12-3-2012

A proposed formula for comparing kill password effectiveness in single password RFID systems

Christopher Bolan
Edith Cowan University

DOI: 10.4225/75/57b55b44cd8dc
10th Australian Information Security Management Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012

A PROPOSED FORMULA FOR COMPARING KILL PASSWORD EFFECTIVENESS IN SINGLE PASSWORD RFID SYSTEMS

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

Abstract

The Electronic Product Code standard for RFID systems plays a significant role in worldwide RFID implementations. A feature of the RFID standards has been the RFID Kill command which allows for the 'permanent' destruction of an RFID tag through the issuing of a simple command. Whilst the inclusion of this command may be vital for user privacy it also opens up significant avenues for attack. Whilst such attacks may be well documented there has been little to no discussion of the efficacy of the differing mitigation approaches taken. A simple formula to calculate the full timing of such an attack on differing RFID setups is presented. The formula allows for users to model the effect that altering such aspects as timeout or transmission response time will have on RFID security.

Keywords
Radio Frequency Identification, Passwords, Brute Force

INTRODUCTION

Radio frequency identification (RFID) technology stems back to Faraday's discovery that light and radio waves were both forms of electromagnetic energy. The first concrete step towards the modern conception of RFIDs was made in 1948, although it was not until 1973 the first direct patent on passive RFID tags was lodged (Stockman, 1948; 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 an attached antenna embedded in a protective material.

Every RFID system consists of three major components (Sarma *et al.*, 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"*.

In a typical RFID system using passive tags, an interrogator (RFID Reader) receives data from an RFID Tag by first broadcasting a continuous-wave RF signal to the Tag (EPC Global, 2005a). Passive tags then use this signal to respond by modulating the reflection coefficient of its antenna, thereby backscattering an information signal to the reader.

Of the numerable RFID standards, arguably one of the more significant in terms of applications is the Electronic Product Code (EPC) standard. The EPC standards were created by EPC global as an open, community based approach to promote the use of RFID technology in supply chain management (EPC Global, 2012). Since EPCs inception, the standards have been used in RFID systems worldwide and are significant in terms of the global RFID market (*ibid*).

PASSWORDS IN RFID SYSTEMS

An important factor in determining how resilient a system is to attack is to have a reasonable knowledge of how vulnerable a password based feature is to an attack. Numerous works (Cross, 2008; Bonneau, 2012) have detailed the primary methods of password cracking:

- Brute Force – Directly trying a sequence of passwords

- Dictionary – Applying a set of predetermined values against a password
- Pre-Computed Hash – Subverting a system by attacking the password hash
- Syllable – A combination of brute force and dictionary approach
- Rule Based – Used where passwords fit a common form

Before a method for determining vulnerability to such attacks could be created, an understanding of the length, composition and usage of passwords is required. EPC Gen 2 systems use two types of passwords or codes that are stored on the RFID tag namely the Kill and Access passwords (EPC Global, 2010). As this research is focused on quantifying the vulnerability of RFID systems to KILL Attacks only the Kill code will be discussed.

The EPC Tag Data Standard (EPC Global, 2008, p.56) defines the Kill password as "*A 32-bit password that must be presented to the tag in order to complete the Gen 2 "kill" command*". This statement clearly shows a physical limitation to the key space of 32bits or put another way one of 4,294,967,290 possible values. This is a considerable improvement of the 16bit size restriction of the generation one EPC standard (EPC Global, 2005b). Given the straightforward nature of this password the only applicable form of attack is brute force.

THE KILL COMMAND

The Kill command was incorporated into the standards as both a privacy and security measure. It was envisaged that the vendor would be able to kill a tag upon a successful sale and thus prevent further user tracking. This technique would also limit the chance that a used tag could give away potential compromising information about the vendor or their setup.

As detailed by the EPC Class One Generation Two Protocol for Communication (EPC Global, 2008, p.67) all tags and interrogators adopting the EPC standards shall implement the Kill command in a set fashion. The procedure for this is detailed in figure 1. In brief, the interrogator (or reader) after establishing communication with a tag then issues a kill requests containing half the Kill password waiting for the tag to respond with its handle then send a second Kill request containing the rest of the password (EPC Global, 2008, p.67).

