

Do No Harm: The Use of RFID Tags in a Medical Environment

Christopher Bolan

School of Computer and Information Science
Edith Cowan University
c.bolan@ecu.edu.au

***Abstract** - With the increasing usage of RFID systems and their potential in a range of common applications especially medical related fields, it is important to investigate the weaknesses of the technology and the potential risks that accompany them. The discussion outlines possible attacks against confidentiality, integrity and availability and speculates how such attacks would effect medical installations.*

Keywords: RFID, Tags,.

1. Introduction

Like most modern professions, medicine is faced with the challenge of coping with the rapid increase of information available since the advent of wide spread information technology (IT) usage. The rapid changes in how society accesses and stores data is threatening the basic privacy foundations of the medical profession [1]. The Privacy Rights Organisation [2] agrees that medical information is shared by a wide range of people both in and out of the health care industry. The research carried out by the organisation demonstrates that while, in theory, access to medical data is obtained only after personal consent is given and/or a 'need to know' has been established, in reality, individuals may have no choice but to agree to the sharing of medical data if they wish to obtain care and qualify for insurance.

With the advent of RFID technology a range of new data storage and tracking options are becoming available. While initially seen by some as a replacement for bar-coding systems as the preferred method of auto-identification [3], through the use of RFID technology a range of new possibilities exist. Examples of current usage include:

- Animal Identification Systems [4] – RFID sensors are embedded in animals to allow each animal to be uniquely identified;

- Product Tracking [3] – RFID sensors where attached to individual items to allow real time product monitoring;
- Long range access control of Vehicle systems [5];
- Prisoner tracking systems in gaols [6] – Prisoners in the Ross correctional facility in Ohio will be required to wear wristwatch size RFID tags to allow movement tracking.

In addition to the implanting of Animals with RFID chips several plans for the use of RFID technology in human subjects have been trialled [7]. The implanting of RFID chips has several uses in areas such as, preventing identity fraud, people based building access systems, and the storage of medical data. Currently the Baja Beach Resort in Spain uses an implanted RFID chip as a way for their clientele to purchase resort services without having to carry cash or other forms of verification [8][9].

For the present RFID systems remain too expensive to completely penetrate all possible markets, with typical transponders costing around US\$0.50 – US\$1.00 [3]. This cost is more easily absorbed in the medical industry though, with mass production coupled with an open standard, supporters aim to bring the price down to around US\$0.05 – US\$0.10. As public awareness and acceptance of RFID increases with projects such as the United States of America mandating the use of e-passports which use RFID technology to store biometric and identification information, experts are predicting other forms of government mandated RFID identification technology [10]. With RFID technology poised to become an integral part of medical information technology infrastructure, it is important that the security implications of such usage be investigated and discussed.

2. RFID Basics

RFID tags now come in various shapes and sizes including stick on labels, tie-on tags, 3mm pellets, and button disks. Internally, they consist of a microcontroller and attached antenna embedded in a protective material. Every RFID system consists of three major components [3] (figure 1):

- “the RFID tag, or transponder, which is located on the object to be identified and is the data carrier in the RFID system,”
- “the RFID reader, or transceiver, which may be able to both read data from and write data to a transponder,” and
- “the data processing subsystem which utilizes the data obtained from the transceiver in some useful manner”.

The RFID transceiver emits a radio frequency carrier signal. When the transceiver is placed within range of a transponder, the antenna of the transponder detects the electromagnetic field. The transponder’s microcircuit then activates, causing the antenna to fluctuate in a coded sequence in such a way to transmit its encoded data. This transmission is then read by the transceiver and utilised by a data processing subsystem.

