A Survey Paper on Radio Frequency IDentification (RFID) Trends

Christoph Jechlitschek, christoph.jechlitschek@gmx.de

Abstract

This paper provides a survey on radio frequency identification (RFID) technology. Initially RFID tags were developed to eventually replace barcodes in supply chains. Their advantages are that they can be read wirelessly and without line of sight, contain more information than barcodes, and are more robust. The paper describes the current technology, including the frequency ranges used and standards. With the increasing ubiquity of RFID tags, however, privacy became a concern. The paper outlines possible attacks that can violate one's privacy and it also describes counter measures. The RFID technology did not stop at item-level tagging. The paper also presents current research that focuses on locating and tracking labeled object that move. Since the uses for RFID tags are so widespread, there is a large interest in lowering the costs for producing them. It turns out that printing tags might become a viable alternative to traditional production. The paper reviews the current progress.

Keywords: Radio Frequency IDentification, RFID, RFID tags, Electronic Product Codes, EPC, Supply Chain Management, Security, organic printing, Location and Tracking

See also: Other Reports on Recent Advances in Networking
Back to Raj Jain's Home Page

Table of Contents

1. Introduction

RFID tags, or simply "tags", are small transponders that respond to queries from a reader by wirelessly transmitting a serial number or similar identifier. They are heavily used to track items in production environments and to label items in supermarkets. They are usually thought of as an advanced barcode. However, their possible area of use is much larger. This paper presents a few new applications that are possible using RFID technology such as locating lost items, tracking moving objects, and others. RFID tags are expected to proliferate into the billions over the next few years and yet, they are simply treated the same way as barcodes without considering the impact that this advanced technology has on privacy. This paper presents possible exploits of RFID systems and some proposed solutions as well.

Back to Table of Contents

2. Historic Development of RFID

The first RFID application was the "Identification Friend or Foe" system (IFF) [Wiki-RFID] [Wizard Wars] and it was used by the British in the Second World War. Transponders were placed into fighter planes and tanks, and reading units could query them to decide whether to attack. Successors of this technology are still used in armies around the world.

The first commercial RFID application was the "Electronic Article Surveillance" (EAS). It was developed in the seventies as a theft prevention system. It was based on tags that can store a single bit. That bit was read when the customer left the store and the system would sound alarm when the bit was not unset. In the end-seventies RFID tags made its way into the agriculture for example for animal tagging.

In the eighties RFID technology got a boost when Norway and several US states decided to uses RFID for toll collection on roads [EZ-Pass]. In addition to toll collection the following decade brought a vast number of new applications, such as ski passes, gasoline cards [Speed Pass], money cards, etc.

In 1999 the Auto-ID Center at MIT was founded. Its task was to develop a global standard for item-level tagging. The Auto-ID was closed in 2003 after completing the work on the Electronic Product Code (EPC). At the same time the newly founded EPCglobal Inc. continues the work.

The probably first paper related to RFID technology was the landmark paper by Harry Stockman, "Communication by Means of Reflected Power" in October 1948. The first patent on RFID was issued in 1973 for a passive radio transponder with memory [US. Patent 3,713,148].

Back to Table of Contents

3. Current RFID Technology

This section describes out of which parts RFID tags consist of, how they work in principle, and what types of tags do exist. It focuses on how tags are powered and what frequency ranges are used. The section concludes by covering a few important standards.

RFID transponders (tags) consist in general of:

- Micro chip

- Antenna
- Case
- Battery (for active tags only)

The size of the chip depends mostly on the Antenna. Its size and form is dependent on the frequency the tag is using. The size of a tag also depends on its area of use. It can range from less than a millimeter for implants to the size of a book in container logistic. In addition to the micro chip, some tags also have rewritable memory attached where the tag can store updates between reading cycles or new data like serial numbers.

A RFID tag is shown in figure 1. The antenna is clearly visible. As said before the antenna has the largest impact of the size of the tag. The microchip is visible in the center of the tag, and since this is a passive tag it does not have an internal power source.

