Using the Generation One EPC RFID LockID command as a method of directed attack

Christopher Bolan

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

Abstract: An unlocked Electronic Product Code (EPC) tag allows for issuance of any command without the need for any authorisation with the exception aforementioned KILL command. 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 dependant on operation. The importance of such findings are increased by the fact that by its very nature, compliance with the standard would prevent any possible mitigation strategy.

1 Introduction

Radio Frequency Identification (RFID) relies on transponders which are incorporated into an object for the purpose of identification or tracking [ZK09]. The transponder (or tag) may be used to store information and will respond to signals sent by a transceiver (RFID reader) [HPP07]. Increasingly such technology is being incorporated into supply chain management systems throughout the world and is expected to eventually replace traditional bar-coding systems [Ju04]. 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. However, until now there has been a lack of published research into the security of the standard with most RFID security research focused on the creation of a satisfactory encryption method.

"The Electronic Product Code is an identification scheme for universally identifying physical objects via Radio Frequency Identification tags and other means" [Ep05a]. 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 [Ju04] states that "the aim of EPCglobal is to see RFID tags supplant barcodes", according to EPCglobal their explicit aims were [Ep05c]:

- *"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 [Ep05c]:

- 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.

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.

2 The LockID command

According to the EPC standard [Ep05b], 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 and KILL code by issuing a ScrollallID or VerifyID command;
3. Lock the tag by programming A5h to the Lock code location;
4. Check that the tag is locked by issuing a VerifyID command. 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' [Ri08]. Subsequent research has demonstrated that resurection 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 [Bo06b].

3 The Attack

To date a range of attacks have been developed against systems utilising this standard, but the LockID based attack differs as it requires no password cracking or additional equipment [Bo06a, Bo07, Bo08, Bo09]. Rather, the idea behind this attack is to utilise the existing controls of the standard to impinge on the functionality of the system.

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. The experimental setup includes 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. The variables concerning this experiment are detailed in the table below.

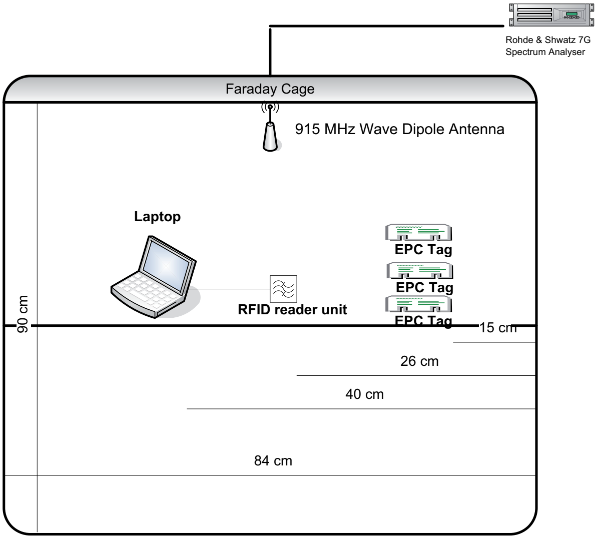

Figure 1: Experimental Setup

Type	Name	Values
Independent Variable	Tag A Status	LOCKED | UNLOCKED
Independent Variable	RFID Tag Number (Tag A)	Tag Dependant
Independent Variable	Tag B Status	LOCKED | UNLOCKED
Independent Variable	RFID Tag Number (Tag B)	Tag Dependant
Independent Variable	Tag C Status	LOCKED | UNLOCKED
Independent Variable	RFID Tag Number (Tag C)	Tag Dependant

Table 1: Experimental Variables

After the setup was planned, the experiments were run with an application that followed the following logic:

1. The application is started and supplied with a Target ID;
2. The application entered an VERIFY and inventory mode for a period of $T = 120$ logging its results;

3. The application then issues a LockID command using the Target ID;
4. The application then enters VERIFY and inventory mode again for $T = 120$.

