Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2009

Spoofing Attack Against an EPC Class One RFID System

Christopher Bolan
Edith Cowan University

Originally published in the Proceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia, 1st to 3rd December 2009
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/3

A Spoofing Attack Against an EPC Class One RFID System

Christopher Bolan
secau - Security Research Centre
School of Computer and Security Science
Edith Cowan University

Abstract
In computing the term spoofing historically referred to the creation of TCP/IP packets using another device's valid IP address to gain an advantage. The Electronic Product Code (EPC) RFID system was investigated to test the efficacy of spoofing a valid tag response to basic requests. A radio frequency transmission device was constructed to determine whether a valid reader could distinguish between the response of an actual tag and a spoofed response. The results show that the device was able to successfully deceive the EPC reader and further, to replace actual tag responses with a spoofed response. The potential for such attacks against inventory systems using the EPC standard would be significant in terms of both operational and actual costs.

Keywords
Radio Frequency Identification, RFID, Spoofing

INTRODUCTION
Radio Frequency Identification (RFID) relies on transponders which are incorporated into an object for the purpose of identification or tracking. 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. A barrier to the uptake of RFID systems was the lack of standards which has been addressed by the creation and dissemination of the Electronic Product Code (EPC) standard. The EPC standard governs the whole scope of an RFID system including the operation of compliant RFID tags and readers.

"The Electronic Product Code is an identification scheme for universally identifying physical objects via Radio Frequency Identification tags and other means" (EPCglobal, 2005a, p.9). The electronic product code (EPC) standards were created by EPCglobal as an open, community based approach to promote the use of RFID technology in supply chain management. While Juels (2004b, p.138) states that "the aim of EPCglobal is to see RFID tags supplant barcodes", according to EPCglobal (2005c, p.11) their explicit aims were:

- "To facilitate the exchange of information and physical objects between trading partners."
- "To foster the existence of a competitive marketplace for system components."
- "To encourage innovation."

In addition, while not explicitly focused on security the standards also purport to (EPCglobal, 2005c, p.12):

- Promote a secure environment for the use of RFID systems, through either built in security features or recommending 'best practice'.
- Protect both individual and organisational privacy.

Having already demonstrated a successful eavesdropping attack against a Generation One EPC setup using a custom made device (Bolan, 2008) which outlined RFID interception the next logical step was to establish if communication spoofing could be successfully carried out. 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.

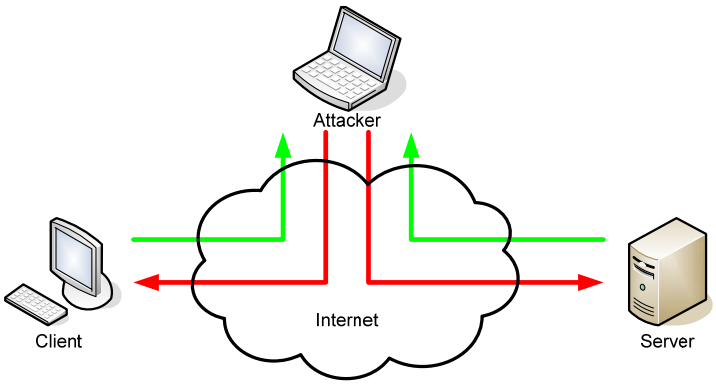

Figure 1 – Man in the Middle Attack

In the above example the attacking agent must monitor the packets transferring from the client to the server. When enough packets have been read the attacking agent then uses this information to send its own packets to the server who believes they are communicating with the client. Given such an attack type the question was posed might such an attack be applied to EPC RFID systems?

CONSTRUCTION OF AN EPC RFID SPOOFING ATTACK

The first consideration in answering this question was to reinvestigate the basic components of an RFID system to determine lines of communication that may be vulnerable to such an attack. In order to evaluate the applicability of such attacks to RFID systems required the construction of a device that was able to output an RFID signal that would be received by a RFID Reader and be thought to be an actual tag. As the previously discussed RFID eavesdropping device developed had the capability to transmit it was decided to utilise the same equipment to generate a spoofed signal (figure 2).

