Continuous RFID-enabled Authentication and its Privacy Implications

Stan Kurkovsky, Ewa Syta, Bernardo Casano
Central Connecticut State University
kurkovskysta@ccsu.edu

Abstract

Radio-frequency identification (RFID) technology has gained a broad popularity in many application areas including supply chain management, retail shopping and access control. We explore using RFID at the workplace and its implications to employee privacy. Continuous authentication provides the benefit of constant or highly periodic verification that the same authorized user accesses the computer system. In a case study presented here, employees use a knowledge- or biometric-based authentication scheme to gain initial entry to a computer system, while RFID is used to continuously verify the presence of a valid user. We analyze the relationship between usability of such an authentication scheme and the degree of protection it provides. We also examine the balance between the increased security brought by adopting an RFID-enabled continuous authentication system and the impact that it could have on employee privacy as a result of increased tracking of many aspects of the users' activity.

1. Introduction

RFID technology has long been used in many application areas including tracking shipments, inventory control, tracking livestock, locating missing pets, and studying wildlife. Recent years saw a rise of a wide range of applications where RFID is used to track and monitor people with a broad objective of improving safety and productivity. RFID is now used to track military and law enforcement personnel, locate lost children in amusement parks, and improve critical response time and efficiency in hospitals by tracking medical personnel. RFID tags intended for tracking people can be either worn or implanted, but either method poses significant ethical challenges to privacy that is threatened as a result of possibly constant tracking and surveillance. Applications involving subdermally implanted RFID tags and their ethical and privacy implications have been surveyed in [6,14]. The main focus of this paper is on RFID systems taking advantage of wearable tags that can be embedded in badges of clothing, their applications for employee tracking at the workplace, and the resulting tension between potential benefits and the loss of privacy.

We briefly discuss the technical background of RFID systems in Section 2; categorization of different threats to security and privacy posed by such systems is presented in Section 3. The rest of the paper examines implications of the latter to employee privacy. A broad range of privacy issues arising from using RFID at the workplace described in Section 4. We focus on using RFID not only for physical access control but also for securing information systems, which can be achieved by continuous authentication, a transparent process to verify the presence of a valid user at a computer workstation by frequently reading their RFID tag. We present a case study of such a system in Section 5 and examine possible privacy implications of continuous RFID-enabled authentication to employee tracking and monitoring outlined in Section 6. Section 7 concludes the paper with a summary.

2. RFID background

RFID is often viewed as a replacement for barcodes due to three distinct advantages. Unlike barcodes that provide information about the type of object, RFID offers a unique identification capability by providing a serial number of the object. Barcodes require a direct line of sight to be scanned, while RFID tags can be read through non-metal obstacles and from a longer distance. Additionally, RFID readers can communicate with multiple tags at once enabling them to scan an entire shopping cart or a shipping container.

RFID technology relies on two components: a tag (transponder) and a reader (transceiver). RFID tags typically contain an antenna and circuitry with limited computational functionality and small storage. Unlike more expensive active RFID tags that use a battery or an external power source, passive tags use the electromagnetic field induced by the reader to power up their circuitry and create a radio-frequency signal.

Depending on the tag features, including their power source and memory, RFID technology is divided into four classes [21]. Different types of tags operate at different frequencies and consequently have different read ranges, bandwidth and capability to penetrate barriers. The read range of a tag also depends on other factors that include size and shape of the antenna, and interference from other electrical devices. A number of environmental conditions can also impede the read range of a tag, as well as

degrade the quality of tag/reader communication. Ambient radio noise, nearby radio-reflective (metals) and radio-absorbing (liquids) objects can also greatly reduce the read range of an RFID tag. In particular, since the human body consists primarily of liquids, it may significantly reduce the read range of ultra-high frequency (UHF) tags if the radio signal has to travel through it. Greater read ranges and stronger signal penetration capability pose a significantly higher threat to personal privacy in an RFID-enabled system. Consequently, it is important to minimize the tag/reader distance by choosing the standard that has the smallest read range sufficient for a particular application [20].

