2012

Utilizing the RFID LOCK Command Against Multiple Targets

Christopher Bolan
Edith Cowan University

Utilizing the RFID LOCK Command Against Multiple Targets

C. Bolan
School of Computer and Security Science, Edith Cowan University, Perth, Western Australia
secau – Security Research Centre , Perth, Western Australia

Abstract - *An unlocked Electronic Product Code (EPC) tag allows for issuance of most commands without the need for any authorization. This means that a system with unlocked tags would allow any attacker to modify tag data at will, whilst also opening the door to a range of other misuse. One possible avenue of active misuse against unlocked tags would be to issue LockID commands and 'permanently' lock some or all of a system's RFID tags. As this attack is simply an issuance of a valid command it fits firmly in the category of an active misuse and could also be considered a limited form of DoS as future valid commands would be ignored and limit or cripple the functionality of a system dependent on operation. This paper details an experiment using the LockID command to lock multiple tags within range.*

Keywords: Radiofrequency Identification, RFID Tags, Information Security

1 Introduction

Radio Frequency Identification (RFID) relies on transponders which are incorporated into an object for the purpose of identification or tracking [1]. The transponder (or tag) may be used to store information and will respond to signals sent by a transceiver (RFID reader) [2]. Increasingly such technology is being incorporated into supply chain management systems throughout the world and is expected to eventually replace traditional bar-coding systems [3].

"*The Electronic Product Code is an identification scheme for universally identifying physical objects via Radio Frequency Identification tags and other means*" [4]. 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 not explicitly focused on security, the standards purport to promote a secure environment for RFID use and protect both individual and organizational privacy.

Whilst EPC tags were primarily designed for write once / read many time applications they are able to be used in a variety of means across their four states of operation (un-programmed, programmed, locked and killed). These states dictate the behaviour of the RFID Tag when a given command is issued. The focus of this research was to investigate the use of the lock state and its related LockID command and builds upon previous work into directed LockID attacks.

2 The LockID Command

According to the EPC standards [5], the LockID command precludes further modification of values contained on an RFID Tag. The command based upon a more specific version of the ProgramID command whereby the [PTR] value points to the most significant bit of the password location and the [Value] must be equal to 0xA5 (hex value A5).

Given this command, the locking of an RFID tag may be achieved through the following steps:

1. Program the KILL code and leave the lock code at 00h;
2. Verify the EPC code by issuing a ScrollallID or VerifyID command;
3. Lock the tag by programming A5h to the Lock location;
4. Check that the tag is locked by issuing a VerifyID command. N

Note: If the tag is locked, the reader will receive no response to this command.

Accordingly, once the tag has been locked it will no longer respond to any programming commands, including the verify command. This suggests that, as the tag does not respond to the programming command, the lock code cannot be removed making it permanently locked. Thus it has been suggested that the only way to modify the tag at all is to utilize the kill command with the programmed password, which will render the tag inactive 'forever' [6]. Subsequent research has demonstrated that resurrection after a tag has been killed is possible – which has the duel effect of resetting the lock but at a significant time cost for any significant tag volume [7].

3 The Attack

To date a range of attacks have been developed against systems utilizing this standard, but the LockID based attack differs as it requires no password cracking or additional equipment. Rather, the purpose behind this attack is to utilize the existing controls of the standard to circumvent the systems normal functionality.

The single lock attack is based on the principle of an attacker selecting a single tag and locking that tag. At its base level this attack is no different to a legitimate user locking a single tag in any valid application. To test the validity of this attack a standard tag / reader setup was created in the Faraday cage as illustrated in figure 1.