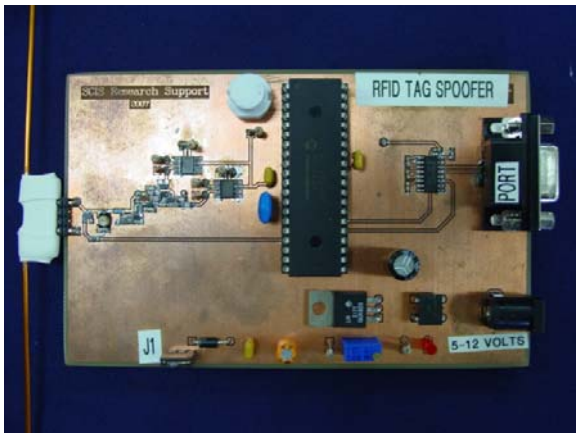

Figure 2 – The RFID Spoofing Device

The first step in creating a spoofed tag response was to investigate the functioning of the SCROLLALLID command in greater detail. The command (illustrated in figure 3) works as follows (EPCGlobal, 2005b, p.44):

1. Upon power up and after a preamble is sent by the reader
2. The Tag transitions to the reply state and backscatters an RN16.
3. The Interrogator acknowledges the Tag by sending an *ACK*.
4. If the Tag receives the *ACK* with a correct RN16 it backscatters its PC, EPC, and CRC-16 and transitions to the acknowledged state.
5. The Interrogator access the acknowledged tag

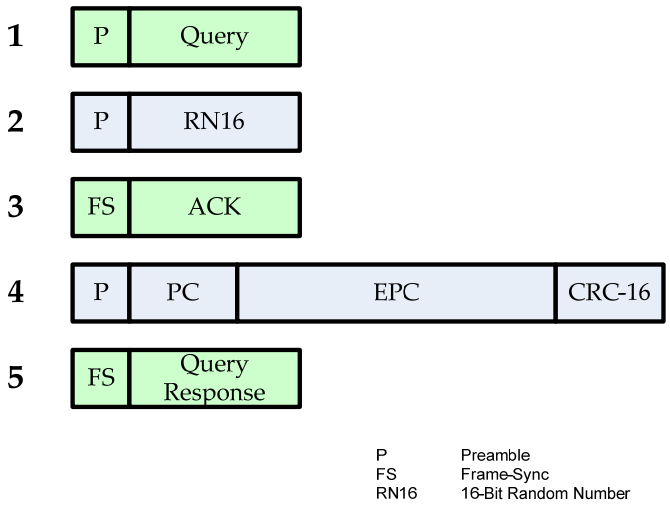

Figure 3 – The EPC Query Process

Thus the first thing the spoofer had to look for was the tag to reader preamble followed by an inventory query command. Normally after this step, as an acknowledgement the tag then backscatters the signal replying with a 16 bit random number (RN16), it was decided for simplicity to use the same number in the code for this proof of concept as collisions would not be a factor. Interestingly even with a preselected number the chance for a collision with a genuine tags RN16 is still quite low with the probability that any two or more tags simultaneously generate the same sequence is less than 0.1% regardless of when the Tags are energized (EPCGlobal, 2005b, p.40).

Once the reader has received the RN16 it responds with a frame sync and an acknowledgement in the form of a standard command of two bits (01) and the RN16 used by the tag. This command allows the reader to focus on an individual tag as that RN16 should serve as a reasonably unique identifier and other tags receiving the incorrect RN16 will then ignore the subsequent commands until a new communication round is started (EPCGlobal, 2005b, p.52). It is the next round of communication that is of real concern to a spoofing based attack where the tag uses the readers ACK signal to backscatter its protocol control bits, its EPC identifier and a 16 bit Cyclic Redundancy Check (CRC-16) to the reader. If the EPC tag number could be emulated then the reader would naturally assume that it has connected to a valid EPC tag and would then establish further communication.

Given these consideration the procedure for tag spoofing may be summarised as follows:

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

The initial concern was to ensure that the experiment was free from outside interference allowing the researcher to rule out outside factors as having an impact on the results. To this end a purpose built faraday cage was utilised as previous testing had already demonstrated its efficacy in isolating the testing rig from outside 'noise' (Bolan, 2008). The next step was the construction of a test to baseline normal behaviour which might later be used to compare the result of any test to ensure that spoofing had been successful. The construction of this setup used a normal EPC Class One tag being inventoried by a laptop setup with a WJ45 RFID Reader. The tag was then left to inventory over a 5 minute period and the software was set to log to a comma separated values file. With the baseline established the setup for the spoof experiment could be conducted. The setup for this experiment was kept similar to the baseline test with the only change being the replacement of the tag used in the baseline with the RFID Tag Spoofer device. This experimental setup is illustrated in figure 4.