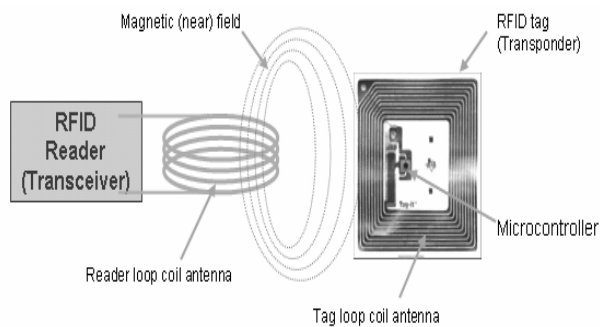


Figure 1. Loop Antenna RFID Tag System (Adapted from [11])

RFID tags or transponders may be either passive or active. Passive tags have no on tag power and thus use the electromagnetic energy transmitted by the transceiver to power the microcontroller through inductive coupling or far field energy harvesting [3]. Inductive coupling uses the magnetic field of the communication signal to induce a current in the coiled antenna which charges an on-tag capacitor providing an operating voltage, and power [3]. This means that inductive coupling is only feasible using the near-field communication signal.

Alternatively, far field harvesting uses the energy from the interrogation signal’s far field signal to

power the tag [3]. The signal works upon the end terminals of the tag antenna inducing voltage which is used to charge a capacitor that in turn supplies an operating voltage. Due to their reliance on transmitted power, passive RFID tags have only small transmission areas ranging from a few centimetres to around fifteen meters for UHF tags. Active tags have an additional power cell used to provide power to the RFID microcontroller. The inclusion of a power source provides active tags with several advantages over their passive counterparts such as the ability to receive lower power signals or to output stronger signals than would otherwise be possible. The higher signal strength means that active tags are able to transmit over greater distances up to around 100 meters. With the added benefits that the active tags bring, also comes a shelf life. Modern tag battery life varies from one to ten years according to usage and data transfer settings. Also, while only slightly larger in size than their passive equivalents, active tags are considerably more expensive ranging from twenty to three hundred dollars per tag [11]. While higher frequencies allow for greater bandwidth and thus greater data transfer rates, they also become more susceptible to interference from external materials such as water or metal. A summary of the uses of the major RFID frequency bands is given in figure 2.

Band	Frequencies	Range (Passive)	Range (Active)	Data Rate	Absorption Resistance
Low Frequency	125 KHz 134 KHz	0.5 m	N.A	Low	Very Good
High Frequency	13.56 MHz	1 m	N.A	Fair	Fair
Ultra High Frequency	433 MHz 860 MHz 930 MHz	20m	1 Km	Good	Affected
Microwave	2.45 GHz 5.8 GHz	1m	300 m	Very Good	Very Poor Fair

Figure 2. Radio Frequency Properties

3. Medical Environment RFID Security

Historically, there has always been a need for security stemming from the basic principle of protecting assets, physical or otherwise, from others. Traditionally, medical security has focused on the protection of data from unauthorised disclosure, ensuring the integrity of the data and maintaining the availability of data. In computer security circles these principles are known as Confidentiality, Integrity and Availability (CIA), which equally apply in the medical arena [12]. Through the use of these principles, the likely problems with the usage of RFID systems in medical environments will be discussed.

3.1. Confidentiality

The underlying ideal of confidentiality is to prevent unauthorised access to data from both internal and external sources. Confidentiality is usually supported through the encryption of data (eg. PGP) and access protection systems (eg. Passwords, Biometrics etc). Confidentiality is considered to be breached when unauthorised individuals or systems may view information that otherwise would be hidden from them.

The idea of confidentiality is closely tied to the legal issue of privacy, which is seen by many as a vital topic in the e-medicine arena [13]. While the principle does apply evenly to all hidden information in a system, the characteristic value of confidentiality increases with the sensitivity of the confidential data. Confidentiality may also cover the aggregation of non-confidential data. For example: patient information may be gathered in small fragments which of themselves are not consider confidential, however the aggregation of such fragments may reveal confidential information.

The amount of data that may be stored on a RFID tag varies with the tag type; regardless of the storage capacity the basic principle of operation is for an RFID tag to broadcast upon request. While the broadcast data transmission may be encrypted, the lack of computational power on most, if not all RFID tags, means that an attacker using a laptop or PC would have greater computational power and thus any encryption would likely be overcome [14]. Even if a tag were constructed with sufficient computational power to allow for a strong level of encryption this would invariably result in a significant increase in tag cost and thus undermine one of the main benefits of current RFID technology.

