PRIVACY AND SECURITY ISSUES IN RFID TECHNOLOGY

J. V. Gorabal
Assoc Prof, CSE, SCEM, Mangalore

Manjaiah D. H
Prof Computer Science Department, Mangalore University, Mangalore.

Abstract—Radio Frequency Identification (RFID) systems are a common and useful in supply chain management, asset tracking, animal tracking and retail inventory control. Due to hectic research and developments, in the near future, low-cost RFID tags may be a practical replacement candidate for optical barcodes on consumer items. Shockingly, the widespread arrangement of RFID gadgets in purchaser things may uncover new security and protection issues. In this paper we discuss various research issues in the area of privacy and security and possible remedies in the present situation.

Keywords—RFID Tag, Privacy, Security.

I. INTRODUCTION (HEADING I)

Radio Frequency Identification (RFID) innovation is picking up an a dependable balance as a progressed standardized identification substitution, a remote smartcard and a bland framework for joining naturally coherent information to protests. Right now RFID is constantly utilized for following products as a part of supply chains, distinguishing vehicles in toll accumulation, following creatures and putting away biometric information in electronic travel papers – simply to name a couple of samples. In any case, while initially RFID may appear as a straightforward specialized issue, it realizes shockingly unpredictable issues at more critical look. These issues incorporate security and protection attentiveness toward companies, purchasers or different clients of this innovation. This paper addresses on some specialized results proposed for handling these issues, and assesses their adequacy as protection security strategies contrasted with their effect on the helpfulness of RFID.

II. A NOTE ON PRIVACY AND SECURITY

Privacy: Right to keep things to yourself. The ability of the RFID system to keep the meaning of the information transmitted between the tag and the reader secure from unauthorized recipients. Everyone in this world they want to live their life with lot of privacy, nobody wants to publicize their personal things. Any computer software application developed in the present world it has to incorporate the principles of privacy. Individuals sometimes choose to remain anonymous to safeguard their privacy, for example, when browsing in a department store or purchasing an "adult" magazine. Browsing the Web has also, to date, usually been an anonymous activity. Moving beyond the Web to the Internet in general, one can send anonymous messages using an anonymous remailer program. It is fairly easy today for a technically sophisticated person to remain anonymous and avoid accountability on the Internet for actions which are questionable or illegal, e.g., sending advertising mail to numerous newsgroups (spamming), running a pornography server, or hacking the Web page of another person.

III. A. Selecting Privacy Threats from today’s computer system

First, The Privacy Act of 1974 [privacy 1974] and information security enactment in different nations has to some degree defused feedback and worry about potential government attack of protection. For sure, restorative, credit, and advertising databases give off an impression of being as troublesome as legislative databases. Some private tries have officially brought noteworthy security concerns up in the Internet group. All the more as of late, in 1996, Lexis-Nexis offered an administration which furnished its 740,000 supporters with 300 million names, past and current addresses, lady and expected names, conception date, and phone number. The wide accessibility of such data raised legitimate and different concerns and has set off an examination by the Federal Trade Commission, reacting to congressional request. Lexis-Nexis at first offered standardized savings numbers also, however changed the framework after various objections from Netizens.

With a specific end goal to actualize "security" in a computer system, we require a more exact definition. We need to choose when and under what conditions to give out particular data. Particularly, we must choose when to permit unknown transactions and when to oblige responsibility. There does not so much must be one and only security administration. Less law and more client decision is conceivable now; innovation can give each client controls adjusted for the offset of security and accessibility that they lean toward [1].
B. Security
It comprises of the procurements and arrangements received by a system overseer to anticipate and screen unapproved access, abuse, adjustment, or refusal of a workstation system and system open assets. System security includes the approval of access to information in a system, which is controlled by the system manager. System security is included in associations, undertakings, and different sorts of foundations. It does as its title clarifies: It secures the system, and in addition securing and regulating operations being carried out. The most widely recognized and straightforward method for securing a system asset is by relegating it a remarkable name and a relating secret key.[2]

Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

C. Big Three of Security (BTS)
As any other mission-critical system, it is important to minimize the threats to the confidentiality, integrity, and availability (CIA) of data and computing resources. These three factors are often referred to as “The Big Three.” The below mentioned figure presents the balance between these three prime candidates. In the present scenario all the systems may or may not need same security requirement, hence it is important to analyze and evaluate each system (sensitivity of the data, potential loss from incidents, criticality of the mission, etc.) to determine the CIA requirements. For example, the security requirements of tags used in e-passports should not equal those in the supply chain [11].

