PRIVACY AND SECURITY CHALLENGES OF RFID

Smriti Pande

Mike Unuakhalu

Abstract

This paper reviews the background of Radio Frequency Identification Device (RFID) as well as the ethical foundations of individual privacy. A number of applications were also explored with the intention of identifying the technology's benefits and possible misuses. The authors offer an overview and discussion of the most important ethical issues concerning RFID, and describe and examine some methods of protecting privacy. Additionally, the paper examines the security risks associated with RFID technology, and privacy issues and challenges that they present to the operations of a business that implement such technology.

1. INTRODUCTION

Inventory tracking and management is of utmost significance to companies as the eradication of procedural and informational bottlenecks can immensely amplify the competence of their inventory decisions and order timing.Technology is ineludible in every sphere of life today; it has always made things easier. The use of technology such as Radio Frequency Identification Device (RFID) can assist companies to improve their business processes locally, nationally, and globally. It is a potent promising technology that allocates companies to accomplish total business appearance by identifying the identity, location and state of assets, tools, inventory, people and more companies can get the most out of processes and reduce operational costs. It is the biggest technology advancement in inventory management with the placement of microchips in product containers, cartons and packaging, shared with the use of special sensors in warehouses or on store shelves that notify a central inventory management system as to shipment coming, product purchases and the need to restock catalog, corresponding via wireless means.

RFID is an emerging valuable tool to automating identification and inventory management. RFID appears as a tag containing the Electronic Product Code data (EPC), which includes various details aboutthe tagged product. RFID technologies have growing visibility in the business processes, facilitating innovation, and escalating competitiveness.

RFID technologyoffers considerableprospective benefits tocompanies and therefore it will come as no surprise that there are a good many RFID trials underway. But, the disturbing news for those championing the technology is thatthese trials have brought faster benefits than anticipated, and the majority has progressed to several applications, raising questions about the privacy issues realized. Since the prospective applications of RFID systems are abundant, it is crucial to address the consumer perspective issues that have resulted in barriers to RFID implementation.

1.1 Background

A RFID system consists of three main components: a tag, a reader, and a computer system. Usually, RFID tags are made by combining a radio antenna with a microchip and then adjoining the two with a protective case. A tag is a small and inexpensive microchip that releases

an identifier in reaction to a query from a nearby reader.RFID tags may be the size of a grain of rice (or smaller), and have built-in logic (microcontroller or state machine), a coupling element (analog front end with antenna), and memory (pre-masked or EEPROM). Passive tags are power-driven entirely by their reading devices, while active tags enclosesupporting batteries on board.These tags are generally able to store up to two kilobytes of information. Accumulated data may comprise product identification, the manufacture date, and the cost of the product. These tags can then be linked individually to the physical product itself or to the product packaging (Glasser, et al. 2007; Rieback 2006). While the useful information is accumulated inside of the tag, it needs a reader to identify, accumulate, and decode the information. At last, a computer system is used to interpret, sort out, and accumulate the collected data in a significant way.

Once the tag isconnected to an object, this small radio can send information particularly about the object to acomputer network. The EPC is a unique number that recognizes a specificitem in the supply chain and is stored on an RFIDtag. Once the EPC is recovered from the tag, it canbe linked with dynamic data such as where an item initiated from or the date of its production or its current location.The ID serial number transmitted by the RFIDtag contains traditional information contained in a printed barcode, as well as a unique serial number for that tag. Barcodes today are usually scanned at the store, during the purchase, not afterwards. However,RFID transponders are, in many cases, eternally part of the product and intended to react when they receive a signal(Krishna & Husak, 2007).

1.2 Infrastructure

The RFID infrastructure constitutes of the elements that controls the devices and tag data. Consumers of the data are the client network elements (usuallyend-user applications). The network elements connecting the tag and the clients form the tool that carries tag data to the applications, and transmit tag operational commands to the RFID devices. At a minimum, the RFID infrastructure (Figure 1) includes tags, readers, RNCs (Reader Network Controllers) and applications running for example, on enterprise servers. Additionally, other devices could also be in the network such as RFID/bar code readers, I/O devices (such as electric eyes, light stacks and actuators), bar code/smart label printers and applicators. Usually, a reader conveys an RF signal in the direction of a tag, which reacts to the signal with another RF signal containing information

recognizing the item to which the tag is connected, and possibly other data. The tag may also comprise extra field-writable memory store, and integrated transducers or environmental sensors for providing data such as the temperature or humidity of the environment(Krishna & Husak, 2007). The reader obtainsthe information and supplies the tag data to the RNC which may do further processing before transferring the data on to the applications.