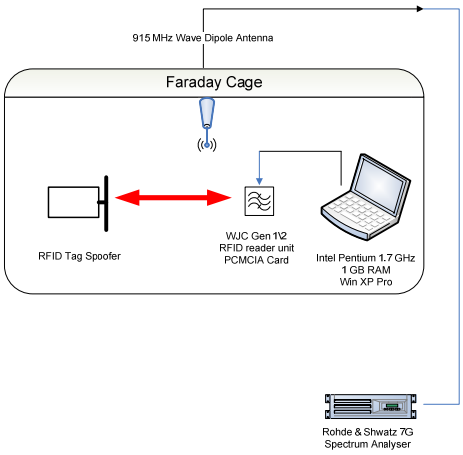

Figure 4 – Experimental Setup

To assist in the demonstration of a successful spoofing attack the RFID tag spoofer was coded to replicate the EPC identifier of the baseline tag. As this was a proof of concept experiment a successful test would only have to demonstrate that a device could successfully get a valid RFID reader to log its interaction as a successful inventory and thus save the 'spoofed' EPC identifier to the .csv log file. The test would be considered unsuccessful if the reader was able to determine that the communication did not comply with the expected communication protocol and thus failed to log the EPC identification to its inventory. To guarantee that the original baseline tag was not influencing the results of the experiment despite the faraday cage, it was moved beyond the distance the reader was cable of receiving.

For this experiment there were two 'independent variables'. Firstly, the status of the 'Responding Device' is a binary state variable with either the spoofer or the tag present. The second independent variable was which RFID tag from the experimental sample was being read or spoofed. Dependent variables are defined as the measurable factors which occur as a result of a change in one or more independent variables, therefore for this experiment the dependant variable was the 'Tag read status'. The status of a Tag read for this experiment is also a binary state variable with either the Reader unit being able to successfully register a tag or spoofing response during a tag inventory round or registering an invalid response. These variables are explicitly stated along with their possible values in table 1.

Table 1 – Experimental Variable

Type	Name	Values
Independent Variable	Responding Agent	TAG | SPOOFER
Independent Variable	RFID Tag Number	Tag Dependant
Dependent Variable	Tag Read	YES | NO

The 'confounding variables' facing this experiment was the manufacture and operating status of the RFID tags in the sample and the functioning of the RFID spoofing device. To limit the influence of the variable, every tag in the sample population was tested for operation both prior and post experiment. In addition the sample size and the number of tests selected also minimised the impact of this factor. The results from the tests are detailed in the next section.

RESULTS

For the tag spoofing experiment the control group was first done across a range of five tags, whereby an actual tag was inventoried over a fixed period. During these control tests the tag (tags 1 through 5) exhibit a normal inventory rate of around 2.48 inventory responses per second. This baseline is contrasted with the responses from the RFID spoofer where the response rate of the spoofing device was much lower on average with a range of values averaging 0.977 responses per second. The responses are graphed in figure 5 which clearly illustrates the high but separate correlation between the two distinct groups.

