2011

A proposal for utilising active jamming for the defence of RFID systems against attack

Christopher Bolan
Edith Cowan University

DOI: 10.4225/75/57b52c81cd8b7
Originally published in the Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

A PROPOSAL FOR UTILISING ACTIVE JAMMING FOR THE DEFENCE OF RFID SYSTEMS AGAINST ATTACK

Christopher Bolan
secau Security Research Centre, School of Computer and Security Science
Edith Cowan University, Perth, Western Australia
c.bolan@ecu.edu.au

Abstract

With a range of documented attacks against RFID systems a majority of the current literature is focused on the encryption of the communication. This paper addresses such attacks by proposing alternative means of protection through utilising some of the same methods that may be used to attack these systems. The proposed methods would allow for increased security within a range of RFID applications whilst still allowing for normal operations compliant with the relevant standards.

Keywords
Radio Frequency Identification, RFID, Active Jamming, Attack, Wireless Security

INTRODUCTION

Radio Frequency Identification (RFID) relies on transponders which are incorporated into an object for the purpose of identification or tracking (Engels, 2004). The transponder (or tag) may be used to store information and will respond to signals sent by a transceiver (RFID reader). Increasingly such technology is being incorporated into supply chain management systems throughout the world and is expected to eventually replace traditional bar-coding systems (Ahson & Ilyas, 2008). A barrier to the uptake of RFID systems was the lack of interoperability between manufacturers, which has been addressed by the creation and dissemination of the Electronic Product Code (EPC) standard (Bolan, 2007c). The EPC standard governs the whole scope of an RFID system including the operation of compliant ts and readers (EPCglobal, 2005).

A range of work has been published on how the standard is vulnerable to a range of attacks and how through the utilisation of such attacks an attacker would be able to shutdown an EPC RFID system completely with a very low cost device (Ahson & Ilyas, 2008; Bolan, 2006; Bolan, 2007b). Some of the less permanent denial of service attacks would still prove effective as no countermeasures exist within the standard to mitigate their effects (Bolan, 2007c). Given these issues this work looks at such attacks to detail how the weakness and techniques that exploit these issues might be used to develop countermeasures or mitigate such attacks.

THE THREAT OF ATTACK

The discarding of used RFID tags in passive based EPC Class One RFID systems may be seen as a normal part of a tags lifecycle (Hunt, Puglia & Puglia, 2007). Given this feature the standard suggests that discarded tags may be issued a KILL command to 'destroy' EPC complaint RFID tags which according to the standard (EPCglobal, 2005, p.40) is irreversible.

It was found in Bolan (2006) that to a standard complaint RFID reader that killed tags appeared non-responsive and acted in accordance with the standard (EPCglobal, 2005). The actual 'KILL' instruction consists of eight bits (11000100) and is standard to all compliant tags, however the instruction is actually part of an overall command illustrated in figure 1.

	Command	Password	RFU	RN	CRC-16
# of bits	8	16	3	16	16
description	11000100	(½ kill password) ⊗ RN16	000_2	handle	

Figure 1. The EPC 'KILL' Command (EPCglobal, 2005, p.59)

The ‘KILL’ operation takes place as follows:

1. The Interrogator issues a Request Random Number (Req_RN) command
2. The Tag responds with a 16bit random number (RN) verified with a 16bit Cyclic Redundancy Check (CRC-16)
3. Using the acquired random number the Interrogator issues the KILL command using the Command (11000100), the most significant bits (bit range 31-16) EXOR the tag supplied random number, the Tags handle and a CRC-16
4. The Tag accepts the command and responds with its handle and a CRC-16
5. The Interrogator issues a second Request Random Number (Req_RN) command
6. The Tag supplies a new 16bit random number (RN) verified with a CRC-16
7. Using the acquired random number the Interrogator issues a second KILL command using the Command (11000100), the least significant bits (bit range 15-1) EXOR the tag supplied random number, the Tags handle and a CRC-16
8. If all steps were followed correctly the Tag responds with the KILL SUCCESS response after which it will “render itself silent and shall not respond to an Interrogator thereafter” (EPCglobal, 2005, p.58)