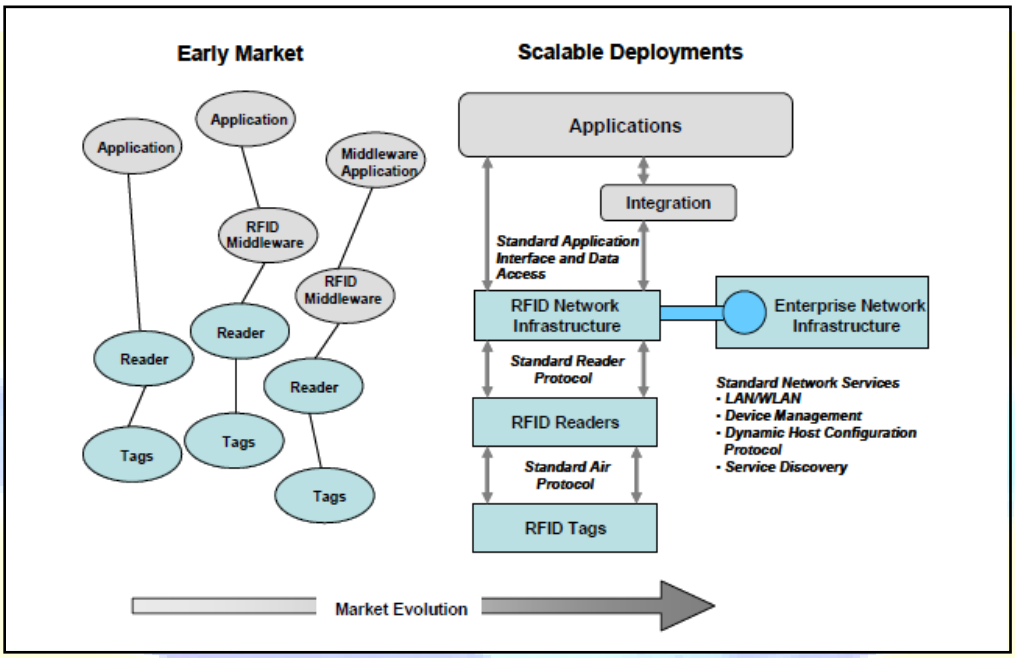

Figure 1: Evolution towards RFID infrastructure(Krishna & Husak, 2007)

2.CHALLENGES

RFID may provide the prospect for companies to enhance customer service or initiate greater value up the supply chain if used creatively and with transparency for consumers. Merging a clear perceptive of business drivers with innovative applications will allow companies and suppliers to truly benefit from RFID (Alder, 1998).

The wider benefits of RFID in the supply chain are often overstated when current performance and different initiatives are measured. For example, maintaining product availability on the shelf is vital for any retailer. The leading grocery multiples already use Electronic Point of Sale(EPOS) data from checkouts to drive store replenishment, and guarantee that staff put shelf replenishment as a high priority. RFID does represent a prospective solution

to improve this process – if every individual product was RFID tagged, and every shelf position also tagged, then automatic alerts could be produced to update the relevant staff that a specific shelf needed restocking. But the cost of that would make it a non-starter.

There are several barriers to RFID implementation. These barriers range from a lack of industry-wide standards, comprehending of total costs, adoption of suitable and essential infrastructures, and consumer privacy violation concerns, all of which result in managers, organizations, and consumers being weary of the benefits and usages of the acceptance of this technology. In the absence of addressing these issues, the successful implementation and acceptance of RFID technologies will continue to prevent companies from achieving the return on investment (ROI) that the technology promises. Project leaders place their efforts mainly into the RFID technology component, with less attention to apprehension of their customers as well as the barriers resulting from data management and privacy challenges; retailers, however, must concentrate on extenuating the privacy concerns of their current and potential customers. If customers and privacy advocates have methods to authenticate the disabling of the tag, the RFID technologies could be used to avert supply chain problems such as incomplete orders, misplaced products, and theft, while still preserving acceptable levels of consumer privacy (Lockton& Rosenberg, 2006).

