

INVASION OF THE RFIDS: ARE WE HEADING TOWARDS “MODERN TIMES”?

Fabio Ghioni

Security CTO, Telecom Italia

Via Torino, 2 – 20123 Milan, Italy

fabio.ghioni@telecomitalia.it

+39 02 85955616

ABSTRACT

RFIDs (Radio Frequency Identification tags) are small integrated circuits connected to an antenna, which can respond to an interrogating RF signal with simple identifying information, or with more complex signals. The main objective of these tags is to store data and make it readily available as well as ensuring that it is safely stored in or on the object or person that is concerned by the data as well as making counterfeiting of objects more difficult, if not impossible.

RFIDs have been introduced in the filament of Euro banknotes in an attempt to keep track of money movements both when ransoms are requested in non-consecutive notes and in transactions where up to today cash was used to guarantee anonymity. RF scanners will most probably be installed in airports, train stations in order to catch people attempting to move large sums of money out or around countries. This measure should, in theory, reduce tax evasion as well as terrorist activities, including arms and drugs dealing.

In principle, when sensitive data is stored, there should be certain level of security involved in its protection. Data on RFIDs cannot, at present, be encrypted. Physically, a RFID cannot easily be stolen if it is implanted in a person's arm but, a hacker with a suitable RF scanner, could access the data with greater ease and without the victim even noticing.

This paper aims at analysing the implications of introducing RFIDs in the filament of the Euro notes as well as discerning the pros and cons of using this technology in various scenarios and studying the psychological impacts and repercussions of crimes related to the theft and use of the data acquired by the perpetrators. The introduction of RFIDs in paper money will most probably bring about a certain level of discomfort as it will inevitably be perceived as a key factor of control upon our lives.

KEY WORDS

Euro, RFID, security, privacy, tax evasion, terrorism, patient records.

INVASION OF THE RFIDS: ARE WE HEADING TOWARDS “MODERN TIMES”?

1 INTRODUCTION

Radio Frequency Identification tags (RFIDs), are a technology similar, in theory, to bar code identification. With RFID, the electromagnetic or electrostatic coupling in the RF portion of the electromagnetic spectrum is used to transmit signals. An RFID system consists of an antenna and a transceiver, which read the radio frequency and transfer the information to a processing device, and a transponder, or tag, which is an integrated circuit containing the RF circuitry and information to be transmitted. One of the key differences between RFID and bar code technology is RFID eliminates the need for line-of-sight reading that bar coding depends on. Also, RFID scanning can be done at greater distances than bar code scanning.

RFID systems can be used just about anywhere, from clothing tags to missiles, banknotes, transport crates and pallets and even pet tags or pharmaceuticals – anywhere that a unique identification system is needed. The tag can carry information as simple as a pet owners name and address or the cleaning instruction on a sweater to as complex as instructions on how to assemble a car.

Today the biggest user of RFIDs is the US Military. In the Iraq war, the Army Material Command required all its shipments and pallets to be tagged. In this way, it was able to keep track of 300,000 containers around the world everyday. The US Navy kept track of its wounded personnel and prisoners in military hospitals with RFID tags.

2 EURO BANKNOTES

The European Central Bank (ECB) tried to keep its project as low profile as possible. The objective was to introduce RFIDs the size of a grain of sand into the filament of Euro banknotes by 2005 [1]. Though the feat seemed impossible, the ECB has apparently already placed RFID endowed banknotes in circulation. Though there is much controversy on the matter, many people feel that this is just another step towards an Orwellian “Big Brother” world, there are many benefits from a security point of view.