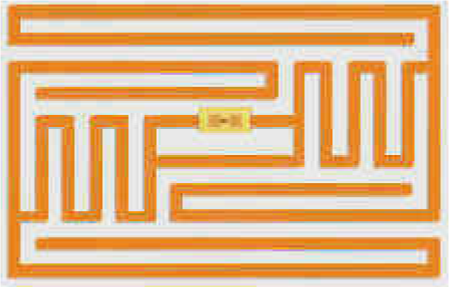

Figure 1: A passive RFID tag
(from [Wiki-RFID], used under the
GNU Free Documentation License)

In principle an RFID tag works as follows: the reading unit generates an electro-magnetic field which induces a current into the tag's antenna. The current is used to power the chip. In passive tags the current also charges a condenser which assures uninterrupted power for the chip. In active tags a battery replaces the condenser. The difference between active and passive tags is explained shortly. Once activated the tag receives commands from the reading unit and replies by sending its serial number or the requested information. In general the tag does not have enough energy to create its own electro-magnetic field, instead it uses back scattering to modulate (reflect/absorb) the field sent by the reading unit. Because most fluids absorb electro-magnetic fields and most metal reflect those fields the reading of tags in presence of those materials is complicated.

During a reading cycle, the reader has to continuously power the tag. The created field is called continuous wave, and because the strength of the field decreases with the square of the distance the readers have to use a rather large power. That field overpowers any response a tag could give, so therefore tags reply on side-channels which are located directly below and above the frequency of the continuous wave.

3.1 Energy Sources

We distinguish 3 types of RFID tags in relation to power or energy:

- Passive
- Semi-passive
- Active

Passive tags do not have an internal power source, and they therefore rely on the power induced by the reader. This means that the reader has to keep up its field until the transaction is completed. Because of the lack of a battery, these tags are the smallest and cheapest tags available; however it also restricts its reading range to a range between 2mm and a few meters. As an added benefit those tags are also suitable to be produced by printing. Furthermore their lifespan is unlimited since they do not depend on an internal power source.

The second type of tags is semi-passive tags. Those tags have an internal power source that keeps the micro chip powered at all times. There are many advantages: Because the chip is always powered it can respond faster to requests, therefore increasing the number of tags that can be queried per second which is important to some applications. Furthermore, since the antenna is not required for collecting power it can be optimized for back scattering and therefore increasing the reading range. And last but not least, since the tag does not use any energy from the field the back scattered signal is stronger, increasing the range even further. Because of the last two reasons, a semi-active tag has usually a range larger than a passive tag.

The third type of tags is active tags. Like semi-active tags they contain an internal power source but they use the energy supplied for both, to power the micro chip and to generate a signal on the antenna. Active tags that send signals without being queried are called beacons. An active tag's range can be tens of meters, making it ideal for locating objects or serving as landmark points. The lifetime is up to 5 years.

3.2 Frequency Bands

RFID tags fall into three regions in respect to frequency:

- Low frequency (LF, 30 - 500kHz)
- High frequency (HF, 10 - 15MHz)
- Ultra high frequency (UHF, 850 - 950MHz, 2.4 - 2.5GHz, 5.8GHz)

Low frequency tags are cheaper than any of the higher frequency tags. They are fast enough for most applications, however for larger amounts of data the time a tag has to stay in a readers range will increase. Another advantage is that low frequency tags are least affected by the presence of fluids or metal. The disadvantage of such tags is their short reading range. The most common frequencies used for low frequency tags are 125 - 134.2 kHz and 140 - 148.5 kHz.

High frequency tags have higher transmission rates and ranges but also cost more than LF tags. Smart tags are the most common member of this group and they work at 13.56MHz.

UHF tags have the highest range of all tags. It ranges from 3-6 meters for passive tags and 30+ meters for active tags. In addition the transmission rate is also very high, which allows to read a single tag in a very short time. This feature is important where tagged entities are moving with a high speed and remain only for a short time in a readers range. UHF tags are also more expensive than any other tag and are severely affected by fluids and metal. Those properties make UHF mostly useful in automated toll collection systems. Typical frequencies are 868MHz (Europe), 915MHz (USA), 950MHz (Japan), and 2.45GHz.

Frequencies for LF and HF tags are license exempt and can be used worldwide; however frequencies for UHF tags differ from country to country and require a permit.

3.3 Standards

The wide range of possible applications requires many different types of tags, often with conflicting goals (e.g. low cost vs. security). That is reflected in the number of standards. A short list of RFID standards follows: ISO 11784, ISO 11785, ISO 14223, ISO 10536, ISO 14443, ISO 15693, ISO 18000. Note that this list is not exhaustive. Since the RFID technology is not directly Internet related it is not surprising that there are no RFCs available. The recent hype around RFID technology has resulted in an explosion in patents. Currently there are over 1800 RFID related patents issued (from 1976 to 2001) and over 5700 patents describing RFID systems or applications are backlogged.