Both verify and inventory commands were used to show the tags were functioning as predicted as whilst a locked tag would respond to an inventory request it should refuse to respond to a Verify command after a successful LockID command has been issued.

4 Results

The following figures detail the tag inventory response over the experimentation period on the upper graph against the responses to VERIFY commands during the same period. In all three figures it may be seen that the targeted tag (tags 3, 5 & 9) ceases to respond to VERIFY commands at $T = 120$ the exact time a LOCK command was sent.

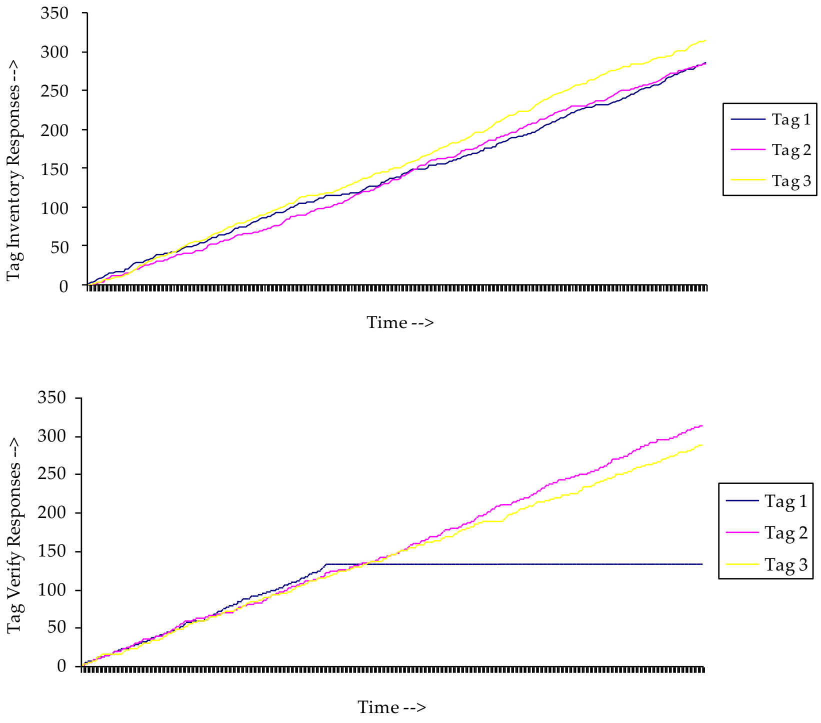

Figure 2: Single LOCK attack results [Tags 1 – 3]

