2008

RFID Communications - Who is listening?

Christopher Bolan
Edith Cowan University

RFID Communications - Who is listening?

Christopher Bolan
School of Computer and Information Science
Edith Cowan University

Abstract

Radio Frequency Identification (RFID) is seeing a surge in awareness across a range of industries as a successor to barcoding. The nature of this technology promises a wide range of benefits but it appears to be at the expense of security. This paper investigates an eavesdropping attack against an EPC RFID system and shows how a simple device may be used to record interactions between both Tag and Readers. The device is used to record and decode signals within range and its output is analysed to verify that the attack was indeed successful. The findings verify previous assertions by other authors that such attacks are viable and acts as a warning to implementers of the standard who expected their transactions to remain private or secure.

Keywords

Radio Frequency Identification, RFID, Eavesdropping

INTRODUCTION

As a normal part of their wireless operation RFID systems require no direct physical contact between tag and reader and are thus theorized to be highly susceptible to Eavesdropping attacks (Hancke, 2008). Whilst there has been some experimentation attacks of this nature against RFID systems, to date much of the focus has been on securing the transmission with cryptography (Rashinge, Engels & Cole, 2004; Knopse & Pohl, 2004). Beyond this, previous literature has usually stated that such an attack is possible without detailing experimental proofs or methods (Sarma *et al.*, 2002; Juels, 2006). Thus, it seems more than appropriate to review the current standards such as the Electronic Product Code Standard (EPC) to demonstrate why and how such an attack would be viable (Auto-ID Center, 2002). This paper will thus demonstrate a successful eavesdropping attack on a Generation One EPC Compliant system, detailing how the attack was conceived and ultimately carried out using a low cost custom device.

Background

Historically, there has always been a need for security stemming from the basic principle of protecting assets, physical or otherwise, from others. Computer security has tradionally been 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). 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 the hottest topic in modern computer related security (Whitman & Mattord, 2003). 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: information may be gathered in small fragments which of themselves are not consider confidential, however the aggregation of such fragments may reveal confidential information.

RFID Eavesdropping

Radio frequency identification (RFID) technology stems back to Faradays' discovery that light and radio waves were both forms of electromagnetic energy. However, the first concrete step towards the modern conception of RFIDs was made by Harry Stockman in his 1948 paper *Communication by means of reflected power* (Stockman, 1948). From that discovery, it was not until 1973 the first direct patent on passive RFID tags was lodged in America by ComServ (Cardullo, 2005). RFID tags now come in various shapes and sizes including stick on labels, tie-on tags, 3mm pellets, and button disks although internally, they consist of a microcontroller and attached antenna embedded in a protective material.

Beyond just tags themselves, every RFID system consists of three major components (Sarma, Weis & Engels, 2002, p.3):

- "*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 amount of data which may be stored on a RFID tag varies with the tag type; but irregardless 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 (Bolan, 2005). 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.

Given these basics, confidentiality based attacks on RFID systems would likely be focussed on capturing any transceiver/transponder communication; and decoding any encryption used, as well as reading any available tags. For example, in a medical environment, such data might reveal to an attacker the location of an item that could be of value, or private patient records (Bolan, 2006). Such attacks may be carried out in one of two ways. Firstly the attacker could use their own transceiver in order to interrogate an RFID tag. Although, such attacks may be detectable if the transceiver is set up in such a way that it logs interactions which may prove unlikely due to the resource constraints of RFID tags.The second and perhaps more worrying type of confidentiality attack is a passive listening attack on authorised transceiver/transponder communications, referred to as spying (Oertel *et al.*, 2004). In this type of attack the attacker simply monitors and records all transmissions which later may be used for malicious purposes. Such an attack would be difficult to detect as the attacker is not required to actively probe or interact with the system (see figure one below). It should also be noted that attacks of this type are often used as the starting step for other more advanced methods (Whitman & Mattord, 2003).

