Tagging The World:

An Investigation into Radio Frequency Identification (RFID) Technology

By Harry Schilbach

Contents

The Brief:

i-Technologies In Course Assessment Part 2

In-Depth Report

Ubiquitous technologies are used every day and can be found in many spheres of life. For this assessment you must write an in-depth report on a novel ubiquitous computing application. This needs to include a specification, information regarding the design and its application relating to general consumers and businesses as well as its impact on the economy. You will need to include advantages and disadvantages in each area. You can use research from Part 1 of the ICA if you wish (assuming you choose the same subject area – you may pick something different).

The Report

The report should be word processed and at least 3000 words but no more than 5000 words. You must hand in two copies of your bound paper report and two electronic copies, which MUST include the following sections:

Introduction

Why Radio Frequency Identification (RFID) tags? I think one of the most fascinating aspects of certain ubiquitous technologies is how they can permeate society without much notice. No wild press fervour as is now the standard for any Apple product, no legion of blog writers dissecting (both physically and metaphorically) every aspect and release of a project, just a simple unseen progression into everyday life. RFID tags are one of those technologies.

Relatively slowly, over the last thirty or so years, as the technology has caught up with the concept and manufacturing costs have fallen enough to make the tags both a mass market item and a disposable item RFID Tags have now become part of our everyday life – whether we realise or not. To CD's bought on the high street, to passports, to travelling on toll roads, to access to your home or office, to implantation in our pets. RFID tags are everywhere.

In this investigation I'm going to be looking at the technology, history and application of RFID Tags. Finally I'll look what the future holds for this technology and concerns around privacy. However before we start our investigation let's try and get a working definition of what RFID is about.

What Are They & How Do They Work?

A RFID system contains two major elements; a small electronic chip, which can store data, linked to an antenna that can communicate that data, via radio waves, and a receiver that can read or write that data. The chip and antenna that broadcasts the data is known as a Tag or Transponder, whilst the receiver is known as a Reader. See *figure I*:

Figure i - Tag & Reader Elements of RFID.

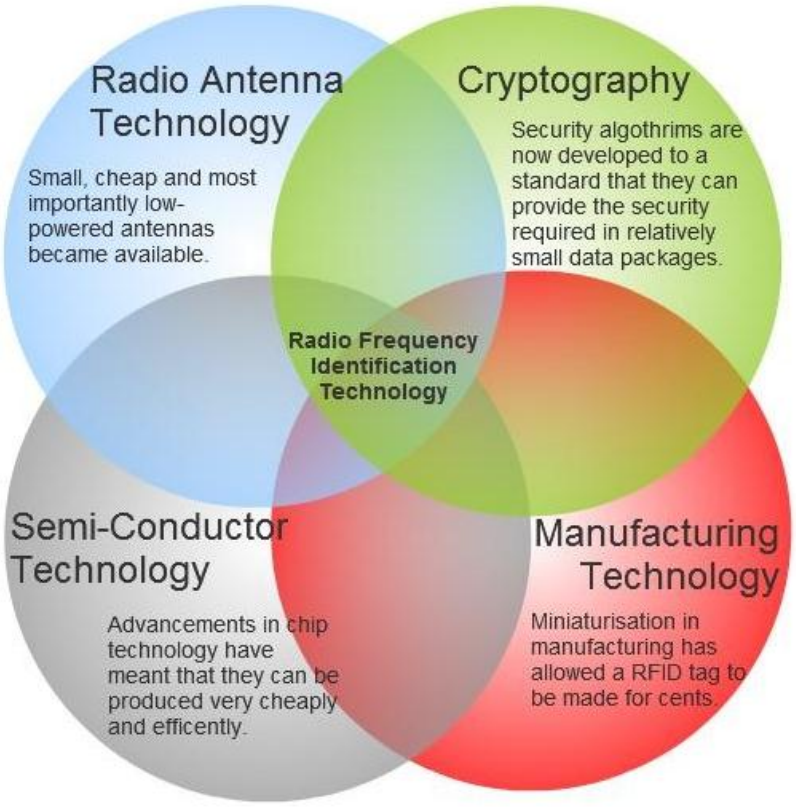
The purpose of RFID tags are to identity objects to a reader for a variety of purposes. The concept can be likened to the bar-code system that it is starting to replace. The tag

contains information that is revealed to the reader when it is in proximity of the tags' range. The advantages over bar-codes are manifold, but include no line of sight required to read them - so that they can be embedded within an object or person. They can also read many items at once and indeed whereas a bar-code identifies a particular type of product, say a 150 g bar of a brand of soap, an RFID tagged product can identify the same bar of soap as well as distinguish it from the millions of other bars of soap that came from the same factory.

The information on the tag could be anything from a product code on a CD to biometric details of a passport holder. Because the tag only has to be in the working range of the receiver the tag does not require physical contact with the reader, giving it an advantage over other technologies such as the aforementioned bar-codes and smartcards.

Technologies from a number of different fields were used in the development of RFID tags. Radio frequency technology was used to enable the data communication between the tag and the receiver; Cryptography is applied to maintain the security of the data transmission; Semi-conductor technology has provided computer chips that are both small enough and inexpensive enough to make RFIDs discreet and applicable to mass application.

Figure ii - Helping to make RFID Ubiquitous - the Technologies needed.



Whilst RFID systems can trace their origins back to World War 2 (Roberti), development and commercialisation really started to take off in the 1970's and whilst '…no single individual may take credit for all of the technological advances that led up to the ultimate development of RFID..' (RFID Contributions, 2005), it was Charles Walton who received approval for an application for a simple RFID system embedded into a door lock; this could be unlocked when a tag with the correct identifying number came within range.

Whilst RFID systems can take many forms and standards the concept of tag and reader are central to all, with a tag communicating data to a reader. RFID tags communicate through radio technology. A signal is sent to a tag, which wakes up and either reflects back a signal or broadcasts a signal.

RFID tags can be broadly segmented into two categories. Passive RFID tags and Active or Non-Passive tags. An active transponder or tag is one that carries its own power supply in the form of a battery, whereas a passive tag is powered or activated by the use of magnetic or electromagnetic fields. Let's explore this a little further.

An active tag has its own battery which it uses to power its own transmitter to broadcast the information it holds to the receiver. The advantages of this are that it allows the tag to have a greater broadcast range meaning that the reader can detect the tag from a greater distance; this is employed to great effect in the shipping container industry where containers have a powerful active tag meaning that they can be located and identified individually within a stack of containers on a dockside or when loaded onto a container vessel or lorry, allowing the container industry to grow to a multi-billion dollar industry and allowing docking facilities to grow in both size and complexity

A passive transponder does not have its own onboard power supply and takes power from the reader or receiver using magnetic or electromagnetic fields. What does that mean? We shall go into this technology a little further as it the application of battery-less transponder that has had a greater impact in making this technology ubiquitous allowing a much cheaper cost and making the tag more disposable or recyclable, however the main advantage is that tags are not dependent on battery life to communicate, allowing deployment independent of power source for a great period of time.

The passive tag is 'woken' by the readers' radio waves. The tag, using radio frequency technology, harvests energy from radio waves, allowing it to power-up and broadcast the information that it holds within its chip. The amount of power required is very small and may only power the device for a fraction of a second, depending on the amount of data scored; a passive tag can store in the range of 64b to a 1kb (Zebra Technologies).

One of the simplest examples of this is the type of passive RFID system employed in retail outlets. A reader device is placed at the exits of the shop, at the checkout and goods within the shop are tagged with a transponder. The transponder holds very little data; it contains only two states on or off, '1' or '0' in binary terms. The tagged goods natural states are on. If the tags pass the readers at the exit in this state the reader is programmed to output to an alarm. The checkout has a reader that is able to write to the tag as well as read, this enables the staff to change the state of the tag to 'off' and the tag to pass through the exit readers without triggering the alarm.

Which type of tag to use depends largely on the object it is being attached too and the field of application. 'Whereas a railway car would have an active RFID tag, a bottle of shampoo would have a passive tag' (Bonsor & Keener, 2007). This would enable the railway carriage to be located in a busy railway siding from several hundred metres and exactly easily stop the shampoo bottle from being stolen from a shop without having its RFID de-activated. This also reflects the cost and size of the differing tags. An active tag is bulkier, more robust and more expensive as it requires a battery and bigger aerial to send its data. The economies of this require the tag to remain within the supply chain and be reused, whereas a passive tag can be mass-produced for pennies economically and environmentally responsibly.

Adoptees of RFID technology face three central challenges according to Microsoft's Javed Sikander. The installation of hardware and software infrastructures and the implementation of the business processes needed to manage the RFID system. We've already looked at the hardware and software options above. The third challenge is to integrate RFID technology into your business processes, 'integrating the data into decision support systems, and sharing data with trading partners for business collaboration.' (Sikander, 2005). This means making use of the data that the RFID technology provides to encourage new business opportunities and exploit efficiencies in current practices. This could mean sharing the RFID data with suppliers' or customers' to enhance your business relationship and provide, through say less wastage, cost savings for both parties.

How We Use RFID?

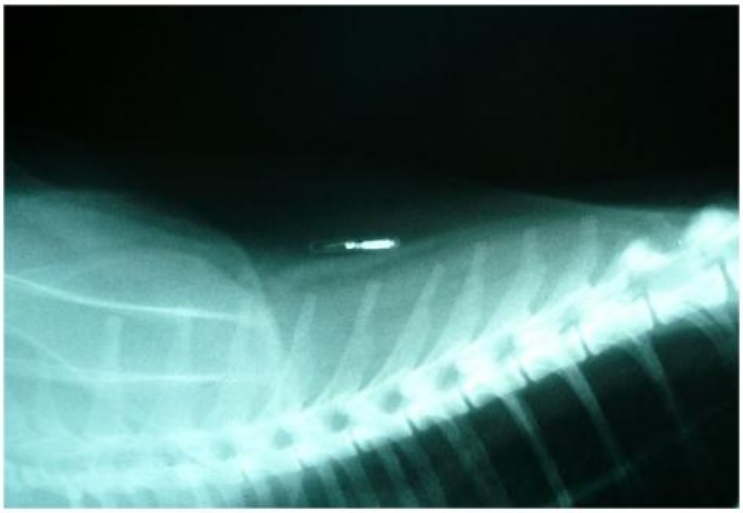
RFID technology's greatest success at present has been in the supply chain – getting goods from our factories to our shops. Again, as we have seen with the 'slow-burn' progression of RFID this is not a new development. One of the first commercialisations of the technology was in the US, in the mid 1970's, the Las Alamos National Laboratory came up with a way of tracking nuclear material by putting transponders within consignments of the material and readers at the gates of secure facilities (Roberti). The readers waking and receiving data from the transponder such as consignment number and driver details, this is still the basic architecture used today – albeit refined.

Let's have a further look at how RFID technology has been the answer to some problems within everyday life; from looking at how it's used to located lost cats to how it can change the way we use toll roads; to helping the spread of counterfeit drugs in a black market worth billions.

Around the turn of the century vets started to offer the facility to tag your pet. Miniaturisation had enabled a passive RFID tag to be produced for the purpose that was around the size of a grain of rice (see figure iv). The RFID tag contains the standard components of a microchip and antenna all sealed in a biocompatible sealed glass casing,

this protects both the animal and the RFID tag. The tag has a unique identifying number held within its memory that is registered with central databases, as well as details of the type of tag and possibly the veterinarian's details. This allows any vets or animal shelter with a reader to scan the animal and access the identifying number to reunite pet to owner. This is much more secure and advanced method over the old collar and tag method, if the pet loses the collar methods of returning the pet are very limited. Cost is affordable at around the £10 - £20 price point and a passive tag will last a cats' lifetime. The only disadvantage over a tag and collar is that without a scanner a person cannot return the animal to its owner without using a scanner.

Figure iii - X-Ray of RFID implant in Cat.



Toll roads and bridges have long created queues and bottle-necks where vehicles have to stop to pay the use the road. This is a problem that RFID Technology can resolve. Using a transponder or tag attached to a vehicles windscreen and a scanner or receiver at certain points of a toll gate (see figure iv), with the data going to an information system to charge an account for using the toll road. This means that vehicles do not have to stop and pay at the toll booth, merely pass within the range of the reader. RFID does not work alone in this system, it works in conjunction with a camera monitoring system that confirms that the details from the tag match the vehicle that it is using it, in future this could be remedied by embedding the tag into the vehicle at manufacture, meaning that a vehicle would have the same RFID identification throughout its life and could be used for a variety of functions from the manufacturer tracking the vehicle through its supply chain to servicing and MOT testing, to allowing the current owner to pay remotely for parking or even petrol. Although some say this creates privacy concerns about who has access to the data, such information could easily make a persons' movements traceable.