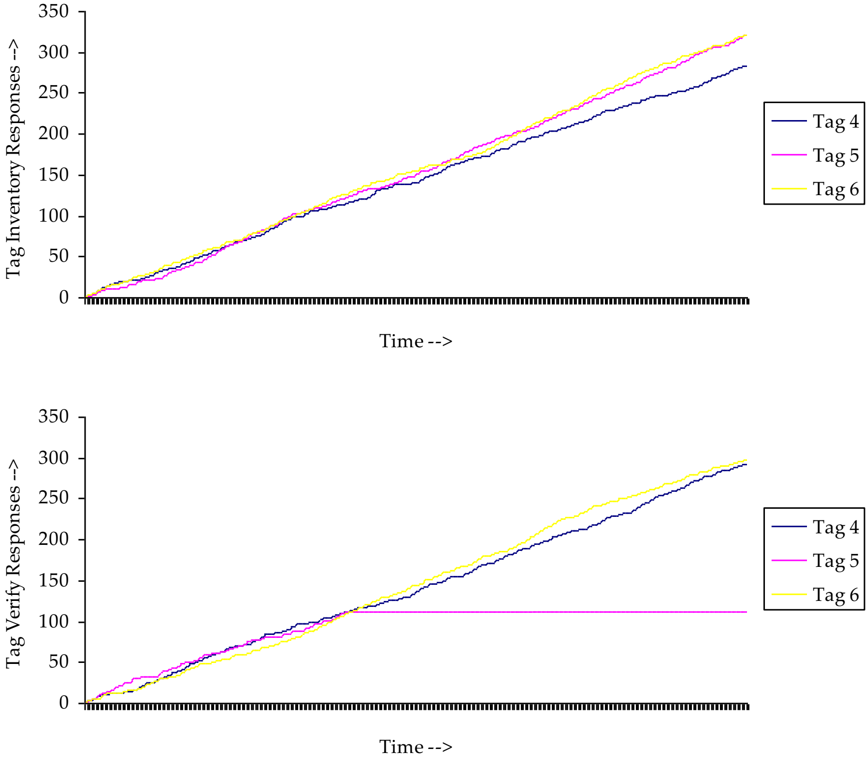

Figure 3: Single LOCK attack results [Tags 4 – 6]

Figure 2 shows the first set of tag results over the specified time period. In this set of graphs Tag 3 was targeted at and ceases full funtcioning after the successful issuance of the LOCKID command. Likewise the comparitive tests illustrated in figures 3 & 4 show tags six and nine exhibiting identical behaviour.

Despite the slight variations in tag inventory response rate across the three sets, there is little mathematical variation in the Pearson correlation between all inventory results above 0.99. Likewise between inventory and verify responses for each tag show a higher than 0.99 correlation with the exception of the locked tags (3, 5 & 9) which showed significantly differing regression lines due to the cessation of tag responses. This demonstrates that the functionality of the tags has indeed been limited through the directed issuance of a LockID command.

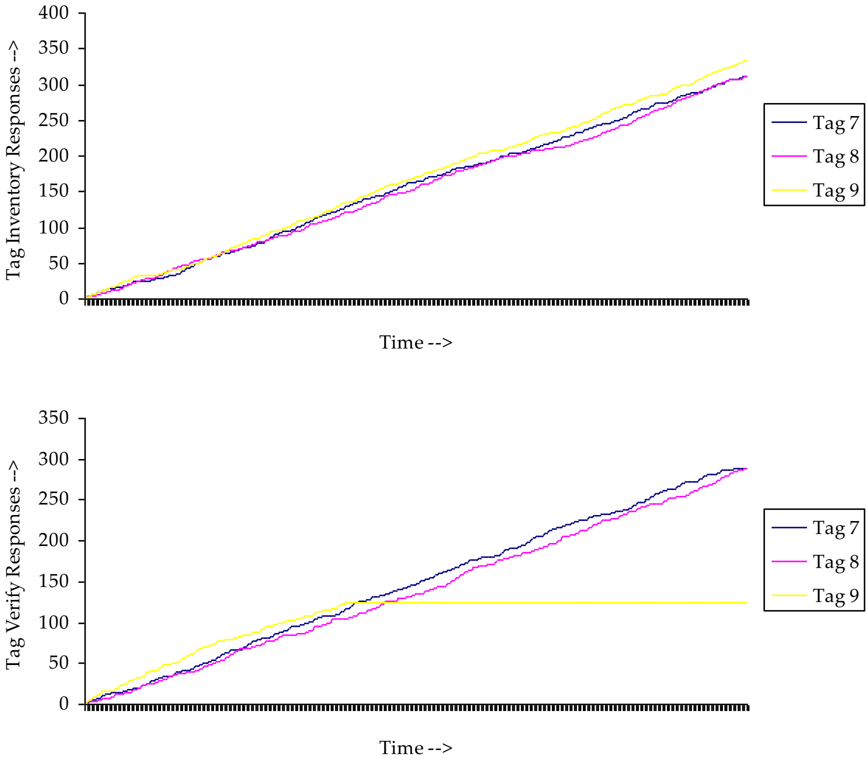

Figure 4: Single LOCK attack results [Tags 7 – 9]

To aid the discussion and highlight the significance of the findings of the discovered vulnerability a fictional scenario of a supermarket will be used. The fictional supermarket would be using EPC standard RFID tags attached to every item within the store in lieu of barcodes, and the thus the general security and checkout features would be based on EPC complaint RFID readers. The lock attack would have a significant and ongoing impact on systems that require the tags to remain unlocked.