3.SECURITY AND PRIVACY

As the manufacturers and retailers are preparing to embrace RFID technologies, the primary challenge are the reluctant knowledgeable consumers. The RFID unknowns and fallacy have generated tremendous privacy concerns that are averting consumers from accepting the new technology. One issue is the likelihood that readers can be hidden and personal objects can be identified on a person without their knowledge or permission which is an infringement of privacy. Consumers fear thatthe tiny chips, which are fitted with even tinier antennas that beam unique identification information to scanners, could be used to track how they shop and what they buy(Glasser, et al. 2007).

Generally recognized as a basic human right, privacy relates to the capability of a person to act as an individual, apart from an individual role in society,improving the ability for personal function without embarrassment or review, even if it sometimes sets the individual's interests at odds with those of the world around him or her.Privacy, then, can be broadly defined as the power to selectively reveal oneself tothe world. According to the Oxford Handbook of Practical

Ethics by Anderson and Labay in 2006, moral philosophers maintain that respecting the many forms of privacy is paramount for respect for human dignity and personhood, moral autonomy, and a workable community life. The importance of privacy is partly a matter of psychological health and comfort.

Anonymity and privacy are problems, especiallywhen there are no standards on whether the tags will be disabled or left enabled by default. Tags must not compromise the privacy of consumers. The privacy threat comes when RFID tags remain active once an individual leave a store. Once they buy RFIDtaggeditem, they could be tracked anywhere they travel. Currently, tags respond to any signal. Anything afirm's transceiver can detect can also be detected by unauthorized transceivers. The privacy issuebecomes more serious when the RFID tags are used in smart cards, badges provided to an individual when they attend conferences (Anderson & Labay, 2006).

Both government and commercial uses demand privacy issues that will need to be dealt with. Business entities might collect and store information without proper consent or data protection and utilize it in ways opposing to the consumer's wishes. Concerns about most government tagging are parallel, relating the fear of tracking and surveillance and of information assembling and dissemination for purposes contrary to individual interests,though the specific concern varies from application to application.Many of the worries surrounding these concerns have to do with the control ofinformation. Chips read by unauthorized readers could permit sensitive informationsuch as credit card numbers and medical histories to become readily accessible.

3.1 Ethical Issues of Implantable RFID Tags in Humans

The first implantable RFID system for humans to reachthe market was invented by the Digital Angel Corporationin South St. Paul, MN, a manufacturer of RFID tags usedin pets and livestock, and by its completely owned subsidiaryVeriChip Corporation in Delray Beach, FL.In 2004, the United States Food and Drug Administration classified the VeriChip Health InformationMicrotransponder System as a class II medical device, clearingits way to market.The VeriChip Corporation is endorsing its system,which it callsVeriMed, for use by patients who

might handto healthcare facilities unresponsive and incapable to presentidentification. Some of the candidates are patients withAlzheimer's disease or severe mental illness, but the company'spromotional literature mentions also patients withcoronary artery disease, chronic obstructive pulmonary disease,diabetes mellitus, seizure disorders, cognitive impairment,who have suffered a stroke (Foster & Jarger, 2008).

There are, however, two areas of present ethical concernthat are distinctive to implanted RFID chips, and in particularthe VeriChip byFoster & Jarger, 2008:

- Disclosure of Risks: Acentral ethical principle embraces that individuals have a right to know about possible sideeffects of a treatment, in this scenario implantation of a chip. Should VeriChip have revealed the results of the rodent studies prior to anti-chip activists elevated this issue? A finding of carcinogenic effect of an implant in rodents is, at least, indicative of the likelihood of a similar effect in humans.
- Coercion: If receiving an RFID tag were purely an issue of consumer choice, few severe ethical issues would occur apart from generic concerns regarding consumer protection.Thus, for example,a consumer might reasonably choose to be chipped most likely not in a tattoo parlor to avoid having to carry a credit card or RFID tag on a key chain. By far the most significant and distinctive ethical issues associated with implanted RFID transponders resultfrom the very real prospect that the chips might be implanted under real or implied coercion, coupled with thedeep aversion or at least discomfort with which many individualsview the technology.