3. Characteristics of RFID security and privacy

It is possible to identify four basic use cases of an RFID system [12]: *identification*, the most basic feature involves retrieving a unique descriptor of an item; *alerting* involves taking an action based on the obtained information (e.g. when a customer with an unpaid item is leaving the store); *monitoring* is enabled by multiple readers that can track the movement of a tagged object in space in time; and *authentication* establishes the presence of a valid tag, which is typically implemented by a cryptographic protocol supported by the tag's circuitry. Technical aspects of RFID tag/reader communication can be characterized using three dimensions of quality: *correctness* determines that the tag is correctly identified by the reader; *security* ensures that the information transmitted between the tag and the reader is secure from adversaries; and *privacy* guarantees that the meaning of the information transmitted between the tag and the reader is not revealed to adversaries. From a broader perspective, as shown in Figure 1, the issue of user privacy in the context of RFID systems is two-fold: one relates to unauthorized tag readouts by adversaries, while the other is characterized by the degree to which consensually collected tag readouts are used for tracking and surveillance.

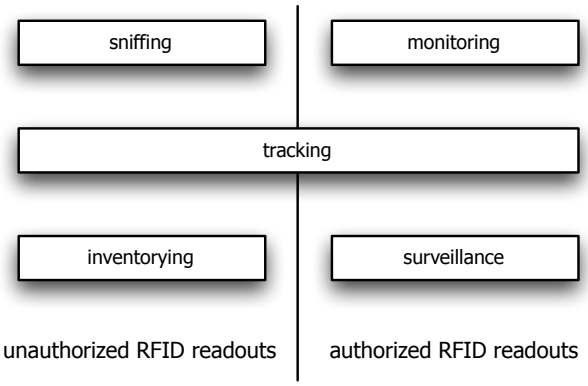

Figure 1. Loss of privacy in RFID systems

The main privacy concerns of RFID technology stemming from unauthorized RFID readouts are related to information leaking, tracking and inventorying [11,16,23]. An RFID tag typically responds to the reader without alerting its bearer. As a result, a person carrying an RFID tag could broadcast a unique serial number to all readers in the vicinity. It is difficult to implement strong and reliable authentication and encryption on RFID tags due to their weak computational power [5,11]. As a result, it is possible for RFID tags to leak information uniquely identifying a person or pertaining to their property. Collected over time, such information effectively enables tracking of that individual. Privacy is threatened further if the tag's serial number is linked to personal information. Inventorying refers to a situation when an RFID reader can covertly collect information about the type of object to which a tag could be attached, which is a very realistic scenario in the realm of EPC tags [3,10,19]. Consequently, an eavesdropper could infer some generalized information about the person carrying these RFID tags.

The key to protecting RFID systems from unauthorized readouts is implementing a secure communication channel between the tag and the reader. Fundamental objectives of information security, such as confidentiality, integrity, authentication, and anonymity typically cannot be achieved in RFID systems unless they incorporate special security techniques [11]. In particular, RFID technology is open to the following security threats [25]: eavesdropping, hotlisting, replay and denial of service attacks, tag cloning, and data forging. Eavesdropping is possible as the tag automatically responds to an inquiring reader. A malicious user can easily obtain the data saved on the tag and use it to track individuals or objects, to perform a relay attack (an adversary acts as a man-in-the middle between a tag and a reader) or even clone the tag. A denial of service attack is a well-known weakness of RFID-enabled solutions based on simple passive tags. The attack can be due to physical characteristics of the reader that could be blocked by

water or metal, too many different tags in its range, or a failure of the device.

Specific issues of preventing unauthorized RFID readouts and consequently increasing RFID security are beyond the scope of this paper, although, a number of different techniques that might prevent misuse of RFID have been proposed, e.g. [3,5,10,21,23,25]. Our main interest, however, is to examine a potential loss of privacy as a result of authorized RFID readouts, and in particular, how a large-scale deployment of an RFID system could impact the privacy of its users.

4. RFID at the workplace

A significant amount of research work has been dedicated to consumer-oriented aspects and concerns of RFID technology and the ways in which it can be exploited to produce a higher amount of personal information that can be used by retailers of goods and services (e.g. [10,17,24]). One of the many uses of RFID technology outside of retail involves physical access control, which consequently enables tracking and monitoring of employees. At many workplaces, employees are required to wear uniforms or badges, which can be easily embedded with RFID tags. With or without the knowledge of employees, these tags can be used to measure the amount of time an employee spends in front of their computer, on breaks, or in the restroom, as well as automatically record the employee's arrival and departure time. These scenarios are a reality and are used every day as a proven element to improve business efficiency, increase workplace security, and provide additional avenues for the employers to monitor their employees [1,8,9]. In addition to tags embedded in uniforms and badges, implantable RFID transponders have been successfully used in several military and law enforcement scenarios [11,13].

4.1. Legislative background

An excellent survey of current legislature and policies regulating the use of RFID technology for tracking and monitoring of employees can be found in [8]. Although some states and nations regulate the use of implantable RFID tags in humans [4], there are no legislative acts or courts decisions specifically regulating the use of RFID technology at the workplace. Privacy implications of using RFID in a place of employment are a subject of an ongoing debate and there are a number of open questions surrounding this issue. For example, in 2007, the European Commission established an RFID Stakeholders Group in order to study the use of RFID technology at the workplace and to produce recommendations detailing related privacy and security issues. In 2006, US Department of Homeland Security published a report that concluded that privacy issues of using RFID for tracking individuals outweigh the benefits of this technology [27]. In 2008, Office of Privacy Commissioner of Canada prepared a consultation paper that outlines a number of good practices for the use of RFID at the workplace [15]. This report lists ten principles that should govern the use of RFID by businesses: accountability; identifying purposes; consent; limiting collection; limiting use, disclosure, and retention; accuracy; safeguards; openness; individual access; and challenging compliance.

4.2. Physical security, safety and privacy

Generally, employees expect some degree of privacy, even if they are located at the employer's premises and are using the equipment provided by the employer. At the same time, people usually consider giving up some privacy as a part of their employment. Employees are typically required to provide some basic information about themselves to the employers to put them on payroll; they may also need to share some of their medical records to ensure they receive full benefits. Furthermore, surveillance technology has long become a ubiquitous element of the modern workplace. Employers routinely monitor electronic communications of employees and use biometric and electronic technology to collect personal information about them. Employers typically cite improved workplace safety and security, increased productivity, minimized liability risks and reduced theft as a rationale for such tracking and monitoring.

Safety and security could be improved by replacing keys, access cards or other access control technology with RFID-enabled systems that would allow only authorized employees to enter critical or restricted areas. RFID cards enable fine-grained security control by authorizing access to the bearer. At the same time, data about each attempted or successful access authorization can be collected and analyzed. Such data typically contains a specific location and a precise timestamp along with a unique ID of the card that can be linked to its bearer. When put together, this information may reveal a larger picture of the card bearer's behavior. User privacy is further threatened when these records are linked to other databases.

RFID-enabled access cards can be easily integrated with other security or access control systems; they can be used to control access to the entire enterprise or to a limited number of locations. Access cards may require additional forms of verification; providing a personal identification number (PIN) ensures that the bearer of the card is the legitimate user of the card. RFID readers could also trigger additional surveillance technology (such as video cameras) whenever an employee enters or leaves an access-controlled area. RFID could also enable collecting personally identifiable information that may be used to investigate misconduct or violations of work rules.

Measuring the amount of time and performed labor, and adjusting the workflow accordingly can increase employee performance and productivity. For example, on production lines or different phases of the supply chain, data collected from RFID-enabled tracking system could create a vast amount of data that could be analyzed to identify potential bottlenecks and therefore optimize the production process and reduce loss.

RFID technology provides many advantages for mobile asset management. In addition to asset tracking, usage data for individual items can be collected and used for more optimal asset allocation. Additionally, attaching RFID tags to items and products can minimize internal theft risks. Employers can further minimize their legal liability risks by using RFID tracking data; for example RFID-generated data could establish location of employees during an accident and prevent frivolous liability claims.

RFID can be used to address a diverse set of business challenges. In particular, with decreasing costs of RFID technology, it becomes ever more appealing to employers as a tool for employee monitoring with a high output volume of personally identifiable data. At the same time, application of this technology raises a number of legitimate questions from employees concerned about the loss of their privacy.

4.3. RFID and information system security

RFID appears to be especially useful in an environment with a high number of different computing devices users may need to access. A unified authentication mechanism facilitates a scheme for coherent access control. As a special case, RFID can be used to control access not only to secured computer workstations, but also to protected information resources. These new scenarios of using RFID at the workplace can lead to more complex implications for employee privacy as the amount of data detailing their activities continues to grow. To illustrate some of these scenarios, the following section describes an RFID-enabled system for continuous authentication.

5. Case study: RFID-AM

The system discussed here, RFID-enabled authentication middleware (RFID-AM), provides *composite continuous authentication* for enterprise desktop users (a detailed low-level description of RFID-AM architecture can be found in [26]). In a typical scenario, a valid user initially may log in to the workstation using a password, but the ongoing presence of that user is continuously verified by reading their RFID tag that is embedded in the user's ID card, name tag, or a badge. *Composite authentication* combines two or more user authentication methods [2]. Ideally, these methods should take advantage of different authentication factors: knowledge-, possession-, or biometrics-based, which enables the system to achieve a higher degree of accuracy while making it more transparent to the end-user. *Continuous authentication* does not stop after the initial login, but is used in a loop to verify the presence and participation of the authenticated user throughout the session [22]. In RFID-AM, initial (point of entry) authentication could be achieved using a knowledge-based method, such as password authentication. Continuous authentication is implemented using RFID tags that could be carried by employees, a possession-based method that is unobtrusive and transparent and does not require any explicit interactions with the user. At predetermined intervals of time, RFID-AM continuously verifies the presence of a valid user by attempting to read their RFID tag. At any moment when RFID-AM cannot verify the presence of a valid user (i.e. it is unable to successfully identify a valid RFID tag), access rights of the user are revoked. To increase the degree of protection offered by the system, user credentials could be verified 'just in time' whenever a file is accessed on an encrypted file system. Consequently, when the user logs out of the system, walks away, or if user credentials cannot be verified for any other reason, all open files are encrypted and the system is locked.

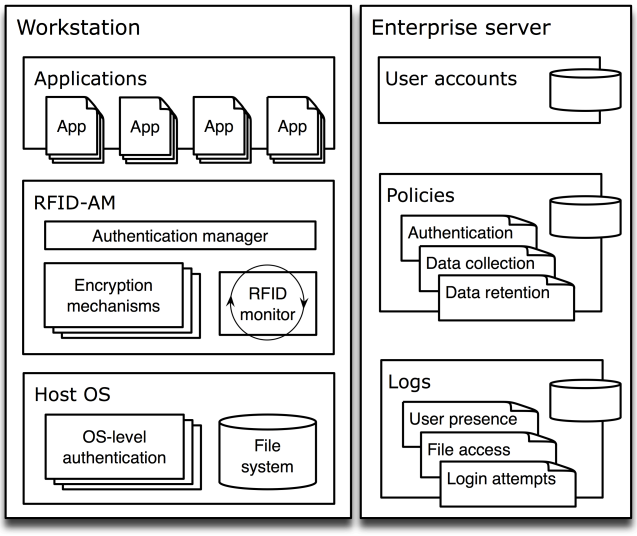

Figure 2. Organization of RFID-AM

As discussed in Section 2, RFID read range is a very important factor that helps maintain the balance between the efficiency of the system and a potential loss of privacy that could result from its use. RFID access cards and tokens are usually carried in a wallet, on a lanyard or on a keychain; the chosen read range should ensure that the user would not be required to put the transponder in a

close proximity of the transceiver while using a secured workstation. At the same time, RFID read range should be short enough to minimize interference from other RFID systems deployed at nearby workstations while providing a guarantee that whenever the authorized user leaves their workstation it would enter a locked state. Adequate read range, small form factor, and cost-effectiveness make Class 1 Gen-2 RFID tags a suitable choice for these purposes [7,25]. Such tags are typically used to store an Electronic Product Code (EPC), a unique number that identifies the manufacturer, serial number of the product and its type; the length of EPC can range from 64 to 256 bits. Dependent on the complexity of the transceiver, it may also contain two 32-bit passwords: the 'access' password used to access the EPC, and the 'kill' password used to permanently disable the tag.

RFID-AM is a middleware offering intermediary services between the host operating system and software applications, as shown in Figure 2. RFID-AM takes advantage of authentication features provided by the host operating system to augment RFID-enabled possession-based authentication with knowledge- or biometrics-based authentication. As a result, operating system and built-in hardware features can provide an efficient point of entry authentication (e.g., many top of the line laptops are equipped with fingerprint scanners). At the same time, RFID-AM implements transparent continuous authentication and transparent data encryption at the file system level assuring access to encrypted files to authorized users while they are present at the workstation.