As depicted in the figure below, depending on the outcome the tag will stay silent in the event of an invalid attempt, send an error code in the case of insufficient power or send confirmation of a valid kill. It is worth noting that if the password is set to a value of 00h the Kill operation is not allowable and the tag will respond with an error code.

The standard is notable for not specifying a timeout between attempts at kill operations. However, as noted in Bolan (2007) some manufacturers have added these features in their tags and the inclusion of this feature does not violate the standard nor seem to preclude the granting of EPC compliance. Using this command an attacker might use a brute force approach and thus try every available password until a successful kill was achieved. In the case of a common password this attack could then kill every tag within range.

To understand the effect of this attack let us consider the effect of a brute force Kill attack against an RFID enabled supermarket. The impact would be nothing short of devastating. An attacker could deploy a device that would render all tags within the store unusable.

Unlike a denial of service or jamming attack this method would continue to be in effect even after the attacking device had ceased operation. Put in context, every item in the store would be invisible to any RFID based security feature, inventory system or point of sale scanners. Whilst it would be possible to recover from such an attack the logistics and cost of doing so would be significant with every tag requiring individual reactivation a task that could take up to a minute an item. Assuming a typical supermarket has one million items and thirty staff were working consistently on reactivating items after a KILL attack has occurred, it would take 23 days to completely restore the supermarket to operation.

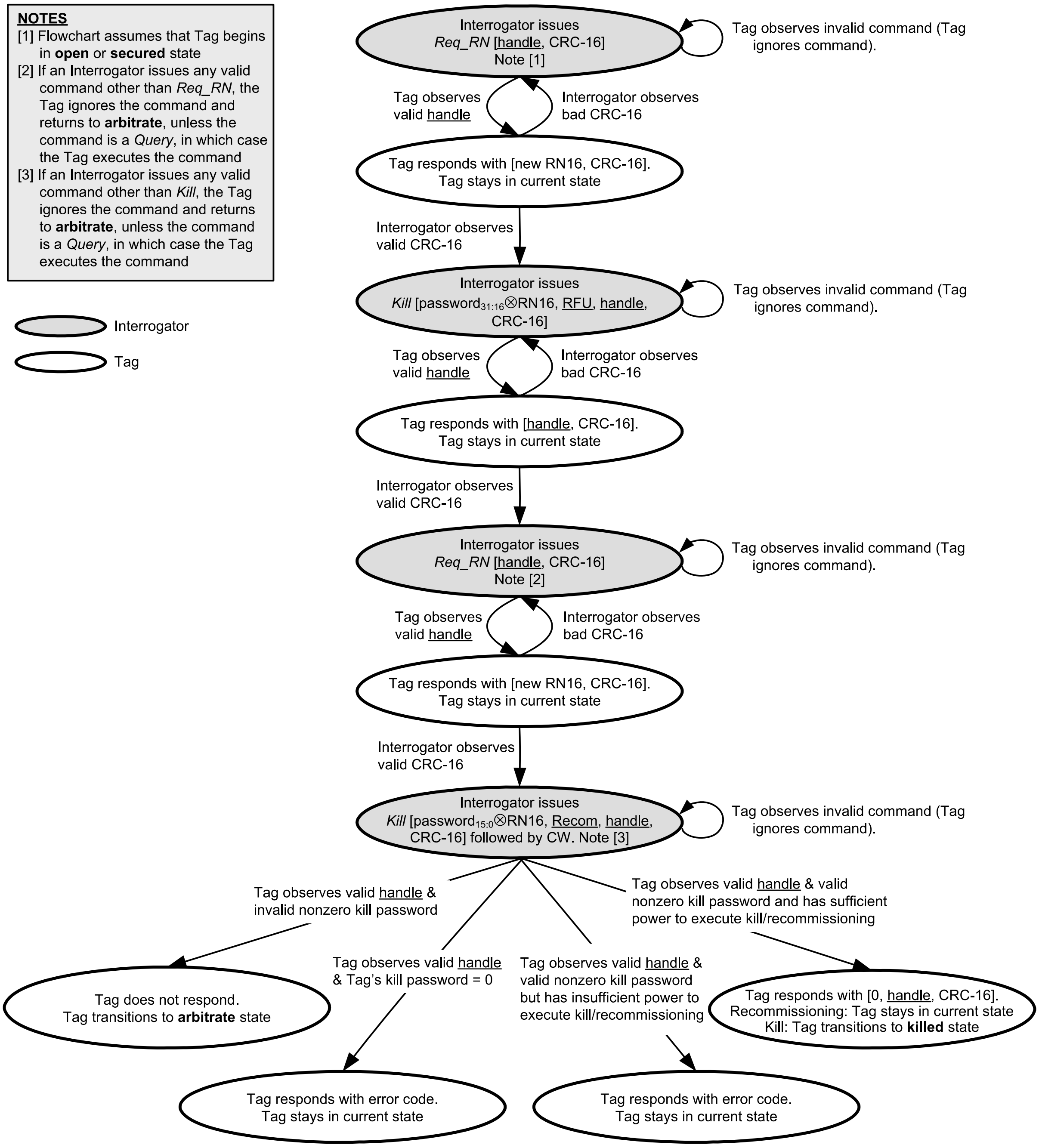
NOTES
[1] Flowchart assumes that Tag begins in open or secured state
[2] If an Interrogator issues any valid command other than Req_RN, the Tag ignores the command and returns to arbitrate, unless the command is a Query, in which case the Tag executes the command
[3] If an Interrogator issues any valid command other than Kill, the Tag ignores the command and returns to arbitrate, unless the command is a Query, in which case the Tag executes the command
Interrogator
Tag
Interrogator issues Req_RN [handle, CRC-16] Note [1]
Tag observes invalid command (Tag ignores command).
Tag observes valid handle
Interrogator observes bad CRC-16
Tag responds with [new RN16, CRC-16]. Tag stays in current state
Interrogator observes valid CRC-16
Interrogator issues Kill [password$_{31:16}$⊗RN16, RFU, handle, CRC-16]
Tag observes invalid command (Tag ignores command).
Tag observes valid handle
Interrogator observes bad CRC-16
Tag responds with [handle, CRC-16]. Tag stays in current state
Interrogator observes valid CRC-16
Interrogator issues Req_RN [handle, CRC-16] Note [2]
Tag observes invalid command (Tag ignores command).
Tag observes valid handle
Interrogator observes bad CRC-16
Tag responds with [new RN16, CRC-16]. Tag stays in current state
Interrogator observes valid CRC-16
Interrogator issues Kill [password$_{15:0}$⊗RN16, Recom, handle, CRC-16] followed by CW. Note [3]
Tag observes invalid command (Tag ignores command).
Tag observes valid handle & invalid nonzero kill password
Tag observes valid handle & Tag's kill password = 0
Tag observes valid handle & valid nonzero kill password but has insufficient power to execute kill/recommissioning
Tag observes valid handle & valid nonzero kill password and has sufficient power to execute kill/recommissioning
Tag does not respond. Tag transitions to arbitrate state
Tag responds with error code. Tag stays in current state
Tag responds with error code. Tag stays in current state
Tag responds with [0, handle, CRC-16]. Recommissioning: Tag stays in current state Kill: Tag transitions to killed state