3.2 Other RFID Associted Risks

RFID benefits may be outshined by several prospects for accidental or intentional exploitation of the technology and its supporting systems, alongside abroad range of matterslinking to system and dataintegrity, personal well-being, and privacy. Tags may beimitated, cloned (duplicated), exchanged, damaged,deliberately disabled (in some cases evenremotely), or otherwise distorted. RFID technology canbe compromised if used with insecure systems.This is predominantlydemanding in sensitive environmentsif RFID tags use unencrypted or (as in the case of theimpending U.S. passports) weak encryption protocols.Additionally, different issues associated to pervasivesecurity problems can direct to larger privacy violationscommitted by insiders and outsiders, such asexploitation of databases associated with RFID tag informationor derived from the circumstance in which the tagsare

used(Lockton& Rosenberg, 2006). System-related examples comprise intrinsicsecurity susceptibility of the ancillary computer systems,insufficient user and operator certification,and overly broad system and database authorizations.Such circumstances can generate widespread opportunities formisuse of the accompanying database information.For example, many prospects will exist for aiming particular victims, widespread selective data mining,and sweeping up entire databases. Possible intention forsuch misuses might consist of robbery, identity theft,fraud, harassment, and blackmail, for example.At the fundamental computer-science level, insufficientsecurity in operating systems, database managementsystems, networking, and other components sustainingthe use of RFID technology are greatly in need ofadvancement. Steady, correct, and up-to-date distributed databases are necessary for system accessibilityand survivability. Several research and directions might besupportive, although these are not limited to RFID technologiesin their implication. Particular requirementscomprisethe capability to build up trustworthy systems, with appropriatesecurity, accountability, auditing, bindingintegrity, privacy-preserving cryptography, and so on(Neumann & Weinstein, 2006).

3.3 Virus Vulnerabilities of RFID Tags

Some research conducted by agroup of European scientists (Stuart & Liu, 2006)warned thatRFID tags have the potential to be infected with viruses that could corrupt the back-end databases and cause major disorder at airports and supermarkets. The researchers have demonstratednumerous types of exploits that can beexecuted by RFID tags through exploiting RFID middleware (Alder, 1998). These exploits include buffer overflows, malicious code insertion, and SQL injection.The researchers also verified that thecreation of a self-replicating RFID virus requiring only an infected RFID tag as an attack vector and discussed the likelihoodof attacking the back-end database of an RFID application scenario, then infecting the clean new tags.

3.4 Low Level Attacks

There are several classes of low level attack against RFID system:

a.Sniffing: RFID tags are intended to be readable by any compliant reader. However this permits unauthorized readers to scan tagged items from great distances. RFID data can also becollected

by snooping on the wireless RFID channel. Unrestricted access totag data can have severe implications; collected tag data might disclose informationlike medical predispositions or strange personal inclination, which could lead denial of insurance coverage or employment for an individual.

b.Tracking: RFID technology assists the concealed monitoring of individuals' positionand actions. RFID readers positioned in locations (like doorways)can record RFID tags' unique responses, which can then be connectedwith a person's identity. RFID tags lacking unique identifiers can also ease on tracking by forming constellations which are frequent groups of tags that arelinked with an individual. RFID technology also enables the monitoring of entiregroups of people. The UK-based workers' union General Municipal Boilermakers (GMB) recently called on the European Commission to ban the RFID tagging of employees in the workplace.GMB accused employers of dehumanizing warehouse staff by forcing them towear computers that track how long it takes to complete tasks with RFID tagged objects. Civil liberties groups also warn that governments could monitorindividuals' movements, threatening to eliminate anonymity in public places(Rieback, 2006).

c.Spoofing: Attackers can generate authentic RFID tags, by writing correctly formatteddata on blank RFID tags. For example, thieves could retag items in a supermarket categorizing them as similar, but cheaper, products. Tag cloning is a different kind of spoofing attack, which constructs unauthorized copies of legitimate RFID tags.