Confidentiality based attacks on RFID systems are focussed on capturing any transceiver/transponder communication and decoding any encryption, as well as reading any available tags. In a medical environment, such data could reveal to an attacker the location of an item that could be of value, or private patient records. Such attacks could be carried out in one of two ways. Firstly the attacker could use their own transceiver in order to interrogate an RFID tag as shown in figure 3. Such an attack may be detectable if the transceiver is set up in such a way that it logs interactions. This sort of facility is unlikely due to the resource constraints of RFID tags.

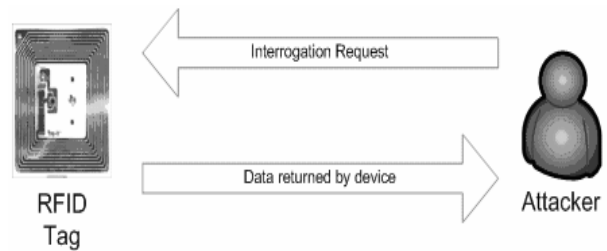


Figure 3. Direct Confidentiality Attack

The second and perhaps more worrying type of confidentiality attack is a passive listening attack on authorised transceiver/transponder communications. In this type of attack the attacker simply monitors and records all transmissions that can later be decoded for analysis and other malicious purposes. Such an attack would be difficult to detect as the attacker is not required to actively probe or interact with the system. This attack is illustrated in figure 4.

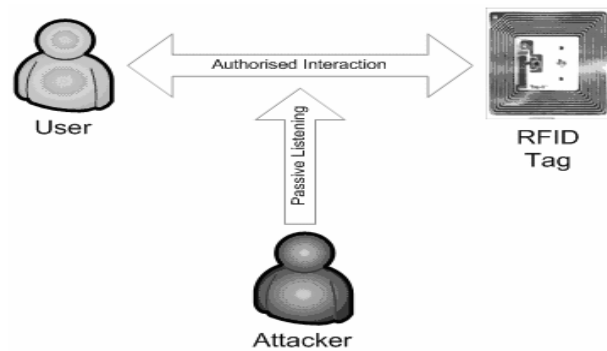


Figure 4. Indirect (Passive) Confidentiality Attack

3.2. Integrity

The second principle, integrity, encompasses the quality of information which must be whole, complete and uncorrupted. Any activity or event that exposes information to corruption, deletion or unauthorised modification is a threat to integrity. Thus integrity defenses cover not only access controls but also checks to ensure information is valid such as file hashing. Unlike confidentiality, integrity may be violated by non human impetus such as data corruption caused by transmission medium or signal degradation.

If a system housing medical data is unavailable for any reason, the data contained in that system is unusable and thus loses value. Should this unavailability occur at a critical juncture, the outcome may foreseeably lead to an incorrect decision or course of action resulting in direct harm to a patient. The literature [15] notes, it is therefore prudent to

investigate ways to guarantee integrity for certain records and to actively prevent likely attacks.

Often, the major threats to integrity and availability are not immediately obvious, for example software bugs and/or hardware failures may occasionally corrupt messages. It is foreseeable that a small error or software bug could alter the numbers on a RFID tag without changing it so grossly that it would be rejected. Even if this only occurred in 1 in 10,000 cases to a GP it would mean a mistake every few years and at least one dangerous error in a career [15].

Another threat arises from a lack of a standard data format for electronic communications. Markwell [16] outlines such a case using an example of a lab technician emailing results to a doctor whose electronic system misinterprets the data due to formatting problems leading the doctor to take an incorrect course of action. This issue is being mitigated through the proposal of common data interchange formats throughout the literature [16][17]. Thus, any integrity breach has the potential of invalidating any benefit of that system.

With RFID systems there are two places where the integrity may be vulnerable to attack: the data stored on an RFID tag may be able to be altered or corrupted (figure 5) and the transmission signal of either transceiver or transponder may be duplicated or corrupted from either an attacker (figure 6) or an accidental transmission (figure 7) causing further integrity problems.

