M. Byers, A. Lofton, A. K. Vangari-Balraj, and D. R. Thompson, “Brute force attack of EPCglobal UHF class-1 generation-2 RFID tag,” in *Proc. IEEE Region 5 Technical Conf.*, Fayetteville, Arkansas, April 20-21, 2007, pp. 386-390.

Brute Force Attack of EPCglobal UHF Class-1 Generation-2 RFID Tag

Micah Byers, Anthony Lofton, Anil Kumar Vangari-Balraj, and Dale R. Thompson

Computer Science and Computer Engineering Dept., University of Arkansas

{byers, adlofto, avangari, drt}@uark.edu

***Abstract* - This paper simulates a brute force attack of the passwords on EPCglobal's UHF Class-1 Generation-2 passive RFID tags. The objective is to simulate a brute force attack on the password accounting for the length of the password, the number of bits to be transferred, the data link bit rate from the reader to tag, the data link bit rate from the tag to reader, and the required number of messages for the protocol between the reader and tag. According to the simulation, the average time to perform a brute force attack on the passwords is approximately thirty days.**

I. INTRODUCTION

A. Problem

Retailers and distributors who manage the supply chain use passive radio frequency identification (RFID) for uniquely identifying products with a serial number called the Electronic Product Code (EPC) [4], [5]. The code is standardized by EPCglobal Inc. [7]. In this form of RFID, the tag does not have its own power source but obtains its energy from the radio frequency signal of a reader. The reader interrogates the tag for its EPC number. Although today RFID tags are primarily attached to pallets and cases, in the future they will be attached to individual items. Therefore, the security of RFID will become important because of the number of objects that have tags.

The EPCglobal UHF Class-1 Generation-2 passive RFID tag (Gen-2) is significantly different from the Class-0 and Class-1 Gen-1 tags, including additional security features [5]. The password that protects the tag for Class-0, Class-1 Gen-1, and Class-1 Gen-2, are 24 bits, 8 bits, and 32 bits, respectively. Even though the password for Gen-2 is only 32 bits, the data link speed between the reader and tag is relatively slow. The speed of the link for exchanging messages between the reader and tag must be taken into account to determine the amount of effort to perform a brute force attack against the 32-bit key in Gen-2. How long on average does it take to do a brute force attack against a single tag?

B. Literature Review

In December 2004, EPCglobal approved the Class-1 Gen-2 UHF air interface protocol [1]. The Gen-2 protocol was created in response to the weak security that Class-0 and Class-1 Gen-1 tags provide. Gen-2 tags operate at UHF frequencies of approximately 900 MHz, and have become the standard in which many companies are producing their new RFID tag products, with promises of greater range, faster reads, simultaneous reads, and more reliability [2]. Since its approval, various companies, consultants, and institutions have been analyzing the security that Gen-2 provides.

Gen-2 has additional security features [5]. A 16-bit CRC (cyclic-redundancy check) is applied to the EPC for error detection [6]. In addition, a 16-bit CRC is used for error detection on certain reader-to-tag and tag-to-reader messages. Gen-2 tags have a 32-bit kill password [6]. The default value for a tag is all zeros and tags will not execute the kill command if the password is set to all zeros. If the tag has a nonzero password and the reader supplies the correct password then the tag will execute the kill command, which permanently disables the tag. Gen-2 tags also have a 32-bit access password whose default value is zero. If a tag has this access password set, the reader must issue this password before transitioning the tag into the secured state. Otherwise, access is denied.

Gen-2 tags have the ability to generate a 16-bit random or pseudo-random number (PRN) [6]. The 16-bit number is used to create a handle during singulation (a process where the reader targets a single tag) instead of using the EPC number, to encrypt reader-to-tag link communication, and to determine the number of slots to wait in the Q-protocol [5]. The 16-bit PRN is used during the inventory phase as a unique identifier that the reader is to acknowledge. Using a random number enhances security by obscuring the identity of the tag.

The random number is also used as a key and is sent from the tag to the reader unencrypted. Therefore, the random number may be intercepted by an attacker. However, the tag-to-reader link is much weaker than the reader-to-tag link, which reduces the probability that it can be intercepted. Transmitting the key in the clear from the tag to the reader is a trade-off between security and the cost of the tags. The reader encrypts the write, kill, and access commands to the tag using the 16-bit PRN from the tag. The reader requests a 16-bit PRN from the tag. The tag responds with the 16-bit PRN. The reader then encrypts the commands by performing a bit-by-bit exclusive-OR using the 16-bit PRN. The tag decrypts the commands with the same 16-bit PRN.