The major risk of such functionality is that an attacker could use the feature to ‘kill’ or wipe all tags in a business. Such an attack would only require knowledge of the ‘self-destruct’ code and a suitable transceiver within range of the transponder that is to be deactivated. While such an attack was noted in the original design of the command in RFID systems, Sarma et al. (2002) suggested that a pervasive network of readers might be used to detect unauthorised ‘self-destruct’ commands. However, they fail to explain if such a system would then allow the blocking of the command or if the network would simply detect the command and let the tags be ‘self-destructed’. Whilst evidence of this type of attack against live systems have yet to be documented this may be due to the lack of wide scale adoption or a reticence to report such a loss.

Another documented attack of concern emanates from eavesdropping on RFID communications. Eavesdropping may be seen as a passive listening attack on authorised transceiver/transponder communications, which in some literature is referred to as spying (Oertel et al., 2004). 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 (figure 2).

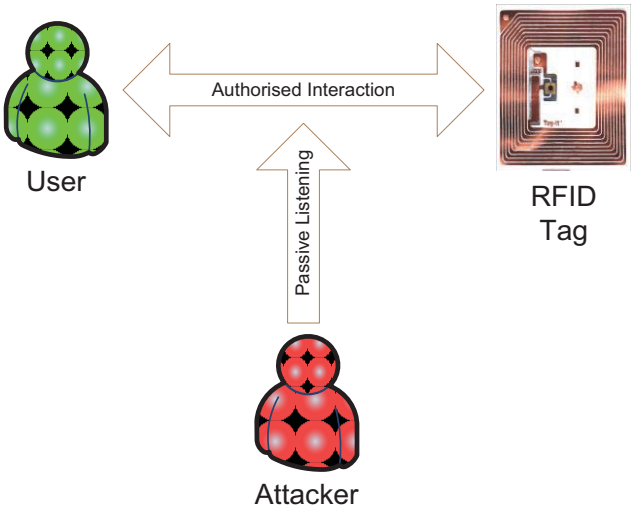

Figure 2. Annotated findings from an Active Jamming Attack

Bolan (2008a) 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.

A third possibility for attack arises from the possibility of tag spoofing. In computing the term 'spoofing', historically referred to the creation of TCP/IP packets using another's IP address thereby gaining some advantage (Basta & Hatton, 2008). A classic example of such an attack is given in the field of cryptography in the form of a man in the middle attack where an attacker uses spoofing to fool both parties in a communication that he is the other party. Thus the attacker receives all communications without the need for cryptanalytic activities. This type of attack is detailed in the figure below.

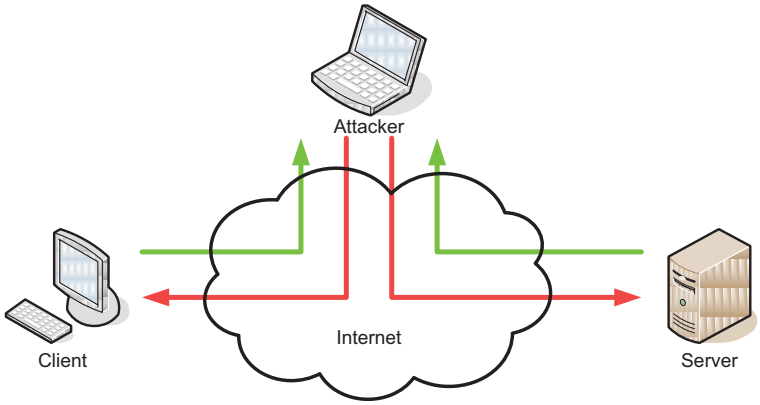

Figure 3. Man in the middle attack

An attack of this nature was shown Bolan (2009) demonstrating a spoofing attack against a Generation One EPC setup using a custom made device. The spoofing process is relatively simple requiring the following steps:

1. Upon power up and after a preamble is sent by the reader
2. The Spoofer backscatters any RN16.
3. The Interrogator acknowledges the Tag by sending an ACK.