3.4 RFID Systems

A RFID reader and a few tags are in general of little use. The retrieval of a serial number does not provide much information to the user nor does it help to keep track of items in a production chain. The real power of RFID comes in combination with a backend that stores additional information such as descriptions for products and where and when a certain tag was scanned. In general a RFID system has a structure as depicted in figure 2. RFID readers scan tags, and then forward the information to the backend. The backend in general consists of a database and a well defined application interface. When the backend receives new information, it adds it to the database and if needed performs some computation on related fields. The application retrieves data from the backend. In many cases, the application is collocated with the reader itself. An example is the checkout point in a supermarket (Note that the given example uses barcodes instead of RFID tags since they are more common; however, the system would behave in exactly the same way if tags were used). When the reader scans the barcode, the application uses the derived identifier to lookup the current price. In addition, the backend also provides discount information for qualifying products. The backend also decreases the number of available products of that kind and notifies the manager if the amount falls below a certain threshold.

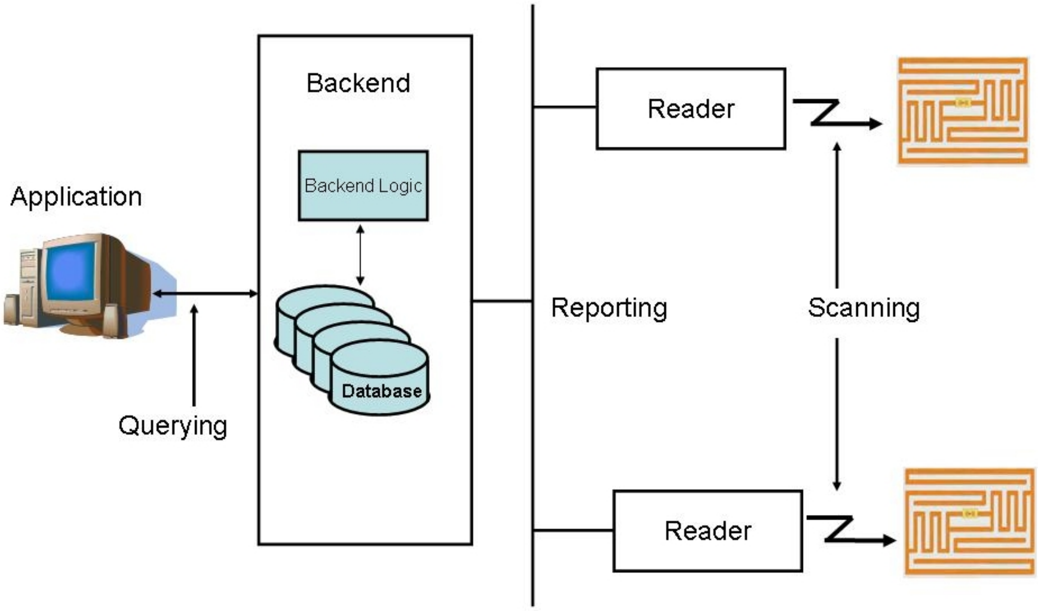

Figure 2: A simplified RFID system

This section describes how RFID tags work in general, what types of tags exist and how they differ. The three frequency ranges that RFID tags typically use are LF, HF, and UHF. Also the difference between passive, semi-passive, and active tags was explained and their advantages and disadvantages were compared. The section concluded by looking at different standards and showed the great interest of the industry by counting the number of issued and backlogged patents [US Patent Office].

Back to Table of Contents

4. Security

The expected proliferation of RFID tags into the billions has raised many privacy and security concerns. A common concern is the loss of privacy when companies scan tags to acquire information about customers and then using data mining techniques to create individual profiles. This section describes possible scenarios where RFID tags can be exploited. Then it describes what mechanisms exist to defeat those threats or at least make them harder to execute. After that the section concentrates on attacks that are directed against RFID systems.

As RFID technology becomes more sophisticated and item level tagging promises more control and large savings in the supply chain management, companies are tagging items within their production process. To maximize the benefits companies start to require their suppliers to label all items delivered to the company. For example, Wal-Mart, Proctor & Gamble, and the US Department of Defense require their suppliers to phase in item-level tagging. However, products are not the only entity tagged. Animal tagging is quite common at large farms to keep track of their moving "property". Also, tagging of humans started to appear. In the Spanish Baja Beach Club, VIP members can get an implant that they can use to pay for their drinks in the club. The implanted tag is a VeriChip.