Confidentiality
Integrity
Availability

Confidentiality: As shown in the figure 1 the tag information must be accessible only to the authorized user. RFID technology allows the tracking of items. From a user perspective, tracking should be avoided. However, companies may control the movements of materials in the supply chains, helps them in increasing the productivity of their processes.

Integrity: The assurance that the messages transmitted between two parties are not modified in transit. Additionally, some systems provide the authenticity of messages. The receipt is able to prove that a message was originated by the purported sender and is not a forgery (non repudiation). An example of this kind of attack is the spoofing attack.

Availability: Another dimension of dependability is systems. System availability for its intended purpose to maintain the good will of the customer or the end user, it is very essential attributes of the computing systems. This predominant factor will determine the overall performance and the scalability level of the system. Denial-of-service (DoS) attacks are usual threats for availability between the tag and the reader secure from unauthorized recipients.

IV. RFID CHALLENGES
In spite of its attractive and user friendly applications acceptance and trust of RFID is low. At the same time there are some vulnerable situations like privacy and security aspects have become bottleneck to growth of the RFID technology. It is not only to make the technology secure and reliable. The perception of security depends on the individual’s reaction to both the risks and the countermeasures adopted. End users will need to be properly educated to change their false perception which will enable the technology to available common man[7]

- Due to the complexity and crisis of RFID systems, a process or regulations needs to be composed and processed to address the problems prior to the deployment of RFID systems.
- Due to deployment of RFID systems there may be threat of loosing the jobs, since manpower in inventory may be reduced. Moreover, RFID will create new jobs, related to data processing and service-related jobs and the overall resulting economic growth may also contribute to the creation of additional workplaces.[3][8]
- Deployment costs will be expensive in RFID systems. The lack of well established standards may lead to mistrust the technology. The small organizations may not come forward due to cost barriers which may lead to deny the usage of new technology.
- Dependability of RFID information systems, especially in critical and real time application areas such as health care , the need to design appropriate procedures in case of system failures. This adds to the costs of deployment and represents yet another obstacle for the growth of the RFID technology
- The growth of the technology that all depends on the policies of the government and the vision of the leaders of the nation. Some people talk more do nothing some leaders make the technology so popular and available to the mass, which obviously increases the revenue for the country. In
this regards Europeans and Chinese are doing better and they are ahead of Indians.

V. SECURITY AND PRIVACY ISSUES IN RFID SYSTEMS

Privacy: the ability of the RFID system to keep the meaning of the information transmitted between the tag and the reader secure from unauthorized recipients.

Security: the ability of the RFID system to keep the information transmitted SECURITY NEEDS

We can list the issues as follows

Eavesdropping

Eavesdropping (White Paper, 2004) is defined as listening in on longer-range communication systems like UHF, which broadcast signals (albeit very weak) up to 100 meters. Tag readers are assumed to have a secure connection to a back-end database. Although readers may only read tags from within the short (e.g. 3 meter) tag operating range, the reader-to-tag, or Forward channel is assumed to be broadcasted with a signal strong enough to monitor from long-range, perhaps 100 meters. The tag-to-reader or backward channel is relatively much weaker, and may only be monitored by eavesdroppers within the tag’s shorter operating range. Generally, it will be assumed that eavesdroppers may only monitor the forward channel without detection (Weis, 2003) (White Paper, 2004). Eavesdropping may cause two kinds of security problems. The first is individual information leakage (Ohkubo et al., 2003) and the other is industrial espionage (Sarma et al., 2002). Shown in figure 2

RFID Skimming is a form of digital fraud or theft, it enables information from RFID based cards to be read and duplicated to an intruder. It can be used as a form of wireless identity theft. It works by reading of RFID chips at a distance using a RFID reader device, which reads the card information and stores, from there, it can be written to a new blank card, which then operates in the same manner as the original card. Since the content are identical on both cards, and the information is only copied, it makes no difference if the original data is encrypted or not.

Traceability

Another important privacy concern is the tracking of personal RFID tags without the knowledge of owner of the tag. A Spy with tag reader sitting at a fixed location can track RFID-labeled items like Inner wear or bikini by people passing by. Suppose a Professor carrying a scotch bottle(RFID tech embedded) in his bag may tracked by a mischievous college student by RFID scanner, the professor loses his privacy in public life. This may lead do damage the professors image in the institute.