d. Replay Attacks: Replaydevices are capable of intercepting and retransmitting RFID queries, which couldbe used to exploit a variety of RFID applications. England's new RFID-enabled license plates (e-Plates) are one instance of a modern RFID system that is vulnerableto attack by a replay device(Rieback, 2006). The active e-Plate tags enclose an encrypted IDcode which is stored in the UK Ministry of Transport's vehicle database. An attacker can easily trace the encrypted identifier when another car's license plate is scanned, and then replay it back later.

e. Denial of Service:RFID systems only execute when RFID tags and back-end databases are accessible. The attacker can execute Denial of Service to steal RFID-tagged items, by removing

tags from the items entirely, or by temporarily deactivating them by putting them in a foil-lined booster bag that blocks RFID readers' query signals. Some attackers can flood RFID systems with more data than the system can handle.

3.5Counter Measures

There are several counter measures for privacy protection-related RFID tags.

a. Third-party authentication:Veri-RFID is a model for a third-party verification process by which RFID tag verification occurs using an infrastructure such as the SSL certificate or credit rating verification. These are currently being implemented for e-commerce by an issuing party as a Certificate Authority (CA) such as VeriSign or GeoTrust, or third parties for credit ratings such as Equifax and TransUnion. The credit rating model has already set the model for distribution and circulating consumer private information with other interestedthird parties who wish to provide additional services to the consumers without compromising privacy of the consumers, similar to what is required to manage the tag information in the RFID-enabled world. The Veri-RFID scheme will provide the consumerwith an option to purchase (at an appropriatecost) a Verification Contract that gives the consumer the power of authentication and the control of the private information about the tag and the contract provides the consumer with the authority to verify, with the third party, whether the RFID tag has been disabled and what information has been distributed with retailers and other interested parties(Shostack, 2004). Next, issues as cost and management must be addressed.

The Veri-RFID Verification Contract will permit consumersto purchase a plan appropriate for their needs.A paid Verification Contract provides consumers withrights to making other decisions about the information.Consumer may decide to control access to thetag information for preserving privacy. One option to managethe Veri-RFID scheme is that the third party offers thefollowing simple plans: free plan and paid plan. Free plan is similar to credit rating companies that are required to provide free credit reports in case a service was denied to the customer based on poor credit rating. In RFID authentication, third parties providing verification services should provide a free annual report of the access activities by other interested parties. Consumers are able to block access to the information by certain parties if it is believed to be misused or poses any threat to the consumer, as identity theft in case of credit

ratings. In the paid plan, a third party will provide a fixed costor pay-per-use plan to the consumer (Murray, 2004). Under thisplan, consumers should have rights to controlaccess to the information.

The real cost to the retailer and manufacturer is minimal as compared to thebenefit of providing third-party verification of the data. The model is flexible and allows the tradeoff between the cost and the privacy and lets consumer choose the appropriate model.

b. Kill tag approach: An RFID tag is permanentlydisabled by a 32-bit killpassword stored in reserved memory sothat it becomes inoperative before it isplaced in the hands of consumers

The "kill tag" approach is typically usedin Point of Sale (POS) applications, where the tags ofpurchased goods are killed after checkingout.

c. Password approach: The RFID tag data is accessed or locked by an optional 32-bit access password stored in reserved memory(Stuart & Liu, 2006). This approach can be applied for controlling unauthorized access to confidential data stored in the tag memory.

d.Active-jamming approach: An electronic device actively broadcasts radio signals to disrupt the operation of any nearby RFID readers (Murray, 2004). A drawback for this application isthat it could cause disruption to normal operations of nearby RFID systems, which may be illegal.

f. Cryptographic approach: Part of the data area on the RFID tag is used to store a cryptographic signature, such as SHA-1 hash, which verifies that the rest of the data reported has not been tampered with and the reported data was encrypted. This approach not onlypreserves data confidentiality but alsoauthenticates user identity. However, the operation flow should be carefully designed in order not to jeopardize the convenience of use, especially in retail and POS applications.

Researchers have developed versions of symmetric key and public key cryptography. RFID-specific authentication schemes have also sprout up, some of which are lightweight, using techniques like minimalistcryptography and human-computer authentication. Other schemesoffload complexity to a back-end database, like hash locksand EPCglobal'sprojected

authentication servers. One of the first RFID-specific authenticationplots to be widely arrangedis the symmetric-key based Basic AccessControl for digital passport(Rieback, 2006).