Though there is a very low level of Euro counterfeiting, the introduction of RFIDs will make it an impossible task. Until now, any transaction that required anonymity was paid for in cash. Non sequential banknotes were hard to trace. This is no longer the case. It will be harder for terrorists, drugs and arms dealers to do business in cash, as it will be just as hard for kidnapers to request ransoms and tax evaders to pack stacks of cash in a suitcase and carry it off to some tax paradise. If, as is expected, RF scanners are installed in airports, train stations and any other point of transit, it will become extremely difficult for the innocent looking suitcases to go very far. One can also envision plain clothes police walking down the corridors of cross border trains, in ports or bus stations with a scanner hidden in a bag, in search of people hiding large amounts of money. The main objective is to oblige any person that has to do large money transactions to do so electronically, thus leaving an electronic trail.

Many people are afraid that the possibility of tracking money will lead to governments tracking every person’s expenditure being kept under control. It is unlikely that a government would spend time and money in checking out how much Mrs. Brown spends in cereals or face creams each month even if she does pay cash every time she goes to the grocery store. If Mr. Clouseau crosses the border from France into Switzerland every week end, with the pretext of filling up with cheaper petrol, the French police may want to RF scan his car because he may be slowly taking money across the border and placing it in a Swiss bank account.

3 OTHER USES FOR RFIDS

RFIDs are being used in hundreds of other environments. One of the vastest is in goods transport. If each pallet or container has a RFID it can be tracked from departure to arrival and in the warehouse. As we said, the US Military is the greatest user of this system of goods tracking and can keep track of 300,000 containers around the world everyday.

3.1 Wal- Mart

Wal-Mart uses information technology (IT) as a tool to improve its operations and gain competitive advantage. Several years ago, following an aggressive expansion plan, internal supply chain improvements, and impressive revenue growth, Wal-Mart looked to RFID technology to further improve its operations. Further advances through RFID, such as reduced labour costs, improved inventory control, and advanced market intelligence, appeared to hold significant promise for Wal-Mart. The promise of total supply chain visibility offered by RFID technology was an appealing value proposition. This is because, in spite of billions of dollars of existing investments in supply chain operations, Wal-Mart (and other retailers) experienced problems with lost or misplaced palletized goods. Pallets were sent to the wrong destination or contained fewer cases than originally ordered. Studies show that, on average, products are out of stock in grocery and mass merchandise stores 7% of the time. Some of the most popular items are not available 17% of the time. As a result, retail locations often choose between ordering more than they really need or contend with insufficient stock for the most popular (and often most profitable) items, resulting in lost sales. RFIDs allow Wal-Mart to track individual pallets, cases, or even single items. For example, when a Wal-Mart store receives a pallet containing cereal boxes, the store manager can quickly discern precisely how many cases and individual cereal boxes have arrived. This information could be derived not only from a tag on the pallet, but also from individual, differentiating tags on every case and box. By integrating this data with the store's existing warehouse management system, that manager immediately knows when the supply is low so that a new order can be placed. With barcodes, such item-level verification of goods is impractical, because of the vast amount of handling required to open up every case in a pallet and scan its contents at the receiving dock. With RFID, the entire contents of a pallet, even those containing a variety of different products, can be identified easily and efficiently with minimal handling [2].

3.2 Patient medical records and the Mexican case

As with all types of hardware, as time passes, the size gradually diminishes. This is also the case with RFIDs. There are now tags that are the size of a grain of rice that can be embedded subdermally. These tags have a variety of potential and effective applications. In the US some hospitals are experimenting their use with patient history storage. Critical pathology patients, such as heart disease patients have a tag embedded in there upper arm and when scanned the computer automatically retrieves the patients records from a central database. This radically reduces the time needed to find the correct records and, as each tag has a unique number, it also reduces the risk of retrieving the incorrect records due to homonymy or human error. Another major advantage of such an application is that, if all national hospitals are networked via the Internet and they all have an RF scanner, they can quickly gain access to a patient's records even if they are in another state. For example, take the case of a person from New York that travels to San Diego on business, he has a complex medical history and several allergies. He has a heat stroke and is taken to hospital. On arrival, his arm is scanned and a

RFID tag is activated, the computer automatically searches the national database for the patient's records which are held in New York. The result is that the doctors will not accidentally administer any of the drugs he is allergic to and they will also have a clearer idea of what may be the cause of the stroke as well as positively identifying the patient who may not have any documents on him. If the patient did not have an embedded tag, all of this could have taken a lot longer and could also lead to the death of the patient if an incorrect medicine is administered or if fast action is not taken.