Figure iv - Diagram Showing RFID in action with E-ZPass System

The pharmaceutical industry is suffering globally from a massive market in counterfeit drugs. The international consultancy Deloitte reckoned the yearly market for counterfeit drugs to be worth a massive $75 to 200 billion a year (The Economist, 2010)**, this is not only a loss of revenue for the manufacturers but a deadly killer of at least 10 000 people a year – estimates an American think-thank. Pfizer, a global pharmaceutical company, has addressed this problem with one of its most counterfeited products – Viagra; Implementing RFID technology into its production process to embed tags in its packaging allowing tracking throughout the supply chain to end retailers' who can use the tag to verify its authenticity over a secure internet connection** (O'connor, 2006), **whilst this application has had great success in Europe and the USA it still has limitation, as the majority of counterfeit drugs are sold in developing markets where access to RFID readers or indeed a secure internet connection.**

How Will We Use RFID -Or Misuse Them?

As we can see RFID systems have penetrated many aspects of modern life, but what does the future hold for this burgeoning technology.

As RFID tags have become more ubiquitous in manufacturers' supply chain we could expect to see how we shop change. Most retailers currently use bar code scanning to process our goods at check outs, with the ubiquity of RFIDs this could easily change within the near future IBM believe that checkout queues will be a thing of the past (IBM , 2006) **with shoppers simply placing items straight into their bags and leaving the shop when they've finished. In the background RFID systems will be at will be at work totalling up what you've left the store with and debiting your registered debit card.**

We've already talked about how ubiquitous RFID is becoming; Ubiquity is required for the concept of the 'internet of things'. The 'internet of things' was first talked about at a Xerox research centre in California where researchers imagined a future where the 'virtual and real worlds collide' (The Economist, 2010)**, where everything in our real world is tagged and**

sending data back to the virtual world. A good working definition comes from Stephen Heller, a development architect at German software giant SAP.

> ***'A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes. Services are available to interact with these 'smart objects' over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues.'***
> **(Haller, 2009)**

Haller and many others envision a near future where everything we have can communicate with its surrounding. From a box of cornflakes to your car (IBM, 2010) sensors can relate not only to each other but also to information systems; for instance your cornflake box could realise that it's getting empty and communicate with your online supermarket account or database adding an order for a new box.

Jesse Schell takes the RFID laden world of the 'internet of things' a step further talking about the 'gamification of life' (Schell, 2010), a world where every tag or sensor has the capacity to give you a points based reward – your toothbrush would use it's RFID Tag to sense when you had brushed your teeth for the recommended amount of time and give you a 1 000 points for doing so, sponsored by the toothpaste company. Every aspect of life could be 'gamified', facilitated by RFID technology, a sort of huge loyalty scheme of the same ilk the major supermarkets run Schell believes that this has the power to alter human behaviour for better – to make us better people and a better world for all. But could social engineering on this scale have a more sinister capacity; who controls the sensors and the huge mass of data that they produce?

In 2010 organisations already struggle to control and secure our personal data as witnessed by Sony's recent admission that it had had 'around 77 million users' PlayStations personal data hacked' (BBC , 2011) and which The Economist is calling the '…biggest breach of data privacy since the advent of the internet.' (The Economist, 2011). How will organisations cope with the virtual tsunami of data that a RFID connected world will produce?

RFID technology has the potential change many aspects of our life, but what are the dangers that accompany this? Partly due to its nature as an unseen background technology there hasn't been much public debate about RFID technology and privacy. Some believe that we're sleep-walking into a world where governments and businesses can monitor our every move through the products we buy and consume.

One area which has attracted a lot of controversy is the implantation of RFID tags into humans. Whilst this holds no technological problems, as we've discussed - we're been implanting animals for many years, however ethical and moral issues abound. In 2004 an American company called Verichip gained approval from FDA for a chip that could be implantable in humans (Gilbert, 2004), the company targets it's products at Alzheimer's

patients in hospital, using the tag to identify them and using a serial number to link to a database that holds the patients' medical records. Verichip feel that it doesn't breach any privacy concerns as no medical records are actually held on the chip. Proponents for mandatory RFID implantation of humans feel that it is just a progression or modification of a national identity scheme –albeit more secure. They state the huge advantages it would have in the forensic identification of people in the aftermath of huge natural disasters such as the tsunami in South-East Asia in 2004 (Thevissen, 2006). Privacy campaigners and libertarians feel that the state implanting people with traceable RFID devices is a step to far and takes the sphere of the state across a line that it was never meant to cross; new legislation would have to be introduced – although we struggle to think of a political climate where this would be welcome by the electorate.

Figure V - Sleepwalking into an RFID world?

But what about a situation where RFID technology becomes so ubiquitous that we are in effect tagged 24 hours a day. A day when everything from our bank card to our clothes, from our mobile phone to the pack of chewing gum we bought this morning contains a RFID tag. Will we not be tagged de facto?

Technology already exists to modify the RFID readers' they currently use to protect stock from theft to scan people and the RFID tags they have about them to offer discounts or special offers based on what we have already bought; in the street anyone with a reader could scan and identify the contents of your bag.

Whatever the future holds for RFID technology, there is no getting away from the fact that we are already in an RFID world, as we have seen, the huge advantages it has for commerce alone ensure that its slide to ever more ubiquity will continue. With the world generating and demanding ever more data RFID technology becomes an ever more useful way of turning that data into useful information. We should, however, remind ourselves that this is a technology that needs to be monitored, legislated for and regulated to ensure that it both remains within our control and satisfies any concerns we have with it.

Bibliography

RFID Contributions. (2005, May). Retrieved 05 27, 2011, from The Lemelson-MIT Program: http://web.mit.edu/invent/iow/waltonc.html

BBC . (2011, May 6). *Hacker group Anonymous denies Sony Attack*. Retrieved May 07, 2011, from BBC News: http://www.bbc.co.uk/news/technology-13309581

Bonsor, K., & Keener, C. (2007). *How RFID Works*. Retrieved April 19, 2011, from How Stuff Works: http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid3.htm

Gilbert, A. (2004, Oct). *Protecting Your ID: RFID Chips in Humans Get the Go Ahead*. Retrieved 05 12, 2011, from Silicon.com: http://www.silicon.com/legacy/research/specialreports/protectingid/0,3800002220,39124983,00.htm

Haller, S. (2009, May 13). *Internet of Things: An intergral part of the future internet.* Retrieved May 06, 2011, from European Furture Internet Portal: http://services.future-internet.eu/images/1/16/A4_Things_Haller.pdf

IBM . (2006). *IBM RFID Commercial - The Future Market*. Retrieved April 27, 2011, from YouTube: http://www.youtube.com/watch?v=eob532iEpqk&playnext=1&list=PL59B4351E9940A156

IBM. (2010, March 15). *The Internet of things*. Retrieved May 06, 2011, from YouTube: http://www.youtube.com/watch?v=sfEbMV295Kk

O'connor, M. C. (2006, Jun 06). *Pfizer Using RFID to Fight Fake Viagra*. Retrieved 05 11, 2011, from RFID Journal: http://www.rfidjournal.com/article/view/2075

Roberti, M. (n.d.). *The History of RFID Technology*. Retrieved 04 27, 2011, from RFID Journal: http://www.rfidjournal.com/article/view/1338

Schell, J. (2010, Feb). *Jesse Schell: When Games invade real-life*. Retrieved May 07, 2011, from TED: http://www.ted.com/talks/jesse_schell_when_games_invade_real_life.html

Sikander, J. (2005, April). *RFID Enabled Retail Supply Chain*. Retrieved 05 08, 2011, from Microsoft Developers' Network: http://msdn.microsoft.com/en-us/library/ms954628.aspx

The Economist. (2010, November 4). *A Sea of Sensors.* Retrieved May 6, 2011, from The Economist: http://www.economist.com/node/17388356?story_id=17388356&CFID=163604726&CFTOKEN=43715570

The Economist. (2010, Sept 02). *Fake Drugs - Poison Pill*. Retrieved May 11, 2011, from The Economist Online: http://www.economist.com/node/16943895

The Economist. (2011, Apr 30). Cloud Computing's growing pains: Break-ins & Breakdowns. *The economist*, p. 14.