Spoofing

In addition to threats of passive eavesdropping and tracking, an infrastructure dependent on RFID tags may be susceptible to tag spoofing (Weis et al., 2004) (Tan et al., 2003) (Anil et al., 2003). There are two kinds of security issues about spoofing. One is theft and the other is counterfeiting which are discussed as follows.

Cloning

When RFID spoofing is done coupled with replicating the original form factor of the tag to give an identical product, the RFID tag is said to have been cloned. RFID cloning is also referred to as a, relay attack.

Theft

By spoofing valid tags, a thief could fool automated checkout or security systems into thinking a product still on a shelf. Alternatively, a thief could rewrite or replace tags on expensive items with spoofed data from cheaper items. Saboteurs could disrupt supply chains by disabling or corrupting a large batch of tags.

Counterfeiting

It is defined as being able to read or intercept data written 336 into a tag, which uniquely identifies or certifies a product. Once the data is known, similar read/write tags could be purchased and updated with the authentic data. Thus it is possible that malicious attacker use counterfeiting products to spoof RFID security system

Denial of Service

The problems surrounding security and trust are greatly increased when large volumes of internal RFID data are shared among business partners. A denial of service attack on RFID infrastructure could happen if a large batch of tags has been corrupted. For example, an attacker can use the “kill” command, implemented in RFID tags, to make the tags permanently inoperative if they gain password access to the tags. In addition, an attacker could use an illegal high power

Industrial Espionage

For competitors. Aggregate logistics and inventory information carries significant financial value for commercial organizations. A store’s labeled inventory may be monitored by competitors conducting surreptitious scans. Sales data may be gleaned by correlating changes over time. Individuals carrying items with unsecured tags are vulnerable to privacy violations. In retail environment, where a competitor capable of reading tags in shops or warehouses may gather business intelligence regarding the turnover rate of stocks, the shopping patterns of customers, and so forth. Somebody could derive sales, inventory data and offer his services to business adversary as a corporate spy (Weis et al., 2004) (Juels, 2004).[4][10]
radio frequency (RF) transmitter in an attempt to jam frequencies used by the RFID system, bringing the whole system to halt.

**RFID Viruses and Worms**

Since RFID systems rely on middleware to communicate with business applications and backend databases, they are susceptible to malware attacks by hackers just as any other software based solution. It has been demonstrated that by merely scanning an infected RFID tag, it is possible to compromise the system’s security and cause malicious pre-programmed damage to the backend database of an RFID implementation. Once the system has been compromised, the malware’s payload can be designed to spread the damage by infecting other tags. Based on the propagation vector that is used, RFID malware can be classified as an RFID worm or RFID virus [5].

The issues relating to security are often those that involve fake or illegitimate tags, rather than readers. The main security problem is that tags can very easily be counterfeited or copied. This allows impersonation of tags and gives rise to a host of problems. Imagine we are in an age that people are implanted with tags, and these tags are used for everything from access control to ATMs to credit card payments. If an adversary copies the tag of another person, then it would be easy for him to access the victim’s bank accounts and withdraw money. Consider another example, of a dishonest company called Company Z. Suppose it handles shipment of goods from point A to point B, and each crate of goods is implanted with an RFID tag. Company Z would find it easy to make a copy of a tag on a crate, and replace that crate with an empty one implanted with the counterfeit tag. They could then steal the original crate with the goods in it, and the fact that the crate arrived empty will be blamed on the suppliers!

**VI. APPROACHES TO HANDLE PRIVACY AND SECURITY ISSUES IN RFID**

**Tag Deactivation**

In this approach Permanent or temporary deactivation of RFID tags can be used as a Brute Force approach to tackle privacy issue. The basic concept behind this strategy is, that when a tag is deactivated, it does not respond to any reader interrogations, thus not revealing any information of the tag even its existence.

We have Two Strategies in this

**Killing**

**Sleeping**

**Killing**

(Damith C. Ranasinghe, Daniel W. Engels2004) Killing is a solution to tackle privacy issues which is employed in current Electronic Product Code (EPC) tags. These low price EPC tags are basically used in supply chain management, but they also appear in consumer products. Killing of tags is to occur at purchase time in order to protect consumer privacy. Once the product is purchased immediately the killing process is done to deactivate the tag. The kill command is used to disable the tag for further use. This kind of disabling of tag is permanent. Once the tag is disabled it cannot be activated. This kind of strategy is applicable for low priced items.