Another use has been found for the subdermal tags. The Mexican government has implanted all its high profile law enforcement personnel that have access to top secret documentation that is stored in a high security bunker and/or that runs the risk of being kidnapped. As is normally the case with RFIDs, each tag has a unique identification code. This code allows the person to gain access to the bunker or, in the case of him being kidnapped, the RFID can be tracked. Wide publicity has been given to this second application so as to deter kidnappings *ex-ante*.

4 RFIDS AND SECURITY AND PRIVACY ISSUES

In the pre-Internet world, data was either kept on paper, on stand-alone computers, or on private computer networks not easily accessible to hackers and intruders. Since the mid 1990s, the widespread use of the Internet has created large amounts of data that is exposed on what is essentially a public network. The dramatic increase in the amount of easily accessible data in our everyday lives brings with it a set of new security and privacy concerns. For example, part of the Internet's popularity centres on electronic commerce, or e-commerce. The Internet offers a convenient way to shop and perform a variety of financial transactions. However, this also means that consumers could reveal confidential or private data, such as detailed identity and financial information over a conceivably insecure medium to potentially untrustworthy parties. A common example of this kind of disclosure occurs each time someone applies for a loan, mortgage, or just opens a bank account online. To help keep data secure, technology solutions, such as encryption, identity management, firewalls, and intrusion detection, are routinely employed.

In many ways, the issues of security and privacy related to the use of RFID applications mirror those created with the introduction of the Internet. RFID tags are essentially tiny little computers that hold information that can be confidential and personal, and potentially available on a public network. RFID applications identify ordinary objects and access or transmit data about those objects, or the object holders (for example, consumers), by radio frequency through the air around us. If left unprotected, this data becomes exposed to malicious or unauthorized use and distribution. As RFID technology and its applications become ubiquitous, nearly every item imaginable a car tire, a box of cereal, a door handle, or a beloved pet will carry an RFID tag whose data could be compromised. Consumer privacy groups contend that RFID tag data could conceivably be used by commercial or governmental agencies to track and trace people's actions and belongings in ways that might violate individual rights to privacy.

Although individual privacy concerns are more often discussed and debated publicly, business enterprises are also concerned with breaches of security that result in unauthorized access and possible manipulation of private or confidential corporate data. For example, in a supply chain RFID application where RFID tags are used to track inventory of products, a business partner who accesses confidential inventory data or tracks the movement of inventory by accessing the tag data, with or without authorization, compromises certain

corporate data and possibly hampers that corporation's capability to negotiate better prices with its suppliers or customers.

As already mentioned, any data that is stored electronically has to be protected with technological instruments that guarantee a sufficient level of protection in correlation to its sensitivity. Password control and encryption are the most evident tools but not the only ones.

5 CONCLUSIONS

Though many people are sceptical about the use of RFID tags for anything other than supply chain management, if the data stored on them and both the connection to the main server and the latter are correctly protected, there should be little or no risk of data theft. In view of the limited distance that is necessary for the radio frequency to be activated, it is not, in effect, easy for hackers to access any data stored on the tags themselves. The risk remains on the server side.

With regards to the new Euro banknotes, though initially they will be regarded as a threat to people's spending habits, in due course, Europeans will better understand the objective of the Central Bank's drive to curtail terrorism and illegal activities once connected to cash transactions and will thus become less sceptical and realise that "Big Brother" is not watching over them but is simply trying to protect them.

6 REFERENCES

[1] Euro Scheme Makes Money Talk, *Janis Mara, Wired.com, July 2003*

[2] RFID Field Guide: Deploying Radio Frequency Identification Systems, *Bhuptani Manish, Moradpour Shahram, Prentice Hall PTR, 2005*