Anti-RFID activists created a few scenarios to show possible exploits if no precautions are taken. The most common one the unauthorized scanning of tags in order to create user profiles. Other scenarios are scanning the medication a person is carrying to conjecture what illness the person might suffer, or a mugger scanning a crowd of people and singling out a person carrying many valuable items (even money, if tagged as proposed). If tags are replacing credit cards eavesdropping becomes also a problem and must be addressed. The above mentioned issues are privacy concerns, but they are not the only issue. Authentication is also needed. For example, newer tags have rewritable memory available to store extra information during the production process. If stores rely on that information to determine the sales price for example, care must be taken so that customers do not change the type of the item to a cheaper one using portable readers. Also the kill command, a mechanism to permanently disable a tag, must be protected from unauthorized access. Recently a paper raised some concerns in the RFID community that claimed that cell phones can be reprogrammed to disable HF tags. In case that tags carry personal information (such as medical history, credit card numbers) a reader has to be authenticated and authorized before it is allowed access the data. In the previous examples the reader has to authenticate to the tag, there are also scenarios when the tag has to authenticate to the reader, for example to detect forged tags.

4.1 Privacy

This section describes methods to ensure privacy. This are usually mechanisms that kick in after the customer bought the product. They are either enabled at time of purchase or controlled by a user-owned device.

- Kill command: A command supported by the EPC Class 1 and 2 tags. The command will render the tag unusable once received. To prevent an adversary to call those commands they are password protected, EPC Class 1 tags have 8 bit passwords and EPC Class 2 tags have 32 bit passwords. A theoretical paper described how to reprogram a cell phone with a firmware update to make it scan for tags and once found to quickly enumerate over all possible passwords. A more intelligent approach is described in [Oren06] where the password for the kill command can be discovered by using power analysis on the back scattered signal. The power analysis works since the strength of the back scattered signal depends on how much power the chip on the tag drains which in turn depends on the amount and type of computation it does. Newer chips try to design the circuitry so that power analysis is not possible anymore.
- Sleep command: A tag cannot always be killed. Killing a tag on a library book would require retagging the book upon return and therefore defeating the purpose. And yet the privacy of library uses should be protected. The sleep command works similar to the kill command. Once received the only command accepted is the password protected wakeup command. The sleep command suffers from the same problems as the kill command.
- Relabeling: [Inoue03] describes an approach where the customer can relabel the item tag with a string of user's choice. Some of the old information however remains in a password protected area. The idea is to make that protected information available when the product is discarded so that recycling plants can

easily sort items by material.

- Split approach: For this approach the information is distributed over two tags and one of the tags is removable by the customer (for example a paper tag on clothing). The fixed tag stores just general information such as the type, care information, etc. of the product while the removable tag contains the serial number. This approach allows item tracking by its unique identifier and still allows the customer to keep track of its own items.
- Proxy approach: [Rieback05] describes the RFID Guardian. It assumes that all tags are protected by a PIN that the user can set. Once an item is bought the guardian sets a new PIN. If another reader wants to have access to the data stored on a tag the reader requests that information from the guardian which retrieves it from the tag and forwards it to the reader if the reader is authorized.
- Distance approach: As described in [Fishkin04], tags use the signal-to-noise ratio to get a rough estimate of the readers distance. The closer the reader, the more information is released. For example, scanning an item from far away returns general information such as "I am a sweatshirt", medium range scanning returns "I am a blue sweatshirt of a certain brand", and close range scanning reveals finally the serial number. The advantage of the scheme is that it does not require customer actions while still providing those benefits. However, those tags are likely to be more expensive.
- Blocking approach: A rather crude approach is the following: A special tag that does not follow the medium access protocol is used. RFID tags use a special protocol that controls the access to the shared medium (air). When a reader is in an area with multiple tags it first discovers all tags in its range and then it polls each of the tags. The special tag suppresses that mechanism by back scattering a random signal, practically jamming the frequency used. The example given in the paper is similar to the following. Items are bought in a supermarket, scanned at the checkout point and then placed in a plastic bag with the blocker tag. While the bag is carried home nobody can scan the content of the bag. At home the items are removed from the bag and placed in the fridge. The fridge can then scan the items and add it to the inventory. Instead of implementing that functionality in a tag it can also be implemented into a cell phone for example which creates a safe bubble around its carrier.

Many more approaches exist to protect the privacy of customers but they cannot be discussed here for space reasons. A common problem in general with privacy in case of RFID is that tags are usually small and often embedded, so most people are not aware of them at all. Similar, scanning of tags happens also without people noticing. Some papers proposed the deployment of reader devices that notify their surroundings if an unauthorized reader becomes active. Examples for possible deployment of those devices are hospitals or other controlled facilities where confidential information is often exchanged.