4. If the Tag receives the ACK and ignores checking responding with a spoofed PC, EPC, and CRC-16
5. The reader then accepts the spoofer as a valid tag and adds it to an inventory of contactable tags

Again, any large-scale system utilising RFID would be *highly* vulnerable to such an attack but there is a lack of data on if such an attack has yet to occur against a commercial system.

PREVENTING TAGS FROM BEING ATTACKED

Due to the current implementations of the standard any alteration of tag operations would require the costly and time consuming replacement of all RFID tags within a system before the vulnerability would be removed. One possible avenue that must be considered are the TALK and QUIET commands which are used to simplify tag to reader communication by removing the likelihood of tag collisions (EPCGlobal, 2005b, p.6).

This is achieved through the issuance of a valid QUIET command which renders a given tag silent until a valid TALK command is issued or the tag is powered down for any period greater than one second. Typically this command is never explicitly sent by a user but is employed by the RFID reader on all tags within range as a default during communication with a single tag. However, this method requires a standard compliant reader in transmission range of every tag, which is unlikely given the range and power of EPC equipment (Bolan, 2008).

This leads then to the idea of utilising active jamming to prevent tags from responding to any command, let alone a KILL request. Active jamming is a well known technique of attack against any technology that utilises radio based communication (Pleikys, 2003). Put simply, this technique requires the jamming of the radio frequency on which an RFID system operates in order to disrupt the operation of all transponders and transceivers within signal range of the jamming device. It is widely stated (Peris-Lopez, Hernandez-Castro, Estevez-Tapiador, & Ribagorda, 2006) that any part of an RFID system disabled by such methods would immediately return to functionality once the jamming device has been disabled or moved from range.

Both the Air Interface for EPC tags and the ISO18000-6 standards allow for Frequency Hopping Spread Spectrum (FHSS) for the reader to tag communications. Utilising this allowance, a number of countries, including the U.S. and Australia, have permitted the use of FHSS for RFID implementations. This means that an RFID reader may, in a pseudo-random sequence, hop between channels within the operating band of frequencies.

A critical reason behind the usage of FHSS is the assertion that it provides some immunity to Denial of Service (DoS) from in-band interference. Such assertions seem to stem from the use of FHSS in typical ‘symmetric’ systems. In symmetric FHSS implementations, both transmitter and receiver lock step, that is the receiver hops with the transmitter to each new channel within the operating frequency. In contrast, RFID systems employ ‘asymmetric’ FHSS, with only the transmitter hopping between channels and the RFID tag, due to processing limitations and lack of continuous power, regarding the *entire band* as a single channel. This means that while a reader may avoid a noisy channel by hopping to the next, an RFID tag is unable to do this. The tag effectively listens on all channels at once and thus, will attempt to react to *a* signal occurring anywhere within the entire band.

In Bolan (2007b) it was shown that by broadcasting an active signal within range of a group of RFID tags would render those tags silent for the duration of the jamming signal. This attack is illustrated in the figure 4 below showing that the addition of the tag is logged by the reader and labelled with a number 1 above with an accompanying reading from the oscilloscope labelled number 5. The attack signal is then introduced and is recorded via another capture from the oscilloscope which illustrates the spike of activity in label 6. The injection of the attack signal into the system is accompanied by a loss of tag to reader communication and this is recorded by the reader as the tag being removed from the communication field and logged in the diagram as label 2. After the period of attack is over the attack signal is then removed (label 7) and almost instantly the reader re-establishes communication and reregisters the ‘adding’ of the tag in label 3. This may be considered an active jamming attack.