3.6 RFID Guardian: Platform overview

There is no unified framework; noefficient means to leverage individual RFID countermeasuresto accomplish the most significant goal of all – theprotection of real people.

The RFID Guardian is a portable battery-powered device that intervene communicationsbetween RFID readers and RFID tags. The RFID Guardian influences anon-board RFID reader combined with novel tag emulation capabilities to audit andcontrol RFID activity, thus enforcing conformance to a specified security policy.

a.RFID Guardian Design Goals

The design of the RFID Guardian was motivated by the following goals,which follow from the nature of RFID applications and deployment considerations by Rieback, 2006:

- Centralized use and management: Most existing RFID countermeasures allocatetheir security policies across RFID tags, which make them very difficult to configure, manage, anduse. To address this concern, Rieback and et al. designed a singleplatform to leverage RFID countermeasures ina coordinated fashion. Personalized security policies are centrally enforced by employing novel RFID security features (auditing, automatic key management, tag-reader mediation, off-tag authentication) together with existing ones (kill commands, sleep/wake modes, on-tag cryptography).
- Context-awareness: Different countermeasures have strengths and weaknesses in different application situation. Low cost Electronic Product Code (EPC) tags require special access control mechanisms than expensive crypto-enabled contactless smart cards. This system sustains both RFID-related context (i.e. RFID tags present, properties and security features, and their ownership status), as well as personal context (i.e. the user is in a non-hostile environment). Context is then used in conjunction with an Access Control List (ACL) to decide how to best protect the RFID tags in question.
- Ease-of-use: This systemis both physically and operationally unobtrusive. The system will be eventually integrated into a PDA or mobilephone, so users will not be burdened with carrying an extra physical device. Accordingly, the RFID Guardian uses an XScale processor and simple RFID HW (barely more complex than RFID HW already found in Nokia mobile phones). Also,

system operation was designed to be non-interactive for default situations, and presents a user interface for the special cases that require on-site configuration.

- Real-world usability: It is essential that the RFID Guardian work with actual deployed RFID systems. They chose a single standard as a proof-of-concept, to prove the technical feasibilityof their ideas. The RFID Guardian implementation supports 13.56 MHz (HF) RFID, and is compatible with the ISO-15693 standard

b. System Functionality

The design of the RFID guardian focuses on four fundamental issues such as auditing, key management, access control, and authentication which are illustrated below Rieback, 2006:

- Auditing: The RFID Guardian examines RFID scans and tags in its vicinity, functioning as a barometer of (unauthorized) RFID activity. RFID auditing is a prerequisite for the enforcement of RFID security policies. Scan logging audits RFID scans in the vicinity, which are either displayed (using an LCD or screen) or are logged for later retrieval.Audited RFID scans should be filtered to avoid confusing the user with boring information. The RFID Guardian monitors RFID tag ownership and alerts individuals of newly appearing (possibly clandestine) tags. Ownership of RFID tags can be transmitted explicitly by the user interface or an authenticated RFID channel
- Key management: Modern RFID tags have a variety of security features varying from tag deactivation commands, to password-protected memory, to industrial-grade cryptography. These security features often need the use of associated key values and the keys must be acquired, stored, and available for use at the suitable times. The RFID Guardian is well suited to handle RFID tag keys due to its 2-way RFID communications abilities. Tag key transfer could take place by eavesdropping on the RFID channel when a reader issues a query containing the desired key information.
- Access control:The RFID Guardian sustains a centralized security policy that determines which RFID readers have access to which RFID tags in which situations. This security policy is executed as an Access Control List (ACL). The ACL resembles one used by a standard packet filter, that allows or denies RFID traffic based upon the querying reader (if known), the targeted tag(s), the attempted command, and the context (if any). Different situations call for different countermeasures. For example, RFID tagged credit cards require less rigorous security at home

than at the shopping mall. The RFID Guardian therefore offers context awareness facilities that perceive an individual's situation and then adjust tag access accordingly.