**Analysis of the approach**

(David Molnar and David Wagner. P 210-219) With the help of this approach we can address two major issues one is tracking and other is inventory threats as mentioned in the (2.2.6). Due to ease of operation and simplicity it is very economic method to resolve the issue. But the limitation here is sold items cannot be taken back to shop. This approach cannot be deployed in the application like Library management, since tag reading will be done in borrowing and as well as in returning books. (Ari Juels, David Molnar and David Wagner. Security and Privacy Issues in E-passports P 74-88 IEEE) Another example is E-Passports, where the reading of biometric information stored on a passport is not possible unless the RFID tag is operational at all the time. (My research issue) [6].

**Sleeping**

(Ari Juels, RFID Security and Privacy RSA Labs ) Sleep and wake functionalities is another approach in place of kill option. In this approach the tag will be disabled for interrogation only temporary. Based on the application we can choose the, whenever interrogation is required it will be awake state else it will be in sleep state. Thus stakeholder’s privacy would be ensured during the transport of the products. The wakeup activity will be done by only after authentication procedure like passwords etc.

**Analysis**

(Simson Garfinkel, Ari Juels and Ravi Pappu. RFID Privacy:) This option provides an effective privacy protection than the killing approach. (Ari Juels. RFID Security and Privacy:) The problem with this solution is, all the time it requires the owner of an item or the activate the tags by using passwords for RFID devices. One user may have many items and many tags and many passwords, this becomes most tedious job to remember passwords for an end user, this poses the usability problem. Since a password transmitted from a reader to a tag might be caught by an eavesdropper, or even guessed by an intruder.

**Blocking**

(Ari Juels, Ronald L. Rivest and Michael Szydlo. The Blocker Tag) Blocking is a way of preventing an unauthorized reader trying to interrogate RFID tags. Blocking is done by some special tags called as blocker tag that blocks a reader from detecting any other nearby tags that need privacy protection. Here we discuss two types of blocking, namely “real” blocker tags and soft blocking.

**Approaches in Blocking Blocker Tags**

(Ari Juels, Ronald L. Rivest and Michael Szydlo. The Blocker
Tag) One tag will be designated as A blocker tag may be called as BT it acts like body guard for the set of tags belonging a defined serial number spectrum. Thus by blocking the intruder tag reader in a specific area and range, tags will be in a safe state. Thus a privacy zone will be created by this blocker tag, to disrupt the intruder Here we have to consider two things one is soft blocking obviously offers no real protection against any threats if the attacker is “breaking the rules” – as attackers very often do. On the other hand, if readers truly follow the given policies neatly, this approach is indeed quite effective, flexible and undoubtedly economic and easy to deploy. Present blocker tag deployments depends on exploiting anti-collision protocols, also called singulation protocols. According to this These protocols allows to read one tag at time to transmit its information to a reader. A blocker tag, on the other hand, does not follow this protocol as shown in the figure 3 [9]

VII. CONCLUSION

Certainly RFID technology is more advantageous compared to barcode identification system. RFID is a most promising technology in various applications. Citizens while interacting in an increasingly digital(RFID) world are more and more leaving their digital traces mostly in an unknowingly to third parties (other persons, commercial companies). With these circumstances there is a tendency to (commercially) exploit citizens’ data; on the other hand, citizens may become vulnerable as their privacy or integrity may be hampered. Present RFID systems are more vulnerable to attackers; this may end-up in loosing goodwill of the stakeholders. In this paper we discussed some existing approaches proposed by researchers to handle privacy and security issues.

References

[4] Chin-Yi Lin Department of Information Management, National Yunlin University of Science and Technology, 123, Section 3, University Road, Douliu, Yunlin, Taiwan p 335-336.
[6] Jimmy Kjällman Helsinki University of Technology” An Overview of Approaches to Privacy Protection in RFID
[7] RFID Privacy and Technical Challenges By Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita© 2005 ACM 0001-0782/05/0900 $5.00
[9] Soft Blocking:Flexible Blocker Tags on the Cheap Ari Juels John Brainard RSA Laboratories Bedford, MA, USA ajuels@rsasecurity.com
[10] Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens Gerhard P. Hancke Smart Card Centre, Information Security Group Royal Holloway, University of London Egham TW20 0EX, UK ghancke@ieee.org