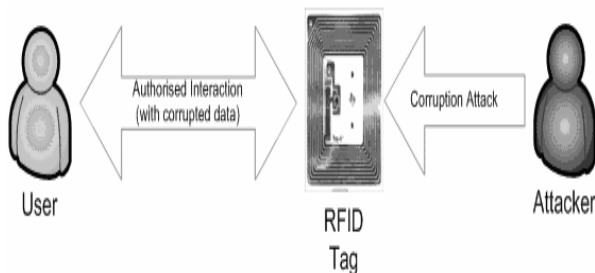


Figure 5. Tag Directed Integrity Attack

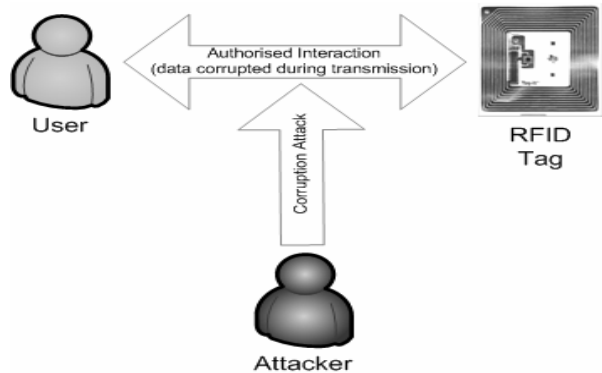


Figure 6. Attacker Based Transmission Integrity Attack

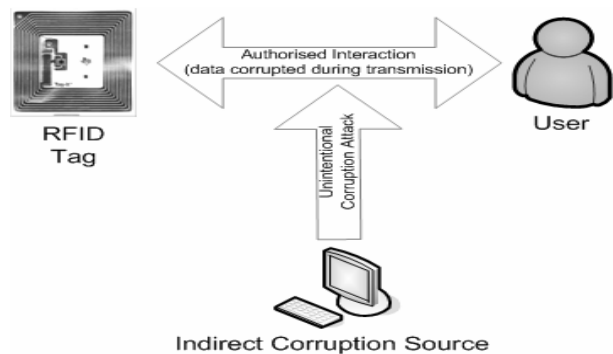


Figure 7. Indirect Transmission Integrity Attack

3.3. Availability

The remaining principle availability is concerned with the ability of an authorised user to be able to access system information and data without impediment and in a usable format. Threats to availability come from denying an authorised user access to the system or to data when requested, or interrupting the supply of data through corruption. Like the integrity principle, to availability do not need to be through malicious acts and may be a by-product of poor system design or external factors such as cross band interference [17].

With RFID systems, availability refers to the ability for transponder-transceiver communication to take place. Possible threats to RFID availability come from interference of the transmission signal from either a malicious attacker or the environs within which the system is operating (figure 8).

RFID tags by their very nature are designed to be located remotely from the reader; this means that any tag not detected by the reader is not necessarily an

availability issue as the tag may be assumed to be out of range. As such RFID availability attacks are particularly effective, and assisted by some of the base protocols of the technology such as KILL commands and Tree Walking. The KILL command is a code that may be transmitted to an RFID tag which instructs the tag to wipe its data and cease operation. The command was created to allow legitimate users to 'destroy' tags that were no longer required, but as an RFID tag has no real way of confirming who sent the KILL command an attacker could easily 'destroy' tags to affect availability.

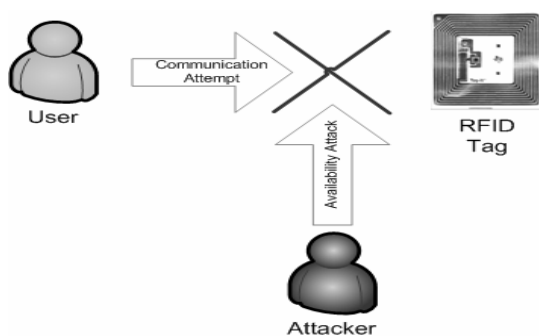


Figure 8. Availability Attack

Similarly the Tree Walking algorithm used to circumvent tag collision problems also opens avenues for availability attacks. The algorithm works on the basis that tags in a RFID system store a unique fixed length identifier. The algorithm searches detected tags using a form of binary tree. If a collision occurs, the algorithm follows the responsive sub-tree and the leaf nodes at the bottom of the unresponsive sub-tree are ignored from then on. Eventually the algorithm will reach an active leaf node at which time it will mark the leaf node as responsive (i.e. a unique tag in detectable range) and then recurse to the last collision point and follow the untraversed path in a similar fashion. At the completion of the algorithm, the reader has a list of the identification numbers of all tags within range and may then address each in turn. Thus if an attacker were to impersonate a tag response to every request, the RFID reader would be flooded and could perhaps stall or crash.

4. Conclusion

While the attacks outlined in this paper are by no means exhaustive, from this discussion it is clear that any proposed implementation of an RFID system in a medical environment is faced with a significant challenge. The consequences of placing data on an RFID tag that is critical to patient care could be

catastrophic. Such systems would be ripe targets for potential attackers who may be able to infiltrate the systems at will. Thus any proposed use of RFID technology in a medical environment should undergo heavy scrutiny before any implementation is undertaken.

5. References

- [1] D. C. Slawson and A. F. Shaughnessy, "Becoming an Information Master: Using POEMs to Change Practice with Confidence," *The Journal of Family Practice*, vol. 49, pp. 63-67, 2000.
- [2] Privacy Rights Organisation, "How Private is My Medical Information," 2004.
- [3] S. E. Sarma, S. A. Weis, and D. W. Engels, "RFID Systems and Security and Privacy Implications," in *Workshop on Cryptographic Hardware and Embedded Systems*, vol. 2523, *Lecture Notes in Computer Science*, 2002, pp. 454-470.
- [4] M. Neary and A. Yager, "Methods of Livestock Identification," Perdue University, West Lafayette AS-556-W, 2002.
- [5] On Star, "Experience On Star in Action," 2005.
- [6] J. Best, "44,000 Inmates to be RFID-Chipped," *Silicon.com*, 2004.
- [7] M. Kanellos, "Human Chips - More than skin deep," 2004.
- [8] V. Jones, "Baja Beach Club in Barcelona, Spain Launches Microchip Implantation for VIP Members," 2004.
- [9] "Baja Beach Club," 2005.
- [10] A. Juels, D. Molnar, and D. Wagner, "Security and Privacy Issues in E-passports," in *Proc. Conference on Security and Privacy for Emerging Areas in Communication Networks - SecureComm*, Athens, Greece, 2005.
- [11] K. Wild, "3D Asset Location for Mobile Devices Using Passive RFID Tags", 2005, unpublished.
- [12] P. A. H. Williams, "The underestimation of threats to patient data in clinical practice", in *Proc. 3rd Australian Information Security Management Conference*, Perth, Western Australia, 2005.
- [13] C. Bolan, "Need to Know: Security or Liability?," in *Proc. 2nd Australian Information Security Management Conference*, Perth, WA, 2004.
- [14] C. Bolan, "Radio Frequency Identification - A Review of Low Cost Tag Security Proposals", in *Proc. 3rd Australian Computer, Network & Information Forensics Conference*, Perth, Western Australia, 2005.
- [15] R. J. Anderson, "Security in Clinical Information Systems," 1996.
- [16] D. Markwell, "Fear of Flowing," in *Proc. Annual Conference of The Primary Health Care Specialist Group of the British Computer Society*, Cambridge, 1995.
- [17] R. Risley, D. Masys, C. Mathews, M. H. Ellismen, and H. Simon, "Medical Records on the Internet - Can Security and Privacy Be Assured," 1996.
- [18] C. Bolan, "Strategies for the Blocking of RFID Tags", to be presented at Sixth International Network Conference, Plymouth, UK, 2006.