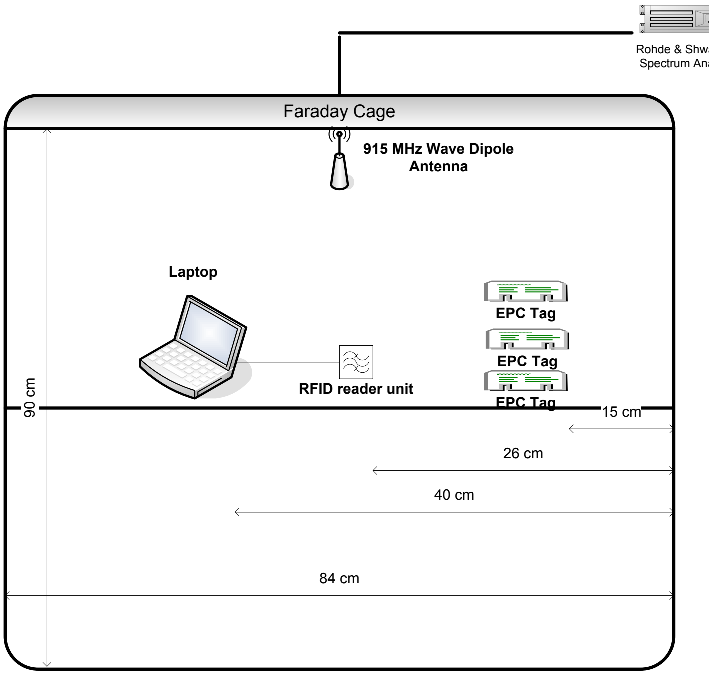

Figure 1 – Experimental Setup

The experimental setup included the use of three EPC RFID tags at a single time; this setup meant that a single tag from the selection may be targeted and locked and the other two may be tested to see if they remain unaltered, showing that a targeted attack against a single tag is viable. As there were three positions that could be occupied by the tags, it was decided that the position of the tag to be locked would be rotated amongst the three positions with each group.

Previous research on this targeted attack showed that the attack was highly effective, In essence the researcher was able to target a specific tag and lock the tag at will. This is demonstrated in figure 2. This new extension of the research was intended to demonstrate that such an attack would be highly scalable. Whilst a large variety of tag numbers were successfully attempted the discussion of results will be limited to three tag setups for the sake of visual clarity.

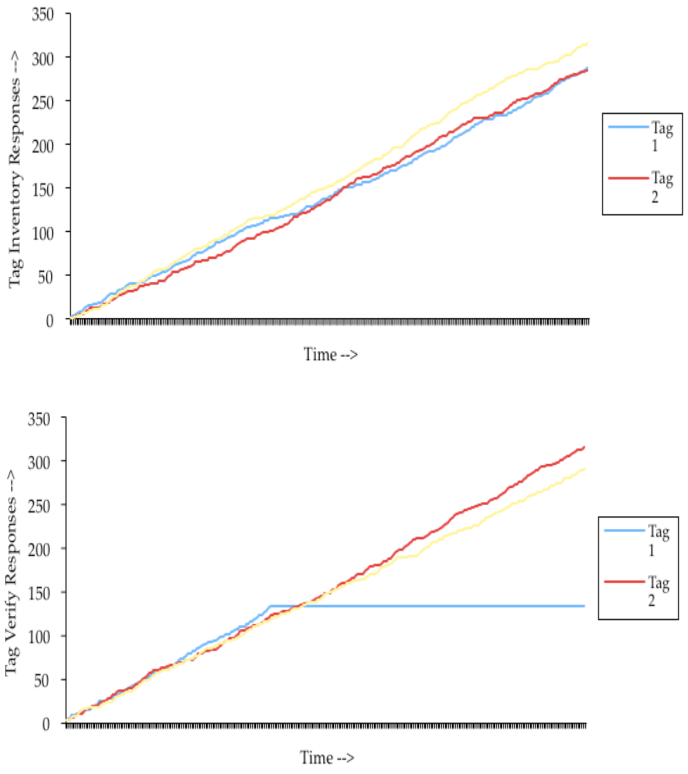

Figure 2 – Single Lock Results

Through experimentation it was found that their were two feasible methods of issuing the attack. The first would be to sequentially issue lock commands for every possible tag id within the tag space. To determine the validity of this attack a few simple calculations were conducted as detailed below:

Tag Identifier Space = 96 bits = 2^{96} =
79228162514264337593543950336

Assuming 100 Lock operations a second:

Complete Lock Attack Time = 2^{96} / 100 =
220078229206289826648734 hours
= 9169926216928742777031 days
= 25123085525832171992 years

Clearly such an attack method would be infeasible, even if a reader could somehow be increased tenfold to allow 1000 lock operations per second, the attack would still take far beyond a single lifetime. With this established, the second more feasible approach was considered whereby the reader would first conduct an inventory of the tags in the area of the attacking machine and then use the list of detected tags to issue focused lock commands.