RFID reader continuously checks the presence of a tag and verifies its validity using a secure tag/reader authentication protocol. A survey of existing authentication protocols for RFID developed in recent years can be found in [18]. RFID-AM may time out while acquiring RFID credentials due to one of three factors: if no RFID tag is present; due to failure of the authentication protocol because of interference; or due to authentication failure if an invalid RFID tag is present. If interference problems are detected, RFID-AM may query the reader several times in attempt to establish a successful communication with the tag before finally timing out. A timeout event leads to authentication failure. Since it is impossible to predict when a device might fail, recovery procedures have to be in place. RFID-AM uses multi-factor authentication; therefore, in case of a RFID reader failure (which could also be due to a denial of service attack), users could be authenticated using a password.

To test the viability of the approach described above, a fully functional prototype of RFID-AM was implemented and subjected to a series of experiments. These test were aimed to verify the reliability of continuous authentication implemented using a Class 1 Gen 2 RFID system used in conjunction data encryption (using AES, DES, or Blowfish algorithm). In particular, the tests were designed to analyze the timing overhead imposed by encryption algorithms and RFID hardware under a range of stress conditions stemming from the movement of the RFID tag in and out of the reading range. Further low-level technical details of RFID-AM architecture, implementation of its prototype, and detailed test results can be found in [26].

Enterprise-level user profiles used by RFID-AM determine authentication policies applicable to each user account; they establish file ownership and access relationships, and associate each user account with one or more RFID tags. These policies could also be used to select a particular file encryption mechanism employed by RFID-AM.

Enterprise-level user authentication policies must determine a set of parameters applied to the process of verification of credentials supplied by the users for point of entry and/or continuous verification. Continuous authentication policies need to specify the frequency of querying the presence of a valid RFID tag and actions to be taken if it is not detected within a certain timeout period.

RFID-AM could generate a sustained stream of data documenting many aspects of end-user activity. This data includes all user authentication updates performed by RFID-AM at periodic intervals of time. .Similarly, authentication update records include a timestamp, a workstation ID, a user ID, and authentication outcome code (e.g. success, failure due to insufficient security privileges). Enterprise-level policies must be established to determine rules for data collection and retention. Data collection policies indicate what types of records or their subsets are to be retained. Data retention policies need to apply similar rules concerning how long these records are to be stored in the respective logs. Privacy implications of establishing specific policies concerning such data are discussed in the next section.

6. Privacy implications of RFID at the workplace

RFID technology can be undoubtedly useful and beneficial in many situations and scenarios, including those described in Section 4; furthermore, it could be used to locate employees in emergency situations and resolve liability or criminal disputes by establishing precise location of employees in space in time. However, use of RFID technology at the workspace raises a number of legitimate concerns.

As RFID technology is introduced at the workplace, it may evolve over time as the personally identifiable information detailing employee location and precise time could be used for new purposes resulting in 'function creep'. Tracking of more activities and discovering new aspects of such tracking could lead to increased

surveillance and using the technology for purposes that may not be related to employment.

With RFID-enabled access cards employers may choose to track physical location of their employees with a varying degree of granularity, ranging from buildings to individual rooms. Although a continuous RFID-enabled authentication system may only be intended for use in close proximity to a computer workstation, the same technology can be easily adapted for tracking employees with a much finer degree of granularity – from rooms to specific locations, such as a desk or a cubicle. Because RFID readers can typically identify multiple tags at once, even with an appropriately chosen RFID read range, a continuous authentication system may be capable of recording detailed presence information about multiple people without installing any additional RFID readers. Consider a situation when employee Alice is authenticated at her workstation and employee Bob visits Alice's cubicle so that she can show Bob something on her computer monitor. Without any disruption to Alice's authentication, the system may be capable of reading Bob's RFID tag and recording his presence near Alice. Using RFID-AM, an employee can be continuously authorized to an appropriate workstation, but can the same system be used for tracking people across other locations? With the help of RFID, it may be possible not only to monitor employee location, but it could also enable tracking of interactions among employees by matching their close proximity in time in space. Can an employer use a 'blanket policy' to track employees everywhere and for every purpose or just for access authorization to enter a specific building or log in to a workstation?

With a plethora of data collected by an RFID-enabled access control system, employers may be inclined to subject it to further analysis by data-mining the collected records. For example, using the data collected by a continuous authorization system, employers will have a fine-grained record of the employee's use or proximity to a computer workstation. Precise clock-in and clock-out time, as well as any absence of the employee from the workstation can be recorded – from lunch or restroom break to a 'stretch break' from sitting in front of the computer to get some physical activity. The amount of time spent by each employee at the workstation is the most obvious metric that can be analyzed. As a consequence, this may encourage some employees to focus on the quantity instead of quality of work. If the time spent at the workstation is monitored by a system similar to RFID-AM and if the management is likely to analyze employee productivity based on that measure, employees might be encouraged to simply spend their time sitting by their workstations, but not necessarily engaged in any productive work. As a result, employees may perceive such a system as a means of control over them rather than a security measure.