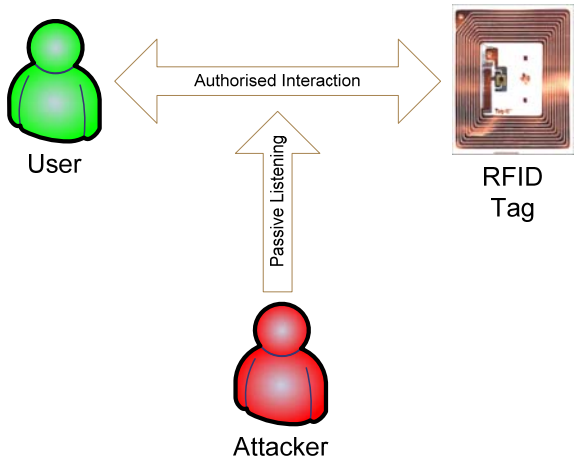

Figure 1 – RFID Eavesdropping Scenario

METHOD

Recalling figure one, for an attack of this nature to transpire usually requires an interception of the communication between two or more elements of a system. As such attacks are most effective when the attacking device is passive the attacker ideally does not supply the communication carrier wave and thus is theoretically able to eavesdrop at a greater distance than the communicating devices would normally allow. This does not remove the distance limitation of the RFID carrier signal but does improve the effectiveness of an attack whilst still requiring the attack to occur during the relatively short communication window.

The interception of a RFID systems communication is not the only measure of a successful eavesdropping attack with the translation of the captured signal to usable information becoming an integral measure of success. Due to the nature of RFID communications and the limiting factor of range, the distance between attacker, reader and tag mean that there are three versions of eavesdropping that must be considered. To allow further discussion of the distances and separate scenarios in this section I will define the following :

- Distance (R) – The distance which the transmission of the Reader may be detected
- Distance (T) – The distance which the transmission of the Tag may be detected
- Signal (R) – The signal produced by the Reader
- Signal (T) – The signal produced by the Tag

The scenarios involving RFID eavesdropping may be described as:

- A detection attack – whereby an attacker may detect a transmission but be unable to reliably translate the transmission signal into usable data.
- A transmission only attack – whereby due to the differential in transmission range between a reader and a tag the eavesdropper is only able to detect and translate the readers signal
- A complete attack – whereby the eavesdropper is able to record and translate both the reader and tag communication.

Obviously the ideal demonstration of an eavesdropping attack on an RFID system would be a complete attack occurring when both Signal (R) and Signal (T) are detected which may only occur when the eavesdropper is in a range inside both Distance (R) and Distance (T) (Juels, 2006). As the success of such an attack combines the elements required in both a transmission only and a detection attack it is this scenario that my experiment was designed to demonstrate. The first stage in this experiment was to first ensure that a signal was available for interception and that this signal was known and replicable to ensure that the conditions for success in the experiment might be explicitly defined. To this end a basic RFID system consisting of an RFID reader and single EPC tag was setup within a controlled environment as detailed in the figure below.

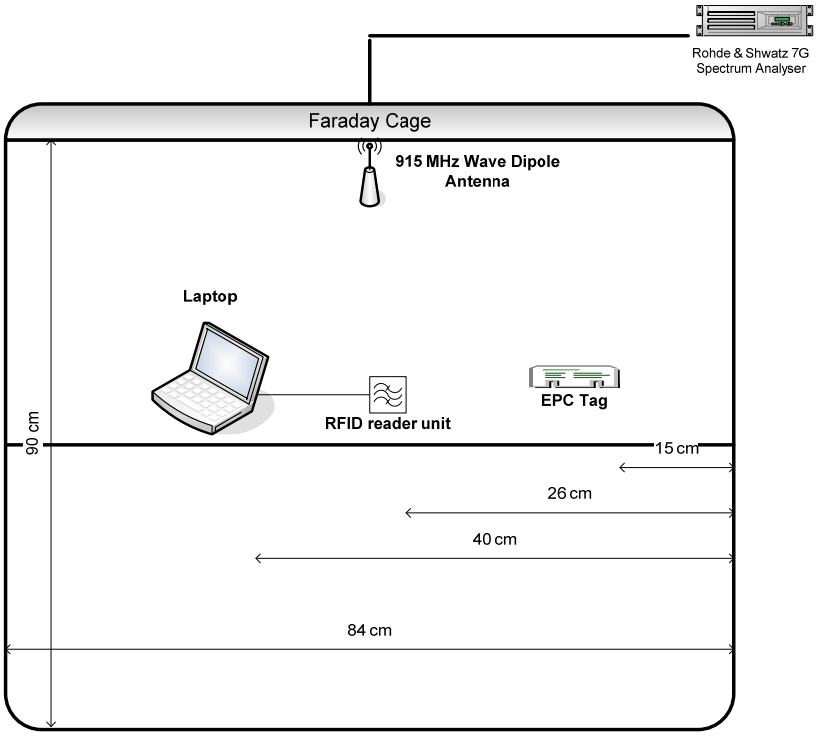

Figure 2 – Eavesdropping Baseline Experimental Setup

To ensure the correctness of the setup two separate measures were taken:

- A capture of the RFID Signal was undertaken via the Spectrum Analyser
- The RFID Reader was setup to log the communication between itself and the EPC tag to a CSV file.

RESULTS

This setup was tested on three separate occasions to ensure identical result and one of which is detailed in the next few figures. Figure three below is a screen capture of the cumulative wave of the RFID communication over the baseline test period showing that the RFID reader was indeed transmitting over the correct spectrum with the graph centred on the 915Mhz frequency.

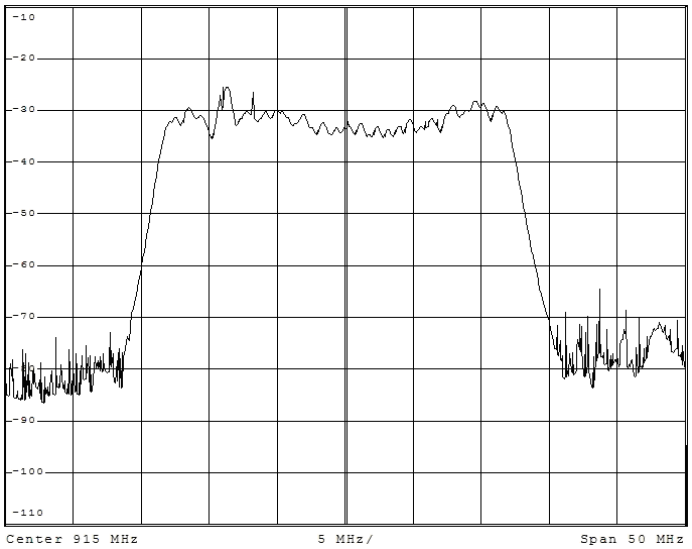

Figure 3 – Cumulative Waveform

Figure four is a snapshot of the spectrum analyser demonstrating the tags response by the second smaller peak on the right of the figure below.

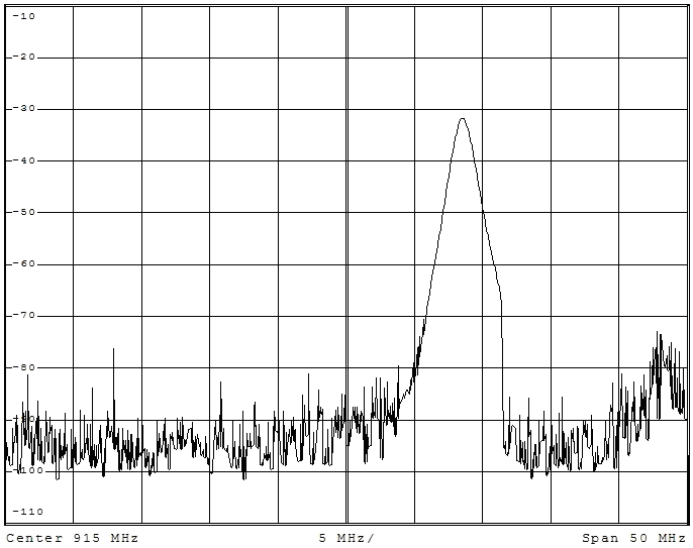

Figure 4 – Individual Snapshot during communication

And finally table one details the inventory of the RFID reader which was recovered from the CSV log on the laptop. The table below illustrates the output from this logfile and demonstrates that the test tag selected for the eavedropping and baseline tests was successfully detected in each test.

Table 1 – Inventory Log from Baseline Test

Time	Tag ID
27/07/2008 12:02:09PM	00 27 32 20 00 00 00 00 00 02 00 02
27/07/2008 12:05:14PM	00 27 32 20 00 00 00 00 00 02 00 02
27/07/2008 12:06:01PM	00 27 32 20 00 00 00 00 00 02 00 02
27/07/2008 12:06:57PM	00 27 32 20 00 00 00 00 00 02 00 02
27/07/2008 12:08:10PM	00 27 32 20 00 00 00 00 00 02 00 02
27/07/2008 12:09:29PM	00 27 32 20 00 00 00 00 00 02 00 02
27/07/2008 12:12:32PM	00 27 32 20 00 00 00 00 00 02 00 02

Now that the baseline test was conducted and the reference data was set, the development of an device able to eavesdrop could occur with the assistance of the SCIS Reasearch Support Engineers. The developed device used a 915Mhz dipole antenna to read the signal and transport it to the microcontroller as seen in the figure five.

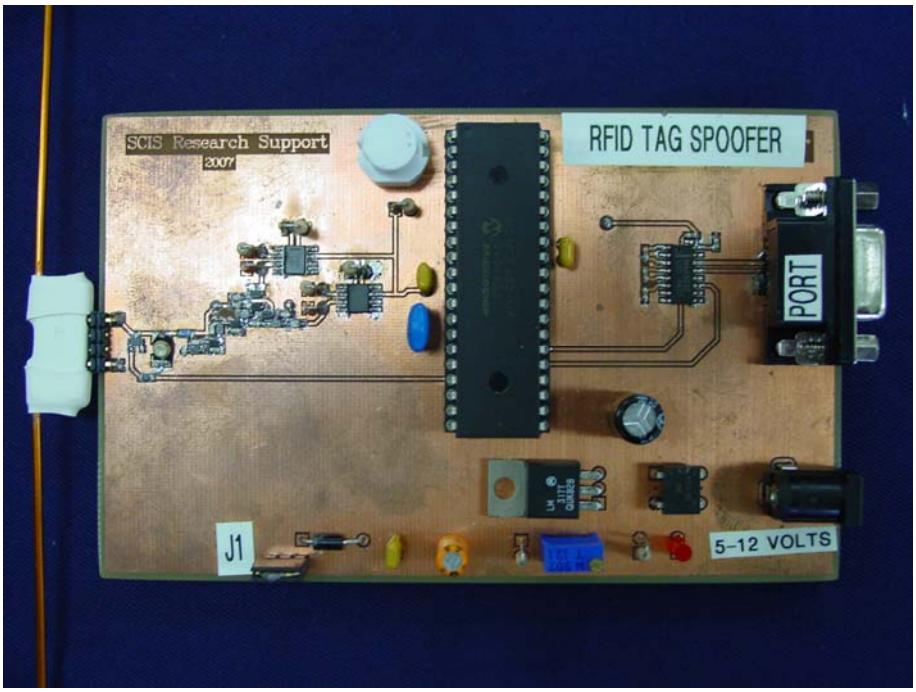

Figure 5 - The RFID Eavesdropping Device

The device above was the programmed via the COM port interface with an algortithm which setup the device and translated the signals received into a binary output following the encoding standard used on the EPC complaint tags (Auto-ID, 2002). This output was then passed out via the COM port interface and logged onto a connected laptop for storage and later analysis an example of this output is shown in figure six below.

```
Starting Program....
Waiting for input....
Input Detected... Initiating Read
0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0
0 1 1 0 1 0 0 0 0 0 0 0 0 0 0 0 1 1 1 0 0 0 0 0 0 1 0 1 1 1 0 1 0 0 0 0 0 0 0
0 1 1 1 1 1 1 1 1 0 1 0 0 1 1 1 0 1 1 1 1 1 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 1 0 1 0
0 0 0 0 0 0 0 0 0 0 1 1 1 0 0 0 0 0 0 1 0 1 1 1 0 1 0 0 0 0 0 0 0 0 1 1 1 1 1
1 1 1 0 1 0 0 1 1 1 0 1 1 1 1 1 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
FINISH
```

Figure 6 – Sample output from eavesdropping device

DISCUSSION

Given the output the next stage was to look for certain patterns to identify the communication stream between the RFID Reader and Tag. The obvious start point for this search was the ScrollAllID (00110100) command as this string is used by EPC Standard compliant readers to ask all EPC Tags within range to respond with a standard identification string (Auto-ID Center, 2002). Using this command string as a reference point the entire Reader command string was then broken down as detailed in the subsequent table and then this was matched against the output again and matches have been highlighted in Table 2 and Figure 7.

Table 2 – Expected results for RFID Reader Inventory String

Field	Number of Bits	Description	Expected Value	Colour Code
PREAMBL	?	Period of no RF Transmission		
CLKSYNC	20	clock synchronization	00000000000000000000	
SOF	1	Start of Frame indicator	1	
CMD	8	Command sent to tag	0 0 1 1 0 1 0 0	
Odd Parity (CMD)	1	Odd Parity of previous field	0	
PTR	8	Pointer to a location	0 0 0 0 0 0 0 0	
Odd Parity (PTR)	1	Odd Parity of previous field	1	
LEN	8	Length of data in VALUE field	1 1 0 0 0 0 0 0	
Odd Parity (LEN)	1	Odd Parity of previous field	1	
VALUE	variable	VALUE	0 1 1	
Odd Parity (VALUE)	1	Odd Parity of previous field	1	
Odd Parity	1	Odd Parity of previous odd parity bits	0	
EOF	1	End of Frame indicator	1	

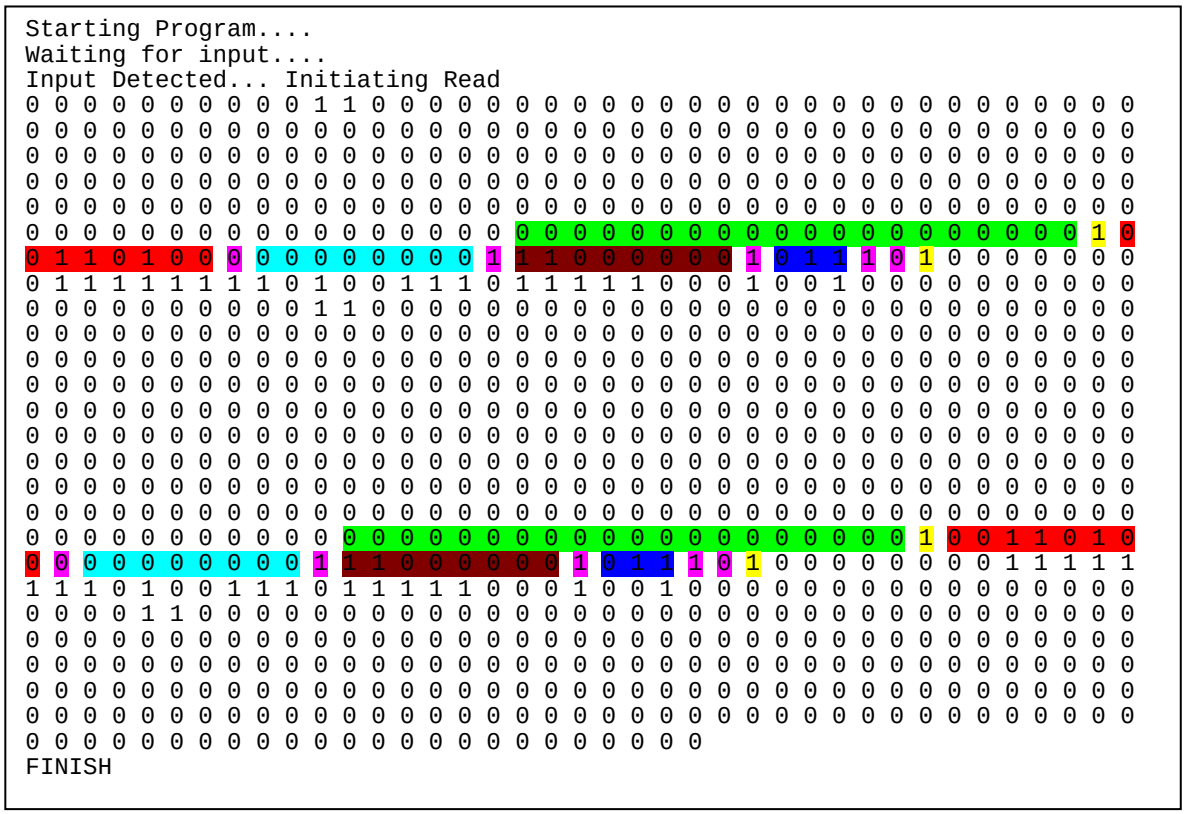

Figure 7 – Eavesdropping output mapped against RFID ReaderInventory String

After the Reader transmission had been successfully identified the next step was to repeat the process to identify the Tag response. The expected response is detailed in table 3 below and is followed by figure 8 showing the fields mapped onto the attackers output with the reader strings highlighted as a block in grey.

Table 3 – Expected Responser from test tag to Reader Inventory String

Field	Number of Bits	Description	Expected Value (HEX)	Colour Code
PREAMBLE	8			
CRC-CITT (16)	16	CRC-CITT of the Tag ID	9D F1	
TAG ID	Variable	Tag identifier in MSB --> LSB Binary fashion	00 27 32 20 00 00 00 00 00 02 00 02	

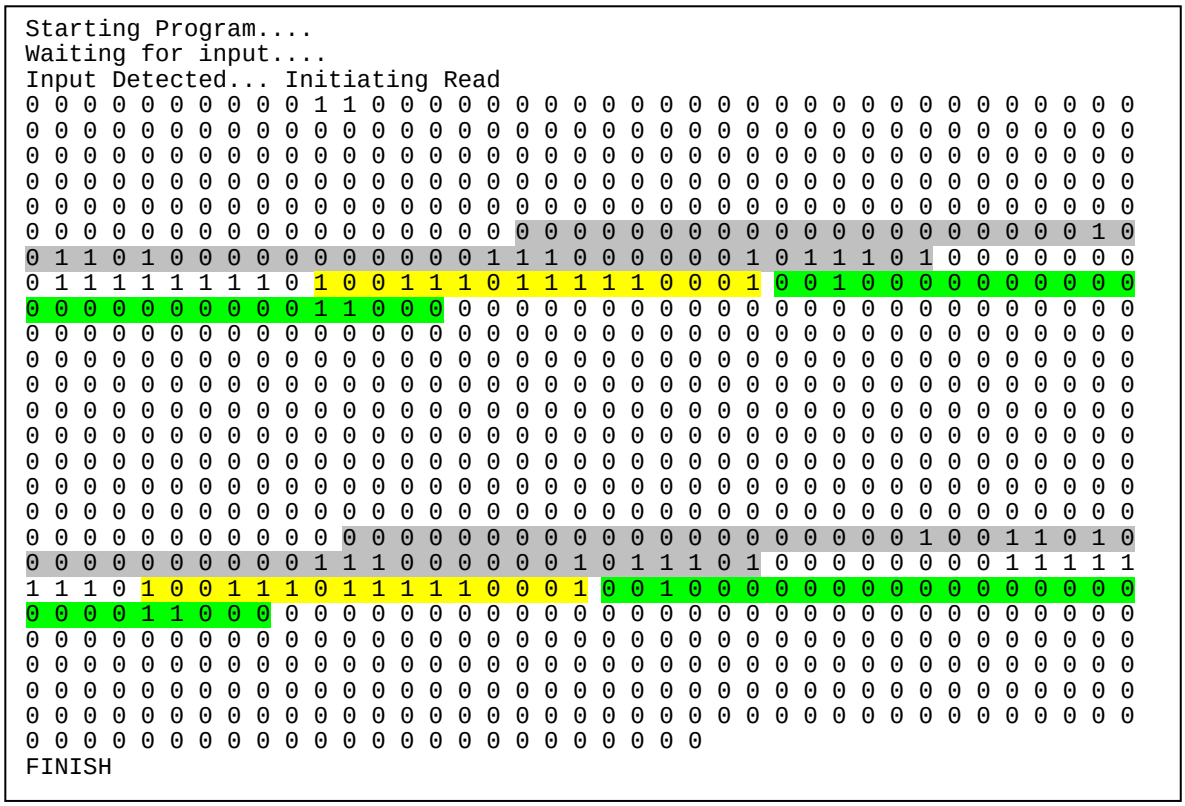

Figure 8 – Eavesdropping output mapped against RFID Tag Response String

From the above sequence it may be seen that a complete eavesdropping attack is viable on EPC Gen One standard based RFID technology. The device constructed to record the signals was created for around $100 Australian Dollars but that cost may be reduced with further design revision, materials and construction methods. The demonstrable ability to eavesdrop on such technologies opens implementations of the standard up to a range of potential threats.

CONCLUSION

This paper has demonstrated a successful eavesdropping attack against a Generation One EPC setup using a custom made device, illustrating the ease in which such an attack may be carried out. The results revealed that EPC Gen One communications are carried out completely in the clear, and may be intercepted by anyone within range of the transmissions. This reinforces earlier assertions by other researchers who have cited such attacks as viable without providing proofs (Sarma *et al.*, 2002; Juels, 2006).

Whilst it has been argued that such an attack would become a more difficult exercise with an appropriate encryption added to the standard it is notable that the second generation of the standard still lacks this feature (EPC Global, 2005). This may be attributable to the difficulty of implementing a secure encryption method that may be implemented on a fast response – computational limited environment such as that offered by passive RFID systems. Such limitiations on processing power mean that new and innovative encryption schemes are required that will allow for secure communication within small operational windows and achieveable with limited resources.

A range of schemes purport to have the solution to this challenge but none has yet to gain acceptance into the EPC standard, a standard which has few if any rivals in its efforts and thus remains a default choice for inventory based systems. Unfortunately, until the standard adopts even a basic encryption algorithm all transmissions conducted with RFID equipment must be considered to be insecure, and thus it is clear that current implementations may well prove easy targets for attacks. It would therefore be suggested that implementers of this standard need to supplement the operation of the standard with their own encryption selection to attempt to avoid such attacks.

REFERENCES

Auto-ID Center. (2002). *860MHz–930MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification*. Cambridge, Massachusetts: Massachusetts Institute of Technology.

Bolan, C. (2005). *Radio Frequency Identification - A Review of Low Cost Tag Security Proposals.* Paper presented at the 3rd Australian Computer, Network & Information Forensics Conference, Perth, Western Australia.

Bolan, C. (2006). *Do No Harm: The Use of RFID Tags in a Medical Environment.* Paper presented at the International Conference on Security & Management, Las Vegas, Nevada.

Cardullo, M. (2005). Genesis of the Versatile RFID Tag. *RFID Journal, 2*(1).

EPCglobal. (2005b). EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960MHz (No. 1.0.9): EPCglobalo. Document Number)

Hancke, G. (2008). *Eavesdropping Attacks on High-Frequency RFID Tokens.* Paper presented at the Conference on RFID Security, Budapest, Hungary.

Juels, A. (2006). RFID Security and Privacy: A Research Survey. *IEEE Journal on Selected Areas in Communications, 24*(2), 381-394.

Knospe, H., & Pohl, H. (2004). RFID Security. *Information Security, 9*(4), 39-50.

Oertel, B., Wolk, M., Hilty, L., Kohler, A., Kelter, H., Ullmann, M., et al. (2004). *Security Aspects and Prospective Applications of RFID Systems*. Retrieved 08/01/2006. from www.bsi.de/fachthem/rfid/RIKCHA_englisch.pdf.

Ranasinghe, D., Engels, D., & Cole, P. (2004). Low-Cost RFID Systems: Confronting Security and Privacy. In *Auto-ID Labs Research Workshop*. Zurich, Switzerland.

Sarma, S. E., Weis, S. A., & Engels, D. W. (2002). RFID Systems and Security and Privacy Implications. In *Workshop on Cryptographic Hardware and Embedded Systems* (Vol. 2523, pp. 454-470).

Stockman, H. (1948). Communication by Means of Reflected Power. *Proceedings of the IRE*, 1196-1204.

Whitman, M. E., & Mattord, H. J. (2003). *Principles of Information Security*. Canada: Thomson.

COPYRIGHT