The RFID Guardian acts as a mediator between RFID readers and RFID tags. TheGuardian uses Selective RFID Jamming to enforce access control by controlling the communications mediation.The RFID Guardian's selective jamming scheme is currently optimized for ISO-15693 tags, which use the Slotted Aloha anti-collision scheme. Selective RFID Jamming utilizes tag emulation to decode the incoming RFID reader query, concludes if the query is acceptable (according to the ACL), and then sends a short jamming signal that specifically locks the timeslot in which the "protected" RFID tag will give its response (Rieback, 2006).

- Authentication: the majority of RFID tags cannot authenticate directly due to application constraints such as cost or power. The RFID Guardian thus authenticates "Guardian aware" RFID readers on behalf of low-cost RFID tags, adapting the subsequent access control decisions to reflect the permissions of the newly-identified reader. The RFID Guardian must also exchange authentication keys with RFID Readers, either ahead of time or using on-the-fly means (ex. user interface, PKI).

c. Implementation

Rieback et al. have tested their system against commonly used RFID equipment – the Philips MIFARE/I. Code Pagoda RFID Reader, with Philips I. Code SLI (ISO-15693) RFID tags. The hardware and software architecturethat their prototype uses to monitor and protect theRFID infrastructure is illustrated belowRieback, 2006:

- Hardware: The RFID Guardian is like a full-fledged portable computer. It contains microcontroller such as the Intel XScale PXA270 processor, with 64 megabytes of SDRAM and 16 megabytes of Flash memory. XScale was used by the strict ISO-15693 timing constraints combined with the computational load of authenticating RFID readers. The prototype has a minimalist User Interface (UI) – a serial RS-232 interface to the PC host, which contains an attached keyboard and screen.
- Software: The Guardian's 12694 lines of code provide device drivers (RFID HW), a protocol stack (ISO-15693), data storage libraries, high-level system tasks, and application libraries. The result is 254728 bytes of cross-compiled functionality dedicated to RFID security and privacy protection. The e-Cos Real- Time Operating System (RTOS) is taskmaster; it ensures fast and

reliable execution, while simplifying developers' lives by handling threads, basic common interrupt handling. It is open-source, free of licensing costs, and has an active developer community. Device drivers are the main software for the RFID Guardian's HW. Driver pairs control the RFID tag device (tag transmitter/receiver), RFID reader device (reader transmitter/receiver), and the jamming signal (random noise generated by the tag transmitter).

d. User interface

Users can correspond with the RFID Guardian by several means: by serial line or socket, over the RFID channel, or using a TFT or Nokia cell phone (via Bluetooth).

Cellphone UI: Two cell phones were tested as platforms for the User Interfacefor the RFID Guardian: the Nokia E60 (shown in Figure 6, Panel 1) is a standard phone with a numerical keypad, five-way navigation key, and two soft keys. Also, the Nokia E61 is a Smartphone with a numerical keypad and QWERTY keyboard.Both of these phones run the Symbian OS along with Nokia's S60 platform,for which an emulator is available(Guardian, 2010).

The Cellphone User Interface can initiate the following high-level functions on the RFID Guardian (shown in Figure 6, Panels 2 and 3) by Guardian, 2010:

- Tag functions: Conduct an RFID scan, transfer tag ownership, manage tagsets, manage tag keys, and manage tag spoofing.
- Reader functions: Manage RFID reader/role lists, manage Guardian-Reader keys/certificates, add and remove readers/roles.
- Access control functions: Select the ACL directory, check the ACL status, load/save/clear the ACL, and set the ACL context.
- Auditing functions: Set real-time alerts, view or configure scan/tag logging, and view/configure general-purpose logs.
- Advanced functions: Security (relay/replay) and Administration (load new programs, reflash EEPROM, backup/synchronize via a reader+PC, cell phone filesystem browser, Guardian filesystem browser,change system time.)

This battery-powered device, which could easily be integrated into a cell phone, can monitor scans and tags in its vicinity, warning the owner of active and passive snooping. It can also perform key management, handle access control, and authenticate nearby RFID readers

automatically, taking its context and location into account. There is no other device in existence or proposed with all of these promising features. The RFID Guardian thus symbolizes a major step that will allow people to recapture some of their privacy that RFID technology is threatening to take away. However there is a need for future research to focus on to improve the RFID Guardian by giving the prototype more capabilities. These capabilities comprise support for more frequencies and standards, improving the communication range, and simplifying the hardware design.