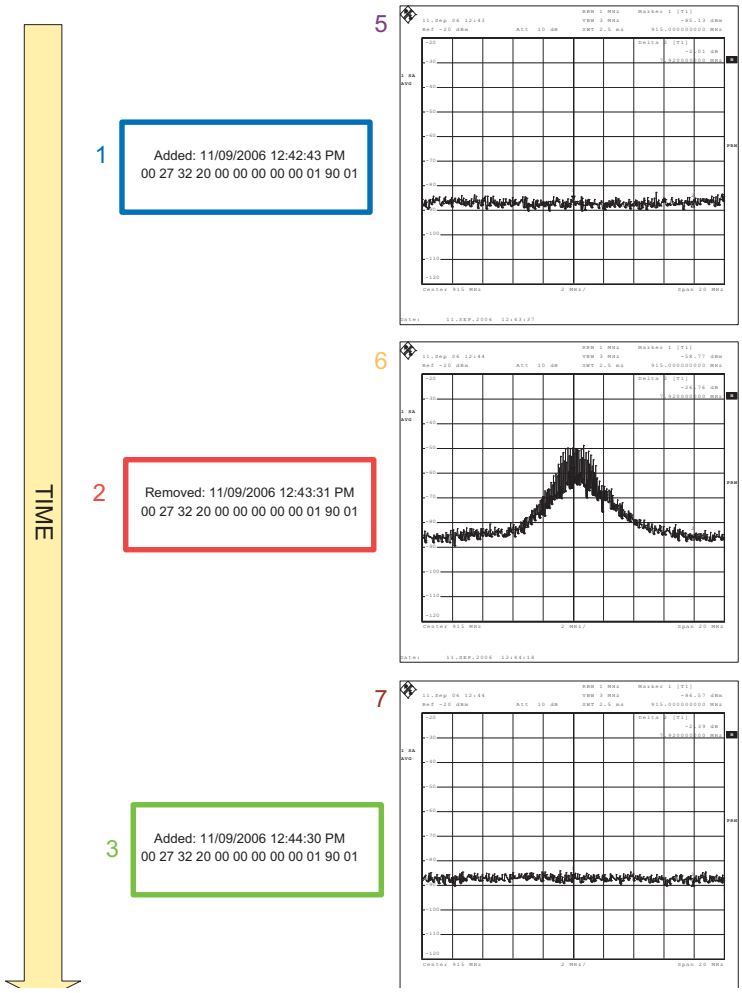

Figure 4. Annotated findings from an Active Jamming Attack

Admittedly the system would require coverage over an area that would include all the tags to be protected but if possible not include any active service area. To illustrate this idea let us explore the scenario of an RFID enabled storage. In this situation the shelving area would be blanketed by the jamming signal as illustrated in figure 5.

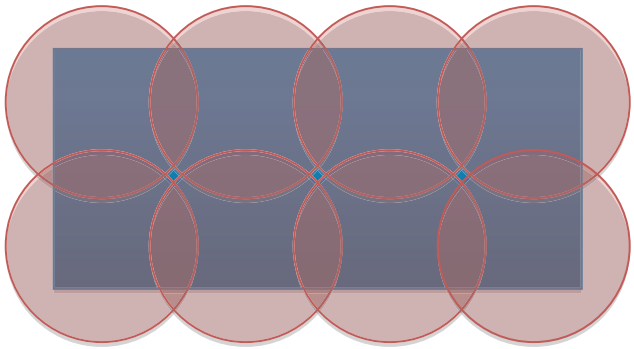

Figure 5. Warehouse with distributed jamming

In this example active jamming devices located in the centre of the red shaded regions (denoting their range) effectively render the warehouse area (blue rectangle) dead to RFID traffic. This would prevent an attacker from not only perpetrating the KILL attack but also other types of attack, including spoofing, or eavesdropping. When the RFID system was required, the jamming signal could be lifted. Whilst this system may be impracticable during hours of normal operation as the RFID may be constantly required, it would prevent such attacks occurring during times when the warehouse was closed. Conversely, this proposal may not be appropriate in systems where the need for availability is constant or there is a possibility of signal leakage from the jamming.

This is of course in the early stages of development and will require further testing to validate the viability of the solution before implementation in a commercial setting. The ideas behind the RFID jamming approach have however been demonstrated individually as viable methods of attack. Yet, until more significant metrics on amounts of RFID attacks within current installations are gathered and when they occur it is impossible to quantify or even speculate as to the actual outcomes.

CONCLUSION

This paper proposed a method for using active jamming against a users own system to reduce the likelihood of attacks such as the KILL attack. Whilst cognisant of the limitations of this approach, it may well offer the best and perhaps only defence against attacks of this nature against this specific generation of tags until a new standard is ratified. The potentially catastrophic effects of having a large amount of RFID tags wiped without any simple or quick recovery mechanism may then be considered to offset any limitations in operation. When viewed in this light the use of active jamming for defensive purposes may be a genuine approach until an update in the EPC standard occurs.

The paper also highlighted the large amount of future work in this area that is required. Such work will always be somewhat theoretical in nature until true metrics are gathered as to the real occurrences of such attacks and adjoining analysis of how such attacks were carried out. Thus, such analysis may form the basis for the next step in this research before data may be gathered on any possible reductions or benefits that active jamming would allow.

REFERENCES

Ahson, S., & Ilyas, M. (2008). RFID Handbook: Applications, Technology, Security, and Privacy. Boca Raton: CRC Press.

Bolan, C. (2006). The Lazerus Effect: Ressurecting Killed RFID Tags. Paper presented at the 4th Australian Information Security and Management Conference, Perth, Western Australia.

Bolan, C. (2007a). Radio Frequency Identification: a review of low cost tag security proposals. International Journal of Information and Computer Security, 1(4), 391-399.

Bolan, C. (2007b). A Single Channel Attack on 915MHz Radio Frequency Identification Systems. Paper presented at the 5th Australian Information Security and Management Conference, Perth, Western Australia.

Bolan, C. (2007c). KILL Features of RFID Tags in a Medical Environment: Boon or Burden? Paper presented at the World Congress in Computer Science, Computer Engineering, and Applied Computing (Security and Management), Las Vegas, Nevada.

Bolan, C. (2008a). RFID Communications - Who is listening? Paper presented at the 6th Australian Information Security Management Conference, Perth, Western Australia.

Bolan, C. (2008b). A Review of the Electronic Product Code Standards for RFID Technology. Paper presented at the Seventh International Network Conference, Plymouth, UK.

Bolan, C. (2009). A Spoofing Attack against an EPC Class One RFID System. Paper presented at the 7th Australian Information Security Management Conference Perth, Western Australia.

Engels, D. W. (2004). RFID: The Technical Reality. Paper presented at the Radio Frequency IDentification: Applications and Implications for Consumers, Washington.

EPCglobal. (2005). EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960MHz (pp. 94): EPCglobal.

Hunt, V. D., Puglia, A., & Puglia, M. (2007). RFID: A Guide to Radio Frequency Identification. Hoboken, New Jersey: John-Wiley & Sons.

Li, F., Clarke, N., & Bolan, C. (2007). User Perception of the Security & Privacy Concerns of RFID Technology. Paper presented at the International Symposium on Human Aspects of Information Security & Assurance, Plymouth, UK.

Pleikys, R. (2003). Radio Jamming in the Soviet Union, Poland and other East European Countries Retrieved 01/09/2008, from http://www.radiojamming.puslapiai.lt/article_en.htm

Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagorda, A. (2006). RFID Systems: A Survey on Security Threats and Proposed Solutions. Paper presented at the 11th IFIP International Conference on Personal Wireless Communications, Albacete, Spain.

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