It is possible to envision a scenario when the comparison and analysis of patterns and work habits of different employees could lead to enabling managerial decisions based on these factors. This is especially troublesome if the data collected by an RFID-enabled monitoring system is linked to personal data in other databases that may exist within the enterprise, e.g. medical or personnel records. For example, behavior analysis of a particular employee could show that they spend more time in the restroom than others. This could possibly be due to a medical condition that may be documented in the employee file, but is off-limits to the immediate management or security personnel who may have access to the data collected by the monitoring system. What if that employee preferred not to discuss their medical condition, but the management assumed that the employee's performance could suffer due to these frequent breaks? As a result, the employee might face a dilemma of either having to disclose their medical condition, inventing an excuse for visiting the restroom frequently on a regular basis, or possibly facing some sanctions from the management.

Furthermore, since employees are required to wear their RFID badges or carry their RFID-enabled access cads at all times while at the employer's premises, they may choose not to remove them and keep carrying these RFID tags elsewhere. This may open the door for a constant observation and surveillance not only at the place of employment, but possibly at other locations due to authorized tag readouts or due to sniffing the tags by eavesdroppers.

Enterprise policies must exist to govern how the data collected by RFID access control or monitoring system can be used [1]. Such policies should establish what personnel (or which enterprise units) can access these records and for what purpose, whether and how this data can be linked to other enterprise records, how this data is protected, how long this data should be retained, how this data and its use is audited to ensure compliance of the enterprise units responsible for its collection. Without such policies, employers could disclose collected information about employees without their knowledge or consent and/or use it for many purposes that could be very different from the original intent. Such enterprise policies [5,12] should bring more clarity to many of the privacy threats and issues including those outlined here. Combined with the appropriate legislative regulation aimed at safeguarding privacy, enterprise-level policies have a strong potential for preventing many possible 'dark scenarios' of RFID data misuse [9].

7. Summary

Introduction of RFID systems at the workplace has shifted the balance between information and physical security, public safety and personal privacy and convenience. Securing access to data and information resources using continuous authentication, physical access control to rooms and buildings, investigation of employee misconduct, and locating employees in emergency situations are among the most obvious design priorities in RFID-enabled access control systems. But ultimately, information and physical security may trump personal privacy [1].

Practical obscurity is an effective privacy barrier made by a significant effort needed to find some information that may be publicly available. For example, finding some public records kept on paper at a municipal office, which might require a manual search and a substantial investigative effort, provides a substantial degree of privacy. Making such records available online removes any such barriers. Similarly, RFID systems at the workplace eliminate practical obscurity by creating a detailed record of employee movements and activities over time. Continuous monitoring adds another dimension to the matrix of data that can be collected using RFID.

RFID-enabled access control systems are used to improve physical and information security at the workplace. But despite the advantages of such systems, their use raises a question whether the advantages of such systems are worth the intrusion. What kind of data is being collected about the employees and whether it is only used for the intended purposes? Answering these questions requires making a priority between moral values (privacy or lack thereof) and business values (productivity, profitability, security of intellectual property, etc.) Weighing business virtues (or security – national, physical, or information security) over a moral value of privacy can easily lead to the rise of surveillance society, especially in the absence of legal or policy regulations.

11. References

[1] E. Balkovich, T. Bikson, G. Bitko, "*9 to 5: Do You Know if Your Boss Knows Where You Are?"* Technical report, RAND Corp., 2005.

[2] N. Clarke, S. Furnell S, "A Composite User Authentication Architecture for Mobile Devices", *Journal of Information Warfare*, 5(2), pp. 11-29, 2005.

[3] B. Fabian, O. Günther, "Security Challenges of the EPCglobal Network," *Communications of the ACM*, 52(7), pp. 121-125, 2009.

[4] A. Friggieri, K. Michael, M.G. Michael, "The Legal Ramifications of Microchipping People in the United States of America – a State Legislative Comparison," *2009 IEEE International Symposium on Technology and Society*, pp.1-8, 2009.

[5] S.L. Garfinkel, A. Juels, R. Pappu, "RFID Privacy: an Overview of Problems and Proposed Solutions," *IEEE Security & Privacy*, 3(3), pp. 34- 43, 2005.