4.2 Authentication

The goal of authentication is to make sure that an entity is what it claims to be. In the context of RFID it means that tags can distinguish authorized readers from other readers. This can be done by using encryption with a preshared key. The other way around is much more difficult. Here a reader has to ensure that the tag it is reading is not altered or copied. As it turns out it is a rather hard problem. Encryption is typically used to establish some trust between both participants of a conversation (in addition to privacy). The main problem for this approach is the very limited resources on the tag itself. Most tags have only a few hundred logic gates, but most encryption schemes require several thousand gates. Several lightweight encryption protocols have been implemented such as AES [Feldhofer04] and [Juels04]. However, it has been shown that they have many weak points and can be broken. For example the Digital Signature Transponder (DST) algorithm protecting the Speed Pass was broken by researchers from the John Hopkins University [Bono05] allowing them to take gas with a cloned speed-pass.

In addition to weaknesses in encryption algorithms themselves, RFID tags provide unwillingly more help to break those algorithms. Many current tags "export" lower layer properties, such as the power and timing of the back scattered signal and the processing delay which differ from input to input. That extra information can be used to break encryption even more easily. Newer tags try to fix that problem by two independent circuits for computation and back scattering.

The hope that future generations of RFID tags will provide more resources to implement stronger encryptions might not come true. The reason for this is that there is (and there might always be) the price pressure that demands cheaper tags for item level tagging. And more resources mean higher prices.

4.3 Attack Ranges

In this section I am presenting different ranges that become interesting in terms of security. At the first look, the transmission range specified in the standard seems to be the only range that an intruder is interested in; however, it turns out that ranges far beyond the specified range can be used to gather information about a tag.

The following five ranges have been discussed in [Juels06] and should be kept in mind when designing a new security protocol.

- Nominal reading range: This is the range specified by the standard. It is the range in which a sender conforming to the standard can communicate with the tag.
- Rogue reading range: This is the range for which a modified sender can communicate with the tag. The modifications can include: sending a signal at higher power than the standard specifies or having a high-gain antenna or antenna array. Needless to say that those modifications can increase the range dramatically.
- Tag-to-Reader eavesdropping range: Here the misbehaving reader listens to the back scattered signal when the tag is queried by another reader. Note that the misbehaving reader is passive in this case. This range is larger than the rouge scanning range since the reader does not need to power the tag which is usually the read-range limitation.
- Reader-to-Tag eavesdropping range: Here the misbehaving reader listens to the signal sent by the reader that queries the tag. That signal can be read from several kilometers away since the reader has to provide a strong enough signal to power the tag. Note that the misbehaving reader is passive again. This range is larger than the previous one. A misbehaving reader that is able to observe the Tag-to-Reader communication can also observe the Reader-to-Tag communication, therefore getting a full transcript of the communication.
- Detection range: This is the range where it is possible to detect the presence of a tag or a reader. At this range it is not possible to capture any intelligible information. However, that might not be needed. The detection range for a reader is much larger than for a tag. An example where this range matters is given now: As described earlier the DOD requires item-level tagging. Now a missile can be developed that locks on to a reader or tag signal. Even though this example is far from real it shows that this range cannot be neglected.

One example of exploiting read ranges is given in [Westhues05] where J. Westhues built an apparatus for recording RF conversations between proximity cards and building access readers from a larger distance. Those recorded talks were later played back to gain access to the building. Note that in this example not only was the reading range exploited, also no authentication was in place. It also shows another problem: Users of RFID technology might not even be aware of an ongoing exploit since it does neither interfere with their current doing nor does it leave a trace.

4.4 Attacks against RFID Systems

This section describes different kinds of attacks and exploits that an RFID system might suffer from.

- Sniffing and eavesdropping: Most systems use clear text communication for various reasons like too few resources for encryption, too expensive to implement, problems with distributing keys for some schemes, etc. In those systems sniffing is a powerful attack as it can reveal a lot of interesting information for the eavesdropper. Also simple RFID tags do not provide any protection against being read by a misbehaving reader. The learned information can later be used in other attacks against the RFID system.

- Tracking: As mentioned earlier, this exploit tries to collect and relate as much information as possible. Especially when item-level tagging becomes ubiquitous it becomes possible to create a precise profile of a person. That results in a loss of privacy.
- Spoofing: In this attack scheme an attacker can read the data from an authentic tag and copy it to a blank tag. Since most tags do not provide some kind of authentication or access control an attacker can simply read tags of passing people and save them onto a blank tag for later use. [Rieback06a] gives an example of a spoofing attack. The attacker reads the tag's data from an item at a store and creates a new tag that replaces the tag for a similar but more expensive item. The retagged item can then be checked out and the attacker will only be charged for the cheaper item.
- Replay: In this attack the attacker intercepts communication between a reader and a tag. At a later time the original tag's response can be reused when attacker receives a query from the reader. An example where the conversations between proximity cards and a building access reader was recorded and played back was given at the end of the authentication section. Another example that is often used is the following: A car can record the response that another car gives to the automated toll collection system and use the same response when passing an EZ-Pass checkpoint. The implementation of a challenge-response protocol can prevent those attacks.
- Denial of service: This attack can have many different forms. One form is by simply jamming the frequencies used by the RFID system, therefore making communication impossible. Similar by interfering with the MAC protocol another RFID tag (see blocker tag in the privacy section) can prevent a reader from discovering and polling tags. To disable a tag it is enough to wrap it in some metal foil. That prevents the tags from receiving enough energy to respond to queries. This is often used by thieves to disable EAS tags. Apparently it became such a problem that the state of Colorado made it a misdemeanor to wear aluminum underwear in stores with the intent to circumvent theft detection systems [ColoradoLaw]. A more manual intensive attack is the following scheme: An Anti-RFID activist might attach random labels on items throughout the store. That causes the RFID system to collect meaningless data that discredits RFID technology.
- Virus: An old attack in a new area is the RFID Virus as presented in [Rieback06b]. The virus targets the database backend in the RFID system. Usually data read from the tags is stored in a database. The virus is a classical SQL injection exploit that targets unchecked or improperly escaped input to the database to execute additional commands.

It becomes more and more apparent that technology alone is not sufficient to address all problems above; it needs support by the legislature. Some US states already released laws such as California's "Identity Information protection Act" of 2005. Even if it would be possible to build a sophisticated tag with strong encryption etc., it would increase a tags price and therefore makes it uninteresting for most applications.

In this section several important issues are addressed. First, possible exploits were discussed and proposals were presented that try to fix those problems. Those proposals range from simple measures such as destroying the tag with the kill command to more sophisticated approaches such as the guardian approach. Then authentication in RFID systems was described. It is a hard problem, mainly because of the limited resources on the chip. Last but not least, several attacks against RFID system have been talked about. Even though RFID tags are simple, there are many possible exploits.

Back to Table of Contents

5. RFID Location and Tracking

RFID tags can be used for more than just labeling items. This section presents two proposals that can locate tags and track the movements of them.

[Jiang06] presents a study on how to detect movements of an object tagged with a RFID chip. The use of handheld readers to monitor the worker's motion and acceleration detecting tags are dismissed as not applicable or too expensive. The proposed method works as follows: The reader polls the tag a certain number of times per second and counts the number of responses. The observation is that the number of responses decreases when the distance increases. By further analyzing changes in derived approximations of signal-intensity levels a one antenna system works only within a short radial range and limited angles. By increasing the number of readers and tags the systems accuracy can be improved.

[Haehnel04] is another paper about mapping and localization. In contrast to the other paper they use a robot with 2 antennae located 45 degree to the left and right with respect to the robot, also the robot (reader) is mobile. By comparing the signal strength received on both antennae they can estimate the position of a tag with the Monte Carlo localization algorithm. They show that their method works also in a highly dynamic environment where tags are attached to moving objects. In addition they show that their method can be used to derive the coordinates of the robot if a map of the environment is available.

[InformationWeek] and [RadarGolf] put RFID location to practical use. An RFID tag is incorporated into a golf ball. The mobile reader carried by the player indicated a balls position on its LCD Screen or via audio feedback. Detection range is 30 - 100 feet. Unfortunately, the method that is used to locate the ball is proprietary and not described.

This section presented a short introduction into the world of tracking labeled object. With the growing ubiquity of RFID tags those mechanisms might become second nature to us when we need to find our items, maybe track where our children go, etc.

Back to Table of Contents

6. New Production Methods

This section discusses new ways of producing RFID tags. Tags produced in the current standard process cost between 7.5 and 15 cents. For item-level tagging that cost is still prohibitive. A survey reported that the ideal tag should cost less than a cent. The current production process uses low cost silicon chips which are placed onto an external antenna. The largest part of the production is the attachment of the chip to the antenna. Even with advanced methods such as pick-and-place and fluid self assembly as reported in [Subramanian05] the cost is still high.

Printing a complete tag seems to be a viable alternative. Organic substance is used as printing material. The first RFID tag made from organic material (although not by printing) was presented in 2004, contained 171 polymer thin film transistors, and worked at 125 kHz [Krumm04]. Another organic RFID tag is described in [Baude04]. Since then many papers report progress of printing active and passive parts of the circuitry. [Subramanian06] for example describes how to print transistors. Currently most printed parts are not able to run at the targeted 13.56 MHz but progress is steady.

The reason why 13.56 MHz is targeted is that higher frequencies, although superior in range, suffer from the presence of metals and fluids, while lower frequencies require too large spiral inductors.

Back to Table of Contents

7. Social Implications of RFID

The following section is not intended to serve as an argument against RFID tags, nor does it provide a scientific foundation. It is merely here to show also the social impact that a new technology creates and has to cope with.

In the security chapter it was discussed that many people do not trust RFID technology and fear that their privacy might get compromised. In this chapter the objection comes from a different group of people with a different background.

The following paragraph is a part from the Bible:

And he causeth all, both small and great, rich and poor, free and bond, to receive a mark in their right hand, or in their foreheads. And that no man might buy or sell, save he that had the mark, or the name of the beast, or the number of the beast. Here is the wisdom. Let him that hath understanding count the number of the beast for it is a human number. His number is - 666. - Revelation 13:16-18

Some people believe that RFID tags are the mark of the beast and rally against it. Their argumentation has two main arguments. The first argument is that RFID tags are likely to replace currencies and credit cards as well as all other ways of paying. In addition they would also serve as identification. That requires people to receive a tag because no one can buy or sell without it, independent of being rich or poor. The second argument is as follows: Since RFID tags are also used as identification they should be implanted to avoid loosing the ID or switching it with someone. Current research has shown that the ideal location for the implant is indeed the forehead or the hand; since they are easy to access and unlike most other body parts do not contain much fluids which interferes which the reading of the chip.

It is unlikely that this issue will prevent RFID technology from succeeding.

Back to Table of Contents

8. Summary

This paper presented a survey on RFID technology. RFID technology has a big potential to become ubiquitous in the near future. Today it is already successfully used in supply chain management to track pallets of items. Tracking allows better coordination and control in the production cycle. Now the industry is pushing towards item-level tagging to increase the control even further. However, that also creates concerns, most common privacy concern, but also other security related issues. The paper presented possible scenarios how privacy can be compromised by RFID tags but also several solutions to protect against it. Since RFID technology becomes more and more common, attacks against the system itself start to appear. This paper listed the most common, starting from common sniffing and eavesdropping over denial of service to new RFID viruses.

The paper also showed that there is more to RFID than just supply chain management. The paper covers mechanisms that allow locating or tracking a possibly moving object. Last but not least the paper also surveys research for new production methods for tags. Currently printing tags with organic materials seems to be a promising approach. By printing tags, the cost-intensive assembly of the two main components, antenna and chip, can be eliminated. It also adds higher flexibility to production.

The paper concludes by looking at some social implications that RFID causes. Although not technically relevant, it provides a good outside perspective.

Back to Table of Contents

9. References

URLs:
[Baja Beach Club] Uses implanted RFID tags to identify and charge VIP members: http://www.bajabeach.es/
[VeriChip] Company that produces human-implantable RFID chips: http://www.verichipcorp.com
[EZ-Pass] Electronic toll collection for toll roads and bridges: http://www.e-zpassiag.com
[Speed Pass] Paying at Exxon and Mobile gas stations with RFID tags: https://www.speedpass.com/forms/frmHowItWorks.aspx?pPg=howTech.htm&pgHeader=how
[Wiki-RFID] Wikipedia-RFID: http://en.wikipedia.org/wiki/Rfid
[Wizard Wars] The invention of IFF in WWII: http://www.vectorsite.net/ttwiz1.html
[US. Patent 3,713,148] The probably first RFID patent: http://patft.uspto.gov/netacgi/nph-Parser?patentnumber=3,713,148
[US Patent Office] http://www.uspto.gov/
[ICAO] International Civil Aviation Organization: Guidelines for RFID enabled passports: http://www.icao.int
[ColoradoLaw] Colorado State Legislature: Colorado state legislature makes aluminum underwear a misdemeanor, http://www.state.co.us/gov_dir/leg_dir/olls/sl2001/sl.162.htm
[InformationWeek] Article on RFID enhanced golf balls: http://www.informationweek.com/story/showArticle.jhtml?articleID=57703713
[RadarGolf.com] A company producing a "Ball Positioning System": http://www.radargolf.com
[Oren06] Yossi Oren, Adi Shamir, "Power Analysis of RFID Tags", Power analysis reveals kill passwords on RFID tags: http://www.wisdom.weizmann.ac.il/%7Eyossio/rfid/
[EPC Global Inc.] http://www.epcglobalinc.org/
[Auto ID Center] http://www.autoidcenter.org/

Papers:
[Landt01] Jerry Landt, "Shrouds of Time": outlines history and present of RFID: http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf
[Baude03] P. F. Baude, D. A. Ender, T. W. Kelley, M. A. Haase, D. V. Muyres, and S. D. Theiss, "Organic Semiconductor RFID Transponders", Electron Devices Meeting, 2003.
[Inoue03] S. Inoue and H. Yasuura, "RFID privacy using user-controllable uniqueness", in Proc. RFID Privacy Workshop, Nov. 2003. http://www.rfidprivacy.us/2003/papers/sozo_inoue.pdf
[Feldhofer04] M. Feldhofer, S. Dominikus, and J. Wolkerstofer, "Strong Authentication for RFID Using the AES Algorithm", Cryptographic Hardware and Embedded Systems 2004. http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=3156&spage=357
[Fishkin04] K. P. Fishkin, S. Roy, and B. Jiang, "Some methods for privacy in RFID communication", in Proc. 1st Eur. Workshop on Security in Ad-Hoc and Sensor Networks, 2004, http://www.intel-research.net/Publications/Seattle/062420041517_243.pdf
[Haehnel04] D. Haehnel, W. Burgard, D. Fox, K. Fishkin, and M. Philipose, "Mapping and Localization with WID Technology", International Conference on Robotics & Automation, 2004.
[Juels04] A. Juels, "Minimalistic Cryptography for Low-Cost RFID Tags", Security in Communication Networks 2004
[Krumm04] J. Krumm, E. Eckert, W. H. Glauert, A. Ullmann, W. Fix, and W. Clemens, "A Polymer Transistor Circuit Using PDHTT", Electron Device Letters, 2004.
[Bono05] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo, "Security analysis of a cryptographically-enabled RFID device", in Proc. 14th USENIX Security Symp., 2005, http://rfidanalysis.org

/DSTbreak.pdf
[Micheal05] K. Michael, L. McCathie, "The pros and cons of RFID in supply chain management", International Conference on Mobile Business, 2005.
[Philips05] T. Phillips, T. Karygiannis, R. Kuhn, "Security Standards for the RFID Market".
[Rieback05] M. Rieback, B. Crispo, and A. Tanenbaum, "RFID Guardian, A battery-powered mobile device for RFID privacy management", in Proc. Australasian Conf. Inf. Security and Privacy, 2005, http://www.cs.vu.nl/~melanie/rfid_guardian/papers/acisp.05.pdf
[Subramanian05] V. Subramanian, P. C. Chang, D. Huang, J. B. Lee, S. E. Molesa, D. R. Redinger, and S. K. Volkman, "Printed organic transistors for ultra-low-cost RFID applications", IEEE Transactions On Components And Packaging Technologies, 2005.
[Jiang06] B. Jiang, K. P. Fishkin, S. Roy, and Matthai Philipose, "Unobtrusive Long-Range Detection of Passive RFID Tag Motion", IEEE Transactions On Instrumentation And Measurement, 2006.
[Juels06] Ari Juels, "RFID Security and Privacy: A Research Survey", IEEE Journal On Selected Areas In Communications.
[Rieback06a] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, "The Evolution of RFID Security"; Pervasive Computing, IEEE Volume 5, Issue 1, Jan.- Mar. 2006.
[Rieback06b] Melanie R. Rieback, Bruno Crispo, Andrew S. Tanenbaum, "Is Your Cat Infected with a Computer Virus?", http://www.rfidvirus.org/papers/percom.06.pdf
[Subramanian06] V. Subramanian, P. C. Chang, D. Huang, J. B. Lee, S. E. Molesa, D. R. Redinger, and S. K. Volkman, "All-printed RFID Tags: Materials, Devices, and Circuit Implications", VLSI Design, 2006.

Books:
[Westhues05] J. Westhues, "Hacking the prox card," in RFID: Applications, Security, and Privacy, S. Garfinkel and B. Rosenberg, Eds. Reading, MA: Addison-Wesley, 2005, pp. 291-300.

Back to Table of Contents

10.Acronymns

AES - Advanced Encryption Standard
DOD - Department of Defense
DST - Digital Signature Transponder
EAS - Electronic Article Surveillance
EPC - Electronic Product Code
HF - High Frequency
IFF - Identification Friend or Foe
ISO - International Organization for Standardization
LF - Low Frequency
RFID - Radio Frequency IDentification
SQL - Structured Query Language
UHF - Ultra High Frequency

Back to Table of Contents

Last Modified April 24, 2006

Note: This paper is available on-line at http://www1.cse .wustl.edu/~jain/cse574-06/index.html