4. LESSONS LEARNED

Information privacy has been recognized as significant for both the functioning of persons, individuals, and societies, and also for freedom of personhood. Bearing this in mind, there are certain guidelines, which are very nearly always proposed when the issue of information privacy, use, storage, and proper dispersion becomes a priority. The primary issues are those of notice, consent, and accountability, which involve that the one about whom information is being collected must know when and what type of information is being collected and permit this to occur voluntarily, and where the one collecting the information is responsible for its accuracy and security.

Some features of the needed regulation can be set forth instantaneously by Anderson and Labay, 2006. First, the collector of information should be accountable for the integrity of the data collected, since incorrect data can direct to unfair invasion of privacy and even to situations as drastic as false investigation or arrest. Second, the collector should be in charge for preserving the security of sensitive data such as medical information, financial information, information that is personally identifying, etc. and making sure that the data are accessible only for the intention for which they were intended and only to those who have a legitimate interest in acquiring access to them. Third, the government should not be allowed to use the data for discriminatory purposes, such as unfair profiling. Fourth, the government should present for notice, consent, and access by individuals to datathat personally concern them whenever there is no outweighing competing interest

5. CONCLUSION

RFID has received a lot of attention in computing environment.RFID-related technologies can have some attractivebenefits in certain carefully delineated situations. However, although it presents vast potential benefits in terms of convenience and security; RFID in all applications, possible security and privacy risksmust be measured objectively.Since privacy is very significant for the functioning of individuals and society at large, it should be appreciated and preserved whenever possible.More importantly, it is critical that weengage now in a far-reaching, society-wide dialogueregarding the conditions and environments within whichRFID systems should or should not be used, and therights of individuals and organizations to controlwhether or not they will be subject to various uses ofthese systems.

6. REFERENCES

Alder, G. (1998). Ethical Issues in Electronic Performance Monitoring: A Consideration of Deontological and Teleological Perspectives, *Journal of Business Ethics*, 17, 729-743.

Anderson, A., & Labay, V. (2006). Ethical Considerations and Proposed Guidelines for the Use of Radio Frequency Identification:. *Science and Engineering Ethics, 12 (2)*, 265-272.

Foster, K., & Jarger, J. (2008). Ethical Implications of Implantable Radiofrequency Identification (RFID) Tags in Humans. *The American Journal of Bioethics, 8(8)*, 44-48.

Glasser, D. J., Goodman, K. W., & Einspruch, N. G. (2006). Chips, Tags, and Scanners: Ethical Challenges for Radio Frequency Identification. *Journal of Ethics and Information Technology*. 9, 101-109.

Guardian, R. (2010, May 21). *User Interface*. Retrieved February 18, 2012, from RFID guardian: http://www.rfidguardian.org/index.php/Documentation#UI_Docs

Krishna, P., & Husak, D. (2007). *RFID Infrastructure- A technical . Vol. 1, No. 2.* Retrieved January 27, 2012, from REVA systems: http://www.milestechinc.com/pdf/RFID-Infrastructure.pdf

Lockton, V., & Rosenburg, R. S. (2006). RFID: The Next Serious Threat to Privacy. *Journal of Ethics and Information Technology*. 7, 221-231.

Neumann, P., & Weinstein, L. (2006, May). Risks of RFID. *Communications of the ACM. 49(5)*, 136-143.

Reaz, M., Hussain, J., & Yasain, F. (2009). RFID Reader Architecture & Applications. *Microwave Journal* , 3, 24-34.

Rieback, e. a. (2006). A Platform for RFID Security and Privacy Administration. *20th Large Installation System Administration Conference (LISA '06)*, 89-102.

Shostack, A. S. (2004). What Price Privacy? (and why identity theft is about neither identity nor theft). In A. S. Shostack, *Economics of Information Security* (pp. 129–142). Dordrecht, The Netherlands: Kluwer Academic Publishers.

Stuart, C., &Liu, J. (2006). Securing RFID Applications: Issues, Methods, and Controls. *Telecommunication & Network Security* , 2, 43-50.