Figure 1 – The EPC Kill Procedure (EPC Global, 2008, p. 69).

FACTORS THAT AFFECT THE PROCESS

In providing a method to determine the relative duration of a successful attempt to brute force a Kill password required the consideration of all factors within the Kill procedure. These were determined to be:

1. *Duration of an unsuccessful Kill attempt*

   One of the most important aspects when determining the duration required for a successful attack is the duration for a single attempt. In EPC RFID systems the speed of a communication round is determined by factors including the closeness of the tag and the interrogator, the speed of the reader and complaint tags as well as the environment.

2. *Duration of a timeout between Kill attempts*

   As noted in the previous section there is no set requirement within the standard for this feature. However, despite the lack of mandatory timeouts, many tags have incorporated this feature and the actual implementations vary between manufacturers.

3. *Number of tags that may be in range*

   As with the variations in speed the range of RFID equipment is dependent on numerous factors. Whilst the power and frequency of EPC compliant equipment is specified within the standards there has been evidence of variations between manufacturers. Beyond these variations the physical location of an interrogator and tags will be significant in determining attack effectiveness.

4. *Key Space – Gen 1 Vs Gen 2*

   Key space is critical in any consideration of cryptography. With EPC complaint RFID systems this key space is limited to either 16 bits for generation one equipment and 32 bits for generation two. However, it is conceivable that future generations will increase the key space so any formula for exploring the effectiveness of brute force Kill attacks should allow for this variable.