The impact of such an attack may be highlighted when viewed in the light of an inventory based sales environment such as a supermarket. In a supermarket the reason for not locking tags would likely be to allow for updates such as price changes, sales, etc. If a lock attack was carried out the only way to restore the writable nature of the tag would be for the store to kill the tags and then resurrect them using the logical scavenging method [Bo06b]. However, unlike the previously published kill attack, the tags would still register and operate on the supermarkets major operations and the DoS would be limited to any updates. Whilst, it would be unlikely that a supermarket would seek to restore the entire inventory, but rather only those items which required updating, this would potentially add a significant time cost to the business. Alternatively, on a poorly designed system this may prevent products from being processed by automatic updates leading to mispricing and potential over/under charging of customers.

5 Conclusion

The research into this command has demonstrated how the command may be targeted to an individual tag without altering the standard functionality of the RFID reader. Should such an attack be perpetrated against a system that utilised functionality that was removed by tag locking it would require that every affected tag be killed and resurrected to return to normal operation.Even if this was done in a system with known kill passwords there would still be a significant cost in time and lost revenue.

Unfortunately, the way the current EPC standard operates would prevent an individual vendor wishing to fully comply with the standard a clear method of securing against such an attack. The only real way of preventing a scenario such as the one described in this paper would be for an ammedment of the standard to allow for a lock password or similar device to be added. Such an addition whilst not a complete preventative, would mean that such an attack would prove much more difficult to perpetrate.

In the mean time any system fully compliant to the relevant EPC standards discussed in this paper will be completely vulnerable to a directed EPC lock attack.

References

[Bo06a] Bolan C. Strategies for the blocking of RFID tags. Sixth International Network Conference. Plymouth, UK; 2006.

[Bo06b] Bolan C. The Lazerus effect: Resurrecting killed RFID tags. 4th Australian Information Security and Management Conference. Perth, Western Australia: Edith Cowan University; 2006.

[Bo07] Bolan C. A single channel attack on 915mhz radio frequency identification systems. 5th Australian Information Security and Management Conference. Perth, Western Australia: ECU; 2007.

[Bo08] Bolan C. RFID communications - who is listening? 6th Australian Information Security Management Conference. Perth, Western Australia: SECAU - Security Research Center; 2008.

[Bo09] Bolan C. A spoofing attack against an EPC class one RFID system. 7th Australian Information Security Management Conference Perth, Western Australia; 2009.

[Ep05a] EPCglobal. EPC generation one tag data standards: EPCglobal; 2005. p. 87.

[Ep05b] EPCglobal. EPC radio-frequency identity protocols class-1 generation-2 UHF RIFD protocol for communications at 860 mhz - 960mhz: EPCglobal; 2005. p. 94.

[Ep05c] EPCglobal. The EPCglobal architecture framework: EPCglobal; 2005. p. 53.

[HPP07] Hunt VD, Puglia A and Puglia M. Rfid: A guide to radio frequency identification. Hoboken, New Jersey: John-Wiley & Sons; 2007.

[Ju04] Juels A. Yoking-proofs for RFID tags. In: Sandu R and Roshan T, editors. International workshop on pervasive computing and communication security - persec 2004. Orlando, Florida, USA: IEEE Computer Society; 2004. p. 138-43.

[Ri09] Rieback M. RFID security and privacy. Amsterdam: Vrije Universiteit; 2008.

[ZK09] Zhang Y and Kitsos P. Security in rfid and sensor networks. Boca Raton: Auerbach Publications; 2009.