Thevissen, P. W. (2006, Mar). *Implantation of an RFID-tag into human molars to reduce hard...* Retrieved 05 12, 2011, from Katholieke Universiteit Leuven: http://www.forensische-tandheelkunde.be/MFO/articles/06_RFID_01.pdf

Zebra Technologies. (n.d.). *RFID Tag Characteristics*. Retrieved 05 10, 2011, from Zebra Location Solutions : http://www.zebra.com/id/zebra/na/en/index/rfid/faqs/rfid_tag_characteristics.html#FAQ_0953

Works Cited

RFID Contributions. (2005, May). Retrieved 05 27, 2011, from The Lemelson-MIT Program: http://web.mit.edu/invent/iow/waltonc.html

BBC . (2011, May 6). *Hacker group Anonymous denies Sony Attack*. Retrieved May 07, 2011, from BBC News: http://www.bbc.co.uk/news/technology-13309581

Bonsor, K., & Keener, C. (2007). *How RFID Works*. Retrieved April 19, 2011, from How Stuff Works: http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid3.htm

Gilbert, A. (2004, Oct). *Protecting Your ID: RFID Chips in Humans Get the Go Ahead*. Retrieved 05 12, 2011, from Silicon.com: http://www.silicon.com/legacy/research/specialreports/protectingid/0,3800002220,39124983,00.htm

Haller, S. (2009, May 13). *Internet of Things: An intergral part of the future internet.* Retrieved May 06, 2011, from European Furture Internet Portal: http://services.future-internet.eu/images/1/16/A4_Things_Haller.pdf

IBM . (2006). *IBM RFID Commercial - The Future Market*. Retrieved April 27, 2011, from YouTube: http://www.youtube.com/watch?v=eob532iEpqk&playnext=1&list=PL59B4351E9940A156

IBM. (2010, March 15). *The Internet of things*. Retrieved May 06, 2011, from YouTube: http://www.youtube.com/watch?v=sfEbMV295Kk

O'connor, M. C. (2006, Jun 06). *Pfizer Using RFID to Fight Fake Viagra*. Retrieved 05 11, 2011, from RFID Journal: http://www.rfidjournal.com/article/view/2075

Roberti, M. (n.d.). *The History of RFID Technology*. Retrieved 04 27, 2011, from RFID Journal: http://www.rfidjournal.com/article/view/1338

Schell, J. (2010, Feb). *Jesse Schell: When Games invade real-life*. Retrieved May 07, 2011, from TED: http://www.ted.com/talks/jesse_schell_when_games_invade_real_life.html

Sikander, J. (2005, April). *RFID Enabled Retail Supply Chain*. Retrieved 05 08, 2011, from Microsoft Developers' Network: http://msdn.microsoft.com/en-us/library/ms954628.aspx

The Economist. (2010, November 4). *A Sea of Sensors.* Retrieved May 6, 2011, from The Economist: http://www.economist.com/node/17388356?story_id=17388356&CFID=163604726&CFTOKEN=43715570

The Economist. (2010, Sept 02). *Fake Drugs - Poison Pill*. Retrieved May 11, 2011, from The Economist Online: http://www.economist.com/node/16943895

The Economist. (2011, Apr 30). Cloud Computing's growing pains: Break-ins & Breakdowns. *The economist*, p. 14.

Thevissen, P. W. (2006, Mar). *Implantation of an RFID-tag into human molars to reduce hard...* Retrieved 05 12, 2011, from Katholieke Universiteit Leuven: http://www.forensische-tandheelkunde.be/MFO/articles/06_RFID_01.pdf

Zebra Technologies. (n.d.). *RFID Tag Characteristics*. Retrieved 05 10, 2011, from Zebra Location Solutions : http://www.zebra.com/id/zebra/na/en/index/rfid/faqs/rfid_tag_characteristics.html#FAQ_0953