5. *Single or Multiple Password Setup*

   The final factor for consideration is whether an EPC compliant implementation uses the same Kill password for each tag or varies the password from tag to tag. Logistically setting individual passwords on each tag may prove a challenge and manufacturers have typically supplied tags with either a standard default value. Given the variability of the setups and the restrictions on this paper the discussion is limited to single password setups.

CONSTRUCTION OF THE FORMULA

With these factors defined let us consider the case of a basic Kill Attack whereby a interrogator attempting to brute force in sequence starting from 01h attacks a single tag and assume no timeout enforced between attempts and Generation One tags. In this scenario we may define the values as detailed in table 1. It should be noted that the key space is lessened due to the 16bit size limitation of generation one tags.

Table 1 – Variables in Scenario One

Variable	Value
Duration of an unsuccessful Kill Command	0.1 seconds
Timeout between Kill Commands	0 seconds
Number of Tags in Range	1
Single or Multiple Passwords	Single
Key Space	16 bits = 32768

In this straightforward scenario it is clear that each attempt will take 0.1 seconds and therefore to cover the entire key may be determined using the formula:

$$\textit{Full Attack} = (\textit{Attack Duration} + \textit{Timeout}) * \textit{Key Space}$$

$$= (0.1 + 0) * 32768$$

$$=3276.8 \textit{ seconds}$$

or approximately 55 minutes (rounded up)

However as noted previously a time out is often implemented in tags and if we now consider a timeout of ten seconds as found in numerous EPC tags we would therefore see:

*Full Attack = (Attack Duration + Timeout) * Key Space*

*= (0.1 + 10) * 32768*

= 330956.8 seconds

or approximately 92 hours (rounded up)

Whilst this formula suffices for a brute force attack against a single tag, the next consideration was to include the number of tags in range where the Kill password was set to the same value on all tags. For this example the variables are shown in table 2.

Table 2 – Variables in Scenario Two

Variable	**Value**
Duration of an unsuccessful Kill Command	0.1 seconds
Timeout between Kill Commands	10 seconds
Number of Tags in Range	10
Single or Multiple Passwords	Individual
Key Space	16 bits = 32768

The above formula would not suffice as the in this scenario the reader would be able to continue to interrogate other tags within range whilst awaiting the timeout for the original attempt. From the above it may be seen that the interrogator would be able to perform attempts against ten values in a single second and then have to wait 9.1 seconds before the next round of attacks. When considering this we have the following:

*Full Attack = Number of Iterations * Effective Timeout*

Number of Iterations = Key Space / Tags in Range

*Effective Timeout = Timeout – ((Tags in Range – 1) * Attack Duration)*

Therefore:

*Full Attack = (Keyspace / Tags in Range) * (Timeout – ((Tags in Range – 1) * Attack Duration))*

*= (32768 / 10) * (10 – ((10 – 1) * 0.1)*

*= 3276.8 * 9.1*

=29818.88 seconds

or approximately 8 hours and 17 minutes

This approach had a limitation whereby the formula would not allow for negative timeout. That is if the number of tags within range is a value such that the effective timeout is less than zero the formula return an invalid value (i.e. a negative). This scenario is illustrated using the values in the table below whereby the number of tags in range is set at 150 (more than required to negate the timeout).

Table 3 – Variables in Scenario Three

Variable	**Value**
Duration of an unsuccessful Kill Command	0.1 seconds

Timeout between Kill Commands	10 seconds
Number of Tags in Range	150
Single or Multiple Passwords	Individual
Key Space	16 bits = 32768

*Full Attack = (Keyspace / Tags in Range) * (Timeout – ((Tags in Range – 1) * Attack Duration))*

*= (32768 / 150) * (10 – ((150 – 1) * 0.1)*

=-1070.4213 seconds

Thus in the case of the timeout value being negated the formula would in essence become:

Full Attack = Key Space / (Number of Attacks a second)

Where

Number of Attacks per Second = 1 / Time of Attack

When considered against the previous formula we now see a more complex condition as shown in figure 2.