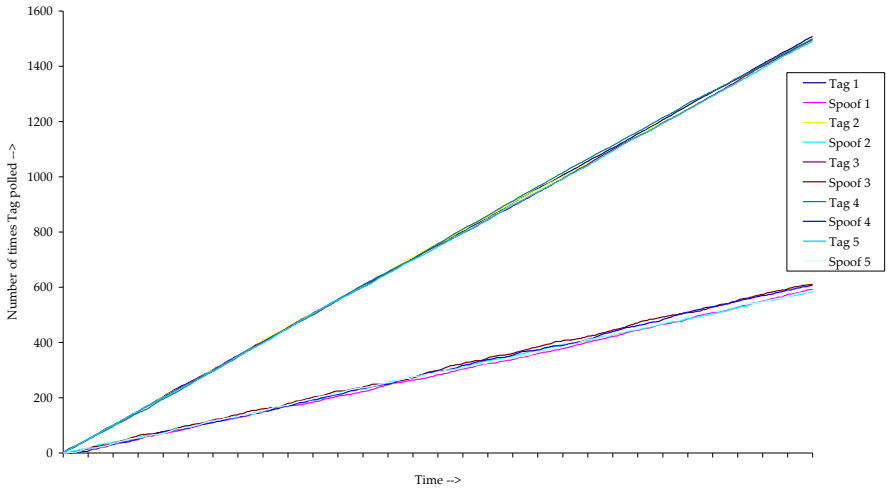

Figure 5 – Actual vs Spoofed Response rates

With the success of the initial results a second grouping was tested (figure 6) to show the responses from a switch between an actual tag to the spoofing device and then from the spoofing device to an actual tag. Again there is a noticeable drop-off in inventory response between the actual Tag and the spoofed response with the addition of small periods of inactivity when the physical switch of the tag and spoofer occurred within the Faraday cage.

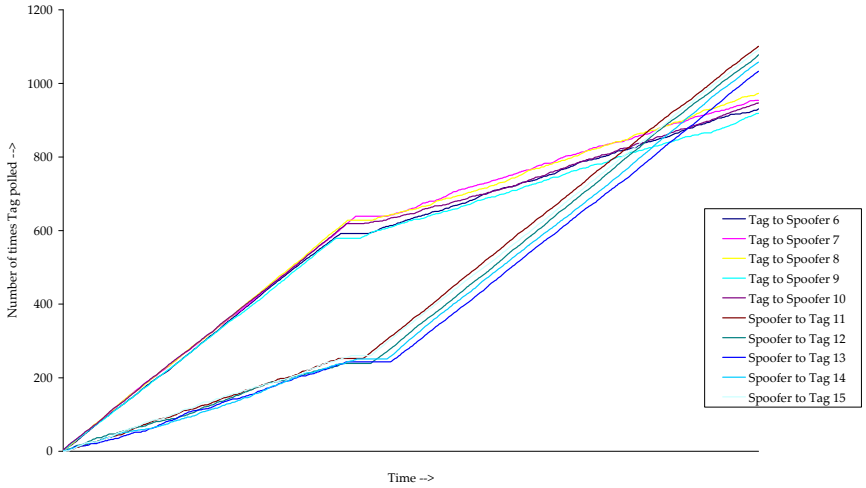

Figure 6 – Tag to Spoofer (Switch Comparisons)

CONCLUSION

This paper has demonstrated a successful spoofing attack against a Generation One EPC setup using a custom made device. Such results were predicted due to tlack of any significant measure within the EPC Standards to prevent such an attack from occurring. These findings further add to the increasing number of spoofing based attacks cited against other RFID systems and standards (Sarma *et al.*, 2002; Juels, 2006).

There has been some agurement in the RFID community that such an attack would become a more difficult exercise with the addition of encryption to the standard, however it is notable that the second generation of the standard still lacks this feature (EPC Global, 2005b). Such an oversight may be in part attributable to the difficulty of implementing a secure encryption method that is able to cope with the fast response – computational limited environments offered by passive

RFID systems. Such limitiations 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 aims to unite vendors at every level across the supply chain and has few if any rivals in its efforts. 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 spoofing based attacks.

REFERENCES

Basta, A., & Hatton, W. (2008). *Computer Security and Penetration Testing*. Florence, Kentucky: Thomson.

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

EPCglobal. (2005a). *EPC Generation One Tag Data Standards* (No. 1.1 Rev 1.27): EPCglobal. (1.1 Rev 1.27)

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

EPCglobal. (2005c). *The EPCglobal Architecture Framework*: EPCglobal

EPCglobal. (2005d). *Reader Protocol Standard - Version 1.1*: EPCglobal

Juels, A. (2004b). "Yoking-proofs" for RFID tags. In R. Sandu & T. Roshan (Eds.), *International Workshop on Pervasive Computing and Communication Security - PerSec 2004* (pp. 138-143). Orlando, Florida, USA: IEEE Computer Society.

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

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).

COPYRIGHT

Christopher Bolan ©2009. The author/s assign the Security Research Centre (SECAU) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SECAU & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors