt, Greg Barber, Lynn Bunn and Ted Phillips, "Guidelines for Securing Radio Frequency Identification (RFID) Systems," *National Institute of Standards and Technology Special Publication 800-98*, 154 pages (April 2007).

[28] Simson Garfinkel, Ari Juels, and Ravi Pappu. RFID Privacy: An Overview of Problems and Proposed Solutions. *IEEE Security and Privacy*, 3(3):34–43, May-June 2005.

[29] Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum. The Evolution of RFID Security. *IEEE Pervasive Computing*, 5(1):62–69, January–March 2006.

[30] Pawel Rotter. A Framework for Assessing RFID System Security and Privacy Risks. *IEEE Pervasive Computing*, 7(2):70–77, June 2008.