Max (Tags Before Repeat) = Timeout / Attempt Time

If Tags in Range < Max (Tags Before Repeat) then

*Full Attack = (Keyspace / Tags in Range) * (Timeout – ((Tags in Range – 1) * Attack Duration))*

Else

Full Attack = Key Space / (1 / Time of Attack)

Figure 2 – Algorithm to determine Brute Force time for RFID Kill Attack

UTILISING THE ALGORITHM TO COMPARE SETUPS

With the algorithm established it is possible to apply the results and metricize the viability of an approach and feasibility of a Kill attack against a specific setup. Table 4 compares the setup and results of a brute force kill attack against a single tag removed from a site against both a generation one and generation two EPC tag.

Table 4 – Comparison of Single Attack against Tag generations

Variable	Generation One	Generation Two
Duration of an unsuccessful Kill Command	0.1 seconds	0.1 seconds
Timeout between Kill Commands	10 seconds	10 seconds
Number of Tags in Range	1	1
Individual or Multiple Passwords	Individual	Individual
Key Space	16 bits = 32768	32 bits = 4,294,967,290
Attack Time	**~92 hours**	**~32687 years**

It is immediately obvious as to the effect of the increased key space. Whilst such a comparison may be obvious, the strength in the algorithm is its use in predictive scenarios. Table 5 demonstrates how by an alteration of tag time outs on generation two tag setups effects the best case attacker scenario whereby the a a sufficient saturation of tags within range to negate the standard 10 second timeout. To expand the impact the setup assumes a faster interrogator is applied.

Table 5 – Comparison of Attack against generation two tag timeouts

Variable	Scenario 1	Scenario 2	Scenario 3

Duration of an unsuccessful Kill Command	0.01 seconds	0.01 seconds	0.01 seconds
Timeout between Kill Commands	0 seconds	60 seconds	90 seconds
Number of Tags in Range	1500	1500	1500
Individual or Multiple Passwords	Individual	Individual	Individual
Key Space	32 bits = 4,294,967,290	32 bits = 4,294,967,290	32 bits = 4,294,967,290
Attack Time	**~32 years**	**~32 years**	**~96 years**

The above example demonstrates that in scenarios whereby an attacker has access to enough tags to negate the timeout features the inclusion of the timeout has no effect. Whereas, an increase of the tag timeout negates the availability of tags and increases the effective brute force time. Similar scenarios may be constructed utilising this approach to a wide variety of hypothetical issues and this allow for discussion upon metrics related to the relative risks of each approach.

CONCLUSION

Whilst straightforward the algorithm presented provides a useful mechanism for the comparison of Kill attacks in multiple scenarios. The application of this model will allow practitioners to effectively gauge the strength of an RFID setup and will also provide a method to calculate if an increase in tag or reader speed will have any effect on the future security of their system.

If we view the above methods in the light of the supermarket example mentioned in the paper, we may see the value of the tool. Utilising this research a security professional could quickly model the feasibility of this attack scenario against differing setups. This would allow for the easier communication of with both technical and non---technical stakeholders, and hopefully a more secure outcome.

As stated in the parameter selection, discussion on the effect of multiple password setups has not been included in this paper. However, the scenarios including this approach have been modeled successfully through minor modifications as well as initial modifications allowing for adaption to other forms of RFID attacks. These models will be the subject of forthcoming publications.

REFERENCES

Bolan, C. (2007). 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.

Bonneau, J. (2012). The science of guessing: analyzIng an anonymized corpus of 70 million passwords. Paper presented at the IEEE Symposium on Security and Privacy, San Francisco, California.

Cardulo, M. (2005). Genesis of the Verstile RFID Tag. RFID Journal, 2(1).

Cross, M. (2008). Scene of the Cyber Crime. Burlington MA: Syngress.

EPC global. (2005a). EPC Radio Frequency Identity Protocols Class 1 Generation 2 UHF RFID Protocol for Communications at 860 MHz - 960MHz (Version 1.0.9) (pp. 94): EPCglobal.

EPC global. (2005b). EPC Generation One Tag Data Standards (pp. 87): EPCglobal.

EPC global. (2008). EPC Radio Frequency Identity Protocols Class 1 Generation - 2 UHF

RFID Protocol for Communications at 860 MHz - 960MHz (Version 1.2.0): EPCglobal.

EPC Global. (2012). EPC Global: Electronic Product Code. Retrieved 15/10/2012, from www.gs1.org/epcglobal

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

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