In figure 3 below, three tags are setup in the cage with an attacking transceiver set to commence operation at a specified interval. From the figure it is clear to see that the attacks occur almost in parallel. Such results were paralleled with every size of victim sample trialed in the study.

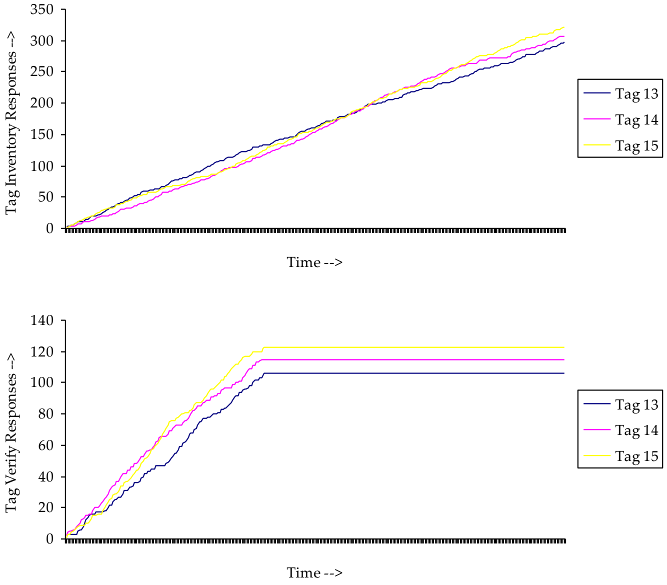

Figure 3 – LockID against multiple tags

Whilst either approach would constitute an active attack (i.e. one that requires direct interaction), it would be possible to integrate the collection method with an eavesdropping attack. Whilst such an attack may take longer to directly target all transponders that were contacted by legitimate users. Such attack blending could limit the detectability of the attack and reduce the likelihood of countermeasures being successfully created and deployed.

4 Conclusion

The paper presented a small but significant extension to the previously documented single lock attack. The simplicity of this approach is that like its directed counterpart the attack requires nothing beyond the standard equipment. The single LockID research demonstrated how the command may be targeted to an individual tag without altering the standard functionality of the RFID reader. Similarly the multiple vector attack was shown to work without the modification of the attacking transceiver.

Through the evidence of the multiple attacks efficacy and the two feasible methods of target gathering it is clear that such a method may be employed to attack complaint RFID systems. An example of this attack would be a Supermarket whereby the attacker could lock all tags in the store preventing prices (stored on the tag) from being altered. In this scenario, every affected transponder would need to be killed and resurrected to return to normal operation. Even using fairly conservative figures there would likely be a significant cost in time and lost revenue.

In the standards used for this experiment, the victim would likely find it difficult if not impossible to defend or detect the attack in time to make a difference. Whilst the EPC standard is rapidly evolving many existing setups may be the target of similar attacks though their currently seems to be a lack of evidence for such attacks taking place within the wider community. This may either be due to a lack of motive in the attackers or the rarity of such setups.

5 References

[1] Y. Zhang and P. Kitsos, Security in RFID and Sensor Networks. Boca Raton: Auerbach Publications, 2009.

[2] D. Hunt, A. Puglia, and M. Puglia, RFID: A Guide to Radio Frequency Identification. Hoboken, New Jersey: John-Wiley & Sons, 2007.

[3] A. Juels, ""Yoking-proofs" for RFID tags," in International Workshop on Pervasive Computing and Communication Security - PerSec 2004, R. Sandu and T. Roshan, Eds., ed Orlando, Florida, USA: IEEE Computer Society, 2004, pp. 138-143.

[4] EPCglobal, "EPC Generation One Tag Data Standards," EPCglobal 1.1 Rev 1.27, 2005.

[5] EPCglobal, "EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960MHz," EPCglobal 1.0.9, 2005.

[6] M. Rieback, "RFID Security and Privacy," PhD, Vrije Universiteit, Amsterdam, 2008.

[7] C. Bolan, "The Lazerus Effect: Ressurecting Killed RFID Tags," in 4th Australian Information Security and Management Conference, Perth, Western Australia, 2006.