The 16-bit PRN security feature has been an issue of great concern among security professionals and academic experts. There is encryption of the data between the tag and the reader

1-4244-1280-3/07/$25.00 ©2007 IEEE

for some commands, but the key is sent in the clear. All the rest of the transmissions are in clear plaintext [2]. If an attacker is able to eavesdrop the PRN, then all communications between the tag and the reader as well any codes may be compromised. Without the advantage of eavesdropping, an attacker will have no choice but to attempt a brute force attack in order to gain access to the tag. Although there have been no known report of a brute force attack on the 32-bit Gen-2 tag password, brute force attacks on digital signal transponders and DST's have been reported [3].

In [3], the process of breaking the 40-bit security password for DST devices is discussed. These devices are used primarily in SpeedPass™, payment transponders, and automobile ignition keys. Using 16 FPGAs operating in parallel, a DST key in under an hour using two responses to arbitrary challenges was recovered [3].

Although Gen-2 tags are relatively new, companies are investing large amounts of man-power and resources to have it implemented in their systems. Smaller companies are also beginning to look at the technology, but they are waiting for companies who have the resources to finish implementing the system in order to take advantage of their mistakes and successes. If the proper security precautions are taken, then this technology can revolutionize many different industries.

C. Objective

The objective of this research is to simulate the average amount of time required to perform a brute force attack of the 32-bit Gen-2 password. The simulation will use the number of attempts that it takes to break a 32-bit password to estimate the time. This objective will be achieved through the use of a 32-bit password cracker program and simulation.

II. METHOD

In the Gen-2 tag there are multiple protocols used for communication security. First, Gen-2 tags generate a 16-bit pseudo-random number (PRN) to initialize sessions with readers, encrypt communication, and single-out a tag during multiple tag sessions. The PRN is sent in the clear from the tag to the reader upon request for communication. The PRN provides limited security because of the number of bits used, any RFID reader can receive their own private PRN, and attackers can eavesdrop on current sessions.

Gen-2 tags have two passwords stored in memory. The kill password is a 32-bit value whose default value is zero. A tag will not execute the kill command if the password is set to default. If the tag has a nonzero password, then the tag will permanently disable itself upon receiving the correct password. Gen-2 tags also have a 32-bit access password whose default value is zero. If a tag has this access password set, a reader must issue this password before transitioning the tag into the secured state. Otherwise, access is denied.

A brute-force attack can be implemented after a tag has been isolated and is in arbitrate mode. At this point, an attack can happen on either the access or kill passwords. An attack on the access password will result in a backscattering of the tag's handle upon success and the tag will be in an open/secure state. Once the tag is in an open/secure state, data can be altered or an attack on the kill password can commence. Conversely, instead of attacking the access password upon singulation, an attack on the kill password results in the backscattering upon success and the tag self-destructs becoming permanently disabled.

This brute-force attack can easily be simulated if the following items are assumed:

1. The equipment used for performing the attack is located near the desired target tag.
2. The target tag has already been singulated.
3. The attacker has enough time to perform the attack.

The simulation consists of two parts. One part generates 32-bit passwords to submit to the simulated tag. The second part estimates the amount of time given the number of attempts.

D. Program Details

The simulation program was designed using Qt v 4.1.0 by Trolltech. Qt is a GUI design suite, similar to that of Visual Basic, which allows for convenient GUI development. The suite allows for easy drag-and-drop placement of items and contains several different classes with many commonly used methods.

The program begins by asking the user which password to attack, followed by the number of tags that will be attacked. There is also a small group of options that will display additional data if the user wishes. A screenshot of the program's user interface can be seen in Fig. 1.

Fig. 1. Program Interface

Once executed, the program spawns a thread, which will randomly create all the necessary passwords and then commence to break them. The program keeps track of the

number of attempts it takes to break each tag; this information is used to calculate the actual time. Once the process is complete, the program displays the results. An example of a completed simulation is shown in Fig. 2.

E. Access and Kill Password Times

After studying the Gen-2 specification, the times to submit either a single access password or a single kill password were calculated. These times assume that the tag has already been singulated and is in the arbitrate state. The necessary transitions are shown in the simplified tag state diagram in Fig. 3.

In order to input a password, the tag must transition from the arbitrate state to the open state. This transition, which can be seen in Fig. 3, takes three commands from the reader, and those commands have the following bit lengths: QueryRep: 4, ACK: 18, and Req_RN: 40 [6]. At the open state a KILL or ACCESS command can be issued. The KILL command has a bit length of 59 and ACCESS has 56 [6]. If either one of those commands fail, then the tag reverts to the arbitrate state. Thus, two loops exist. The ACCESS loop requires 118 bits per cycle, and the KILL loop requires 121 bits per cycle. Now that the number of bits for the reader has been calculated, the number of bits transmitted by the tag per cycle is calculated.

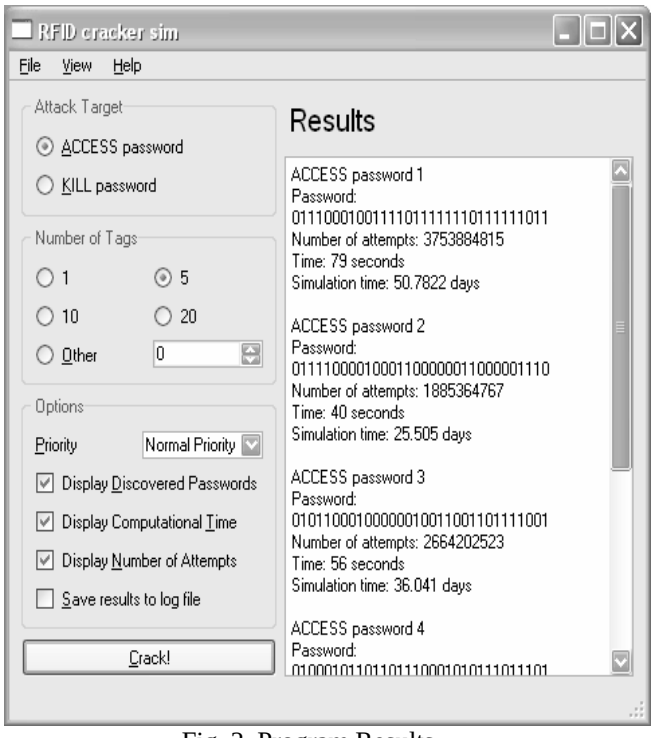

Fig. 2. Program Results

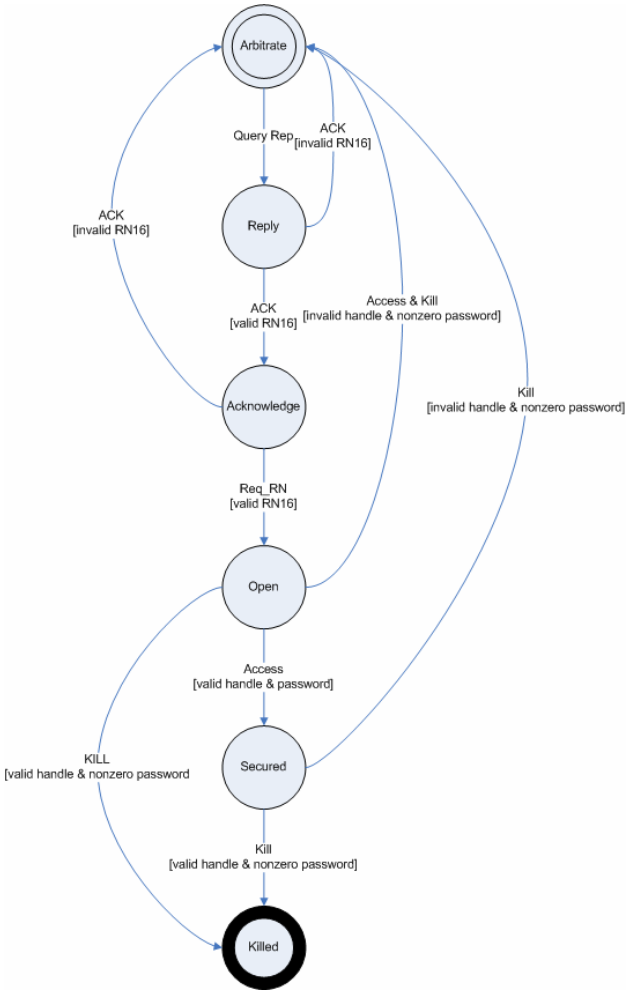

Fig. 3. Tag State Diagram

Typically, transmissions from the tag come in the form of a 16-bit value, which is known as the tags handle [6]. However, if the reader transmits a successful ACK command, the tag will reply with a 128-bit value, which contains the EPC number. Table 1 shows the bit length of tag replies per reader command.

Table 1
Bit length of tag replies per command

Reader Commands	Tag response bit lengths
QueryRep	16 bits
ACK	128 bits
Req_RN	16 bits
ACCESS/KILL	16 bits

This table shows that the total amount of bits sent by the tag are the same regardless of the attack target. Now the 176 bits from the tag are combined with the bit totals from the two command loops to determine the command loop bit lengths for the ACCESS and KILL commands and are shown in Table 2.

Table 2
Command Loop Bit Lengths

Command Loop	Reader bit length	Tag bit length
ACCESS	118	176
KILL	121	176

With the total command loop bit lengths, a per-loop time can be calculated by dividing both the reader and tag's bit lengths by their respective maximum bit rates (128 Kbps for reader-to-tag and 640 Kbps for tag-to-reader [6]), which yields the results in Table 3.

Table 3
Loop Times

Command Loop	Reader Bit Length/Rate (seconds)	Tag Bit Length/Rate (seconds)
ACCESS	0.0009002685546875	0.0002685546875
KILL	0.00092315673828125	0.0002685546875

Now column 2 and column 3 from Table 3 are combined to form a single time value for one command loop. The results from this calculation are shown in Table 4.

Table 4
Total Time per Loop

Command Loop	Time (seconds)
ACCESS	0.0011688232421875
KILL	0.00119171142578125

With these two values, there is now a means to calculate the amount of time it would take to break the 32-bit ACCESS and KILL passwords assuming the maximum bit rates.

III. RESULTS

The simulator was set to attack both the ACCESS and KILL passwords on 20 different tags. The ACCESS results are shown in Table 5.

Table 5
ACCESS password attack results

Tag	Days
1	56.0133
2	17.9144
3	47.9197
4	34.5349
5	3.3228
6	20.4434
7	43.4937
8	12.5332
9	11.5874
10	17.5844
11	32.6957
12	2.89707
13	30.446
14	42.6062
15	0.874612
16	55.9747
17	49.8665
18	42.7106
19	54.7748
20	15.868

These results yield an average time of 29 days to access a tag. These values show that it is possible to do a brute-force attack on an ACCESS password. The KILL password attack yields similar results, which are shown in Table 6.

Table 6
KILL password attack results

Tag	Days
1	28.9497
2	3.47507
3	20.068
4	15.2547
5	13.0617
6	13.4072
7	54.7896
8	55.4389
9	54.801
10	0.711883
11	27.8684
12	41.8597
13	40.3139
14	5.63918
15	50.7987
16	55.4209
17	41.0871
18	52.1404
19	4.43891
20	44.8941

The KILL results also show that it is possible to do a brute-force attack. The average time to kill a tag is 31 days.

IV. CONCLUSION

The average time to perform a brute force attack on the 32-bit ACCESS password of an EPCglobal UHF Class-1 Generation-2 tag is 29 days and on the 32-bit KILL password is 31 days. This assumes the maximum reader-to-tag link speed of 128 Kbps and the maximum tag-to-reader link speed of 640 Kbps. The Gen-2 specification permits the link speed to be slower for environments with more noise. The attacker must have access to the tag for a relatively long time to perform the attack. The tag can mitigate such a brute force attack if it throttles access and kill commands from the reader. For example, if the tag received three incorrect passwords it could go dormant for some amount of time before communicating again to extend the amount of time to perform the attack.

REFERENCES

[1] *EPCglobal Class 1 Gen 2 RFID Specification.* Alien Technology Corporation, tech specification, (2005). Available: http://www.alientechnology.com/docs/AT_wp_EPCGlobal_WEB.pdf

[2] *EPC Class 1 Generation 2 RFID Tag Specification Available Online.* Spy Blog. June 20, 2005. Available: http://www.spy.org.uk/spyblog/2005/06/epc_class_1_generation_2_rfid.html

[3] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo, "Security analysis of a cryptographically-enabled RFID device," in *Proc.14th USENIX Security Symposium*, Baltimore, MD, USA, July-Aug. 2005, pp. 1-16.

[4] D. R. Thompson, "RFID technical tutorial," *The Journal of Computing Sciences in Colleges*, vol. 21, no. 5, pp. 8-9, May 2006. Available: http://www.csce.uark.edu/~drt/pubs.htm

[5] N. Chaudhry, D. R. Thompson, and C. Thompson, *RFID Technical Tutorial and Threat Modeling*, ver. 1.0, tech. report, Dept. of Computer Science and Computer Engineering, University of Arkansas, Fayetteville, Arkansas, Dec. 8, 2005. Available: http://www.csce.uark.edu/~drt/rfid/

[6] *EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz*, ver. 1.0.9, EPCglobal Inc., Jan. 31, 2005. Available: http://www.epcglobalinc.org/.

[7] EPCglobal Inc., http://www.epcglobalinc.org/