[6] D.J. Glasser, K.W. Goodman, N. G. Einspruch, "*Chips, Tags and Scanners: Ethical Challenges for Radio Frequency Identification*", Ethics and Information Technology, 9(2), pp. 101-109, 2007.

[7] D. Henrici, "*RFID Security and Privacy: Concepts, Protocols, and Architectures*". Springer, 2008.

[8] W.A. Herbert, "The Impact of Emerging Technologies in the Workplace: Who's Watching the Man (Who's Watching Me)?" *Hofstra Labor and Employment Law Journal*, 25(2), pp. 355-393, 2008.

[9] P. Hert, S. Gutwirth, A. Moscibroda, D. Wright, G.G. Fuster, "Legal Safeguards for Privacy and Data Protection in Ambient Intelligence," *Personal Ubiquitous Computing*, 13(6), pp. 435-444, 2009.

[10] H. Holtzman, S. Lee, D. Shen, "OpenTag: Privacy Protection for RFID", *IEEE Pervasive Computing*, 8(2), pp. 71-77, 2009.

[11] A. Juels, "RFID Security and Privacy: a Research Survey", *IEEE Journal on Selected Areas in Communications*, 24(2), pp. 381-394, 2005.

[12] M. Langheinrich, "A Survey of RFID Privacy Approaches", *Personal and Ubiquitous Computing*, 13(6), pp. 413-421, 2009.

[13] A. Masters, K. Michael. "Humancentric Applications of RFID Implants: The Usability Contexts of Control, Convenience and Care," *The 2nd IEEE International Workshop on Mobile Commerce and Services*, pp. 32-41, 2005.

[14] M.G. Michael, K. Michael, "Uberveillance: Microchipping People and the Assault on Privacy," *Quadrant*, vol. LIII, pp. 85-89, 2009.

[15] Office of the Privacy Commissioner of Canada, "*Radio Frequency Identification (RFID) in the Workplace: Recommendations for Good Practices*", http://www.priv.gc.ca/information/pub/rfid_e.pdf

[16] M. Ohkubo, K. Suzuki, S. Kinoshita, "RFID Privacy Issues and Technical Challenges", *Communications of the ACM*, 48(9), pp. 66 – 71, 2005.

[17] A.R. Peslak, "An Ethical Exploration of Privacy and Radio Frequency Identification", *Journal of Business Ethics*, 59(4), pp. 327-345, 2005.

[18] S. Piramuthu, "Protocols for RFID Tag/Reader Authentication". *Decision Support Systems*, 43(3), pp. 897-914, 2007.

[19] A. Razaq, W.T. Luk, K.M. Shum, L.M. Cheng, K.N. Yung, "Second-Generation RFID," *IEEE Security and Privacy*, 6(4), pp. 21-27, 2008.

[20] P. Rotter, "A Framework for Assessing RFID System Security and Privacy Risks," *IEEE Pervasive Computing*, 7(2), pp. 70-77, 2008.

[21] S. Sarma, S. Weis, D. Engels, "*RFID Systems, Security and Privacy Implications*", AutoID Center, MIT, Cambridge, MA, Tech. Rep. MIT, AUTOID-WH-014, 2002.

[22] T. Sim, S. Zhang, R. Janakiraman, S. Kumar, "Continuous Verification Using Multimodal Biometrics," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4), pp. 687-700, 2007.

[23] B. Song, C.J. Mitchell. "RFID Authentication Protocol for Low-cost Tags", *1st ACM Conference on Wireless Network Security*, Alexandria, VA, USA, 2008, pp. 140-147.

[24] S. Spiekermann. "RFID and Privacy: What Consumers Really Want and Fear", *Personal and Ubiquitous Computing*, 13(6), pp. 423-434, 2009.

[25] H.-M. Sun, W.-C. Ting, "A Gen2-Based RFID Authentication Protocol for Security and Privacy," *IEEE Transactions on Mobile Computing*, 8(8), pp. 1052-1062, 2009.

[26] E. Syta, S. Kurkovsky, B. Casano, "RFID-Based Authentication Middleware for Mobile Devices," *43rd Hawaii International Conference on System Sciences*, 2010.

[27] US Department of Homeland Security, Data Privacy & Integrity Advisory Committee. *The Use of RFID for Human Identify Verification*, Report No. 2006-02, http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf