A Weak Password Cracker of UHF RFID Tags

Zhentao Zhao[1,2,3], Shufang Li[2],Yang Kang[1,3], Jiankai Li[1,3],Shengguang Li[1,3],Weijun Hong[2]
1:First Research Institute of the Ministry of Public Security of PRC, Beijing 100048, People's Republic of China
2:Beijing Key Laboratory of Network System Architecture and Convergence, Beijing University of Posts and Telecommunications, Beijing 100876, People's Republic of China
3:Police Key Laboratory of IoT Application of the Ministry of Public Security of P.R.C
E-mail: 54zhaozhentao@163.com

***Abstract*—Under the ISO/IEC 18000-6C protocol of UHF RFID an electronic tag's information security is based on password protection, but its natural defect is unable to reject brute tests which can be exhaustive. By the protocol analysis, this article theoretically proves that tags' weak passwords can be cracked. Combined with a concrete Tag-Interrogator module a method for improving the cracking efficiency is given out with a special concise password library. Furthermore this paper implements the password cracker has carried on the exploration of distributed detection. By this method most electronic tags' passwords can be cracked within one week. The ultimate goal of this paper is to remind that UHF RFID industry projects should enhance the security level of tag's password practically.**

***Keywords*—UHF RFID ; password; crack; EPC Class1 Gen2 tag.**

I. INTRODUCTION

RFID is one of the key technologies of Internet of things(IoT). The RFID application of UHF frequency (860~960 MHZ) is to implement low cost, long distance, non-contact, fast pass-by, and large quantities of inventory "things connecting". The current main technical standard is ISO/IEC 18000-6C and GB/T 29768-2013. Limited by tags' storage capacity and computing ability, the current password security protection mechanism cannot prevent brute violence cracking. Once the password is conquered, the damage of the electronic tag will emerge: the information be stolen, counterfeited, copied (cloned) or tampered by illegal speaking, reading or writing equipment operation.

Reference [1] regularizes that a tag's memory is divided into the reservations (Reserved), Electronic Product Code label (EPC), Tag identification number (TID), and the users area (User), four independent storage banks. The Reserved area is used to store the kill password and access password.

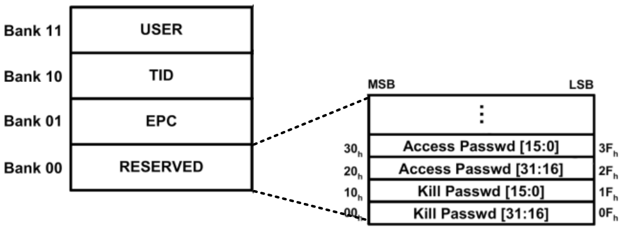


Figure 1. Four Independent Storage Banks of a Tag

An access password is a 32bit value stored in the Reserved from 20h to 3Fh, which is MSB first. The default (unprogrammed) value shall be zero. A tag with a nonzero access password shall require an interrogator to issue this password before transitioning to the secured state. A Tag may optionally implement an access password. A Tag that does not implement an access password operates as if it has a zero-valued access password that is permanently read/write locked. The interrogator may now issue further access commands. Tags in the open state can execute all access commands except Lock and BlockPermalock. A tag in open may transition to any state except acknowledged.

Under the EPCglobal Architecture Framework，the EPC Gen2 protocol specifies that each tag contains a secret 32bit access password. Any interrogator that wishes to access the data stored on a tag must authenticate itself by proving its knowledge of the tag's access password. This is usually done in the following manner: the tag first transmits its EPC to the

978-1-4673-7211-4/15 $31.00 © 2015 IEEE
DOI 10.1109/UIC-ATC-ScalCom-CBDCom-IoP.2015.283

interrogator. Based on the EPC, a legitimate interrogator can then retrieve the tag's access password from a back-end server through a secure channel and present the retrieved password to the tag [2].

Current password security mechanisms provide only 32 bits for Access Password and Kill Password. The majority of users are using the default Access Password "0000 0000", or as an extremely simple password, such as "2222 2222". The introduction of UHF password cracker is used to detect whether a RFID application in the project of the electronic tags by reasonable safety strength encryption.

This paper uses an access password as an example. Kill password is the same with it.

II. CRACK TECHNIQUES

From the initial design the Gen2 protocol has no mechanism to resist violence crack, so the effectual parameters can be altered to change the communication between a tag and an interrogator and a tag can be deciphered limitlessly. With sufficient times of crack and a correct crack strategy, the password can be cracked. This section demonstrates the parameters that can be modified to enhance the efficiency.

From subsections III-A to III-F main parameters are derived for reducing the crack time. Subsection III-G, mentions the confliction of the parameters.

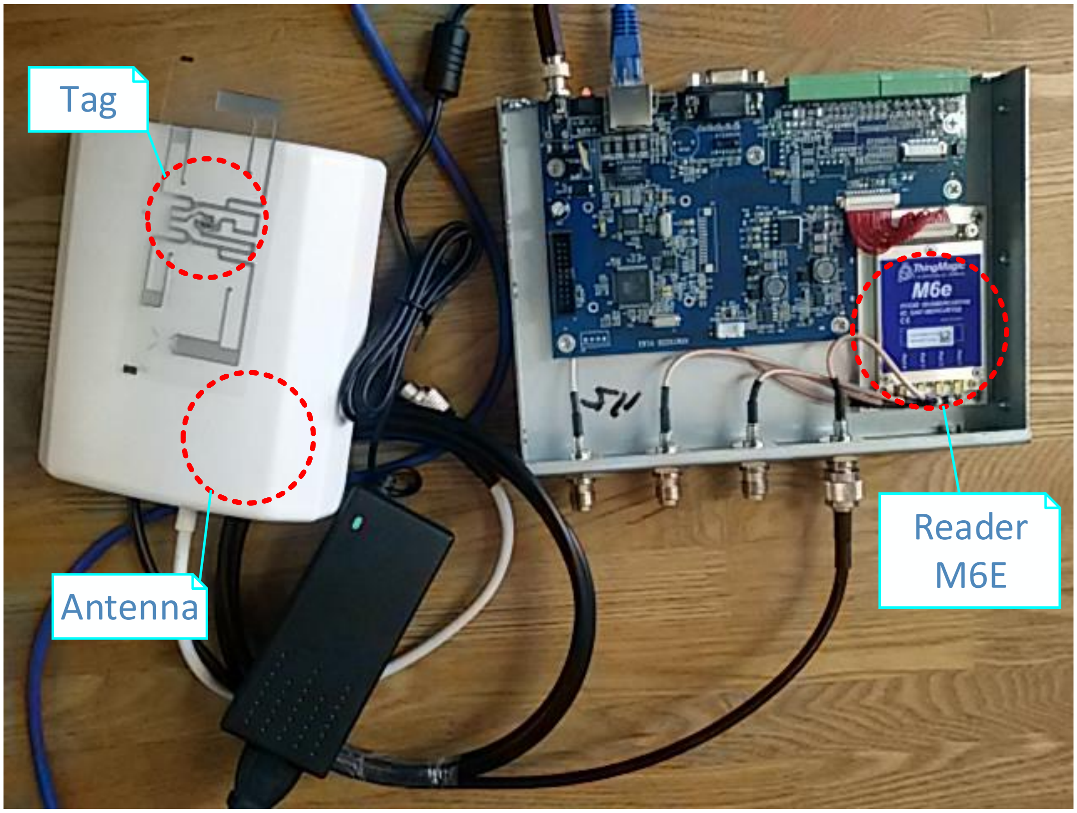


Figure 2.The Prototype of a Weak Password Cracker

The embedded UHF RFID interrogator module is Mercury6e (M6e) from Trimble Navigation Limited company which is based on the RF module R2000 from Impinj Limited. Most parameters of Gen2 are configurable. The used tag is the Alien A9640.

The most important and effectual parameters and their default values are：

Tari = 6.25μs; OpTimeout = 1000ms; Q = 4; BLF = 250kHz; Encoding Format = FM0; Gen2Session = Session0.

Each password test time (Time_PWD_Once) needs about 1050ms.If the password is tried out after 2^{32} times of traversal tests of all possibilities, the total password test time(Time_PWD_Out)is about 150 years. This could be considered as impossible, but according to the probability (according to III), the vast majority of passwords can be detected in the 2^{26} calculation. So the Time_PWD_Out could be reduced sharply to merely 3 years [3].

Figure 3 illustrates R=>T and T=>R link timing. The figure (not drawn to scale) defines Interrogator interactions with a Tag population. RTcal is defined as Interrogator-to-Tag calibration symbol whose value is 2.5 Tari $\leqslant$ RTcal $\leqslant$ 3.0 Tari; Tpri is the T=>R link period (Tpri = 1/BLF). An interrogator shall use a fixed R=>T link rate for the duration of an inventory round; prior to changing the R=>T link rate, an interrogator shall transmit CW for a minimum of 8 RTcal [1].

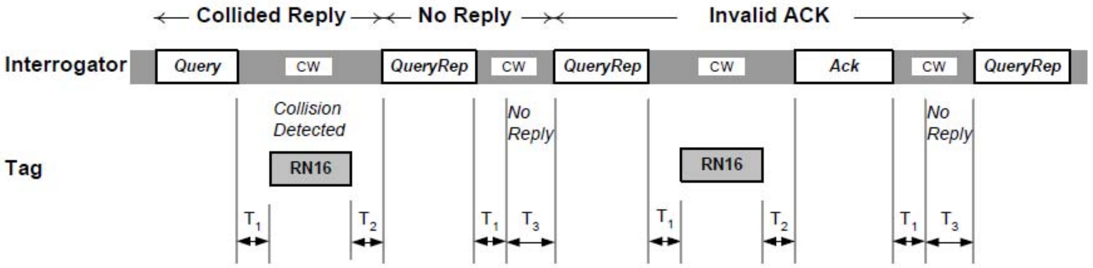


Figure 3. Link Time of An Interrogator and A Tag

T_1‘s nominal value is MAX(RTcal,10Tpri).

T2 is between 3.0Tpri and 20.0Tpri.

A. *Tari*

Tari is the reference time interval for a data-0 in Interrogator-to-Tag signaling. Interrogators shall communicate using Tari values in the range of 6.25µs to 25µs.For M6e the Tari’s option is 25µs、12.5µs or 6.25µs.

Obviously, the smaller of Tari the faster of inventory. So the choice of the value of Tari is 6.25µs which is the default value of M6e. So the Time_PWD_Once keeps as 1050ms.

B. *OpTimeout*

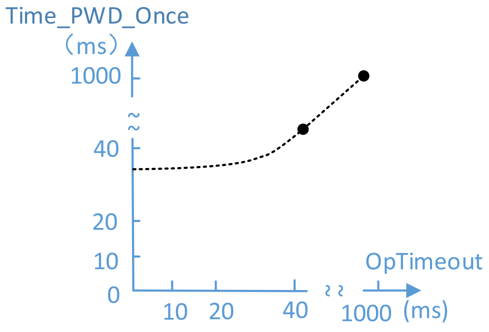


Figure 4. OpTimeout’s Effect to Time_PWD_Once

In M6e OpTimeout is the most dissipative time. OpTimeout means an interrogator’s blocking time when tag operation failed. The blocking time will be less than this time when the operation completes sooner. OpTimeout includes all the Query QueryRep, ACK, and Invalid ACK period whose default value is 1000ms.

According to figure 4,when reduced to 15ms, the effect is not significant.Thus the OpTimeout is modified to 15ms.

C. *Gen2Qvalue*

The inventory command Query contains a slot-count parameter Q. Upon receiving a Query participating Tags pick a random value in the range (0, 2^Q–1), inclusive, and load this value into their slot counter. Tags that pick a zero transition to the reply state and reply immediately.

As the collision will bring extra time loss, the Q value should be chosen as 0 to ensure only one tag to be inventoried each time in order to improve efficiency [4].

In M6e the default Gen2Qvalue is 4 .The value of Time_PWD_Once becomes 540ms while setting “Q=0”.

D. *Gen2BLF*

In M6e Backscatter-link Frequency (BLF = 1/Tpri = DR/TRcal) is chosen from 40kHz、250kHz、400kHz and 640kHz. Divide Ratio(DR) is chosen from 8 and 64/3 whose default value is 64/3. Here Gen2BLF=400kHz because Time_PWD_Once will be larger when Gen2BLF is 40kHz or 250kHz, while the inventory will be unstable when Gen2BLF is 640kHz.

E. *Encoding Format*

Tags encodes the backscattered data as either FM0 baseband or Miller modulation of a subcarrier at the data rate. The interrogator has four encoding choices:FM0、miller2、miller4 or miller8. FM0 inverts the baseband phase at every symbol boundary; a data-0 has an additional mid-symbol phase inversion [1].

TABLE 1. ENCODING FORMAT'S DATA RATE

Modulation type	Data rate (kbps)
FM0 baseband	BLF
Miller subcarrier	BLF/2
Miller subcarrier	BLF/4
Miller subcarrier	BLF/8

As shown in table 1, FM0 has the fastest data rate, so encoding format is kept as the default FM0.

F. *Gen2Session*

The Gen2Session option is Session0, Session1, Session2 or Session3 whose default value is Session0. For a large number of tags(more than 20) and slowly moving inventory operation, Gen2Session can be set to Session1. For a small amount of tags(less than 20) Session0 has the best effect. So Session0 is chosen.

G. *Parameters Competing*

The main parameters of Gen2 maybe affect each other. When the other parameters are determined, the range of a parameter value in not all optional, such as when BLF=40, Tari cannot be chosen as 6.25µs.

On the other hand, the configurations of the RF module of each manufacturer are different. For example BLF cannot be set as 640 kHz in M5e module of ThingMagic company, OpTimeout cannot be modified either. In order to get cracking efficiency, experimental test is essential.

III. PASSWORD LIBRARY

Access causes a tag with a nonzero-valued access password to transition from the open to the secured state (a tag with a zero-valued access password is never in the open state) or, if the tag is already in the secured state, to remain in secured.

If the entire received 32bit access password is correct, the tag transitioned to the secured state and backscatters its handle to acknowledge that it has executed the command successfully; otherwise the tag does not reply and returns to arbitrate.

Password dictionary is used as a series of brute password dictionary file. Only when the dictionary contains the correct the password it can be cracked [5].

The passwords in the password dictionary are accustomed to people .This can improve possibility of the code cracking and shorten the time to decipher a password. Tend to contain more possible passwords the password dictionary file is caused too large, even beyond the calculation capacity of the hardware. The work becomes meaningless if it need thousands of years to crack a password.

How to improve the efficiency and success rate of crack? A concise dictionary containing the passwords is the key.

According to the analysis of a website more than 5.9millions among all the 6millions of accounts use lightweight passwords which mainly comprise historical events memorial days, birthdays, phone numbers, QQ numbers, etc [7].

While UHF RFID has its own characteristics, according to the investigation of the current application of UHF RFID in more than 90% of the project in access password using the default zero. Secondly a tag’s access password structure is ACCEC0DEh. Each byte has only 16 values, range from 0~9 to A ~F. A lot of English words and Chinese pinyin cannot be used. So the possibility of using English words password basically ruled out. In the remaining RFID projects with the value of nonzero, the passwords are always used as a unified weak password [8].

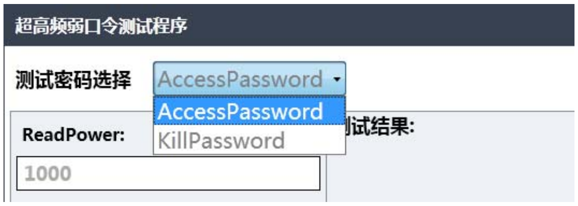
A weak password is the most simple and convenient memory code, such as a character of simple repeated: "3333 3333", "AAAA AAAA". According to the order of characters: "1234 5678", "ABCD ABCD", it is easy to guess. This fully shows that the of convenience method is not safe, safety is not easy. Password dictionary built the most common weak passwords, you can generate the weak password dictionary included, can be used in their weak password file into the special part in the dictionary, then generated again without operation [9].

With this simple password database, an efficient selection method is needed to enhance the selection speed based on the UHF RFID technology.

On the basis of chapter II, this paper also deals with the distributed brute force method. Within the same network, the password strength analyzers will automatically assign dictionary parallel cracking work. This method has achieved no more than 20 sets of parallel work. It can greatly shorten the time of crack. Most of the tags' weak passwords can be broken within one week.

IV. ACTUAL APPLICATION

When the RFID's oprational parameters are changed, the operation effect will be different, with different efficiency and different quality.



超高频弱口令测试程序

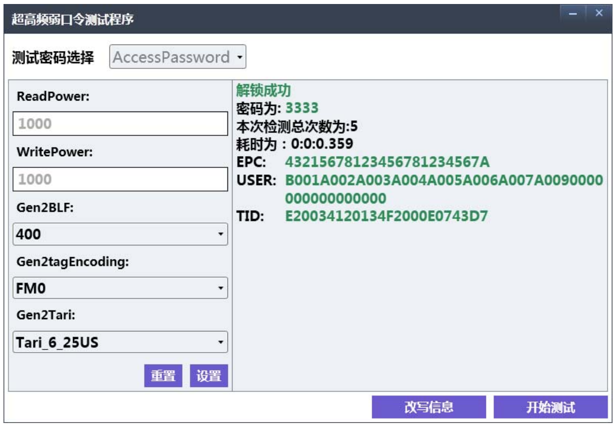
测试密码选择 AccessPassword

Figure 5. The Type of A Password

Figure 5 is about the design of the application software interface. Whether AccessPassword or KillPassword should be chosen first as AccessPassword is the default value.

As shown in Figure 6, ReadPower and WritePower meaning the interrogator power, have the range of 0-3100 (value of 0dBm-31.00dBm), suggesting that the current gray text for the interrogator to read the power.

When an unconformable parameter is inputted (for example: an alphabet), this will force the settings for the recommended configuration. This parameter will be forced to set to the default value.



超高频弱口令测试程序

测试密码选择 AccessPassword

ReadPower: 1000

WritePower: 1000

Gen2BLF: 400

Gen2tagEncoding: FM0

Gen2Tari: Tari_6_25US

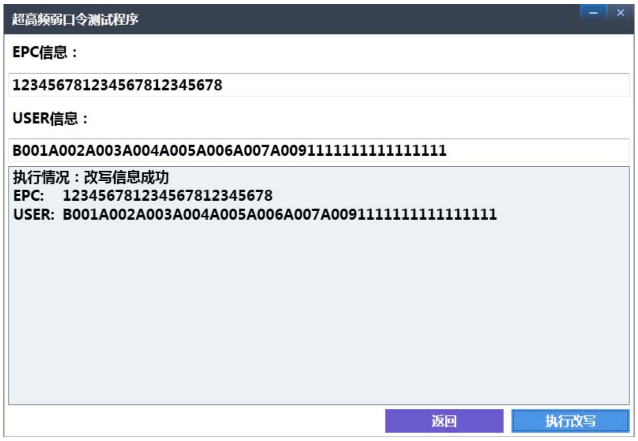
```
解锁成功
密码为: 3333
本次检测总次数为:5
耗时为：0:0:0.359
EPC:   43215678123456781234567A
USER:  B001A002A003A004A005A006A007A0090000
       000000000000
TID:   E20034120134F2000E0743D7
```

Figure 6. The Cracking Result of A Password

Place a tag within the control range of the integrator's antenna and click the start button of test software to test the password. When succeed the software will display the running password database name, the current execution time, and the remaining estimated time of the password database.

For a period of time, if the password is a weak password and is cracked, it will be shown in plaintext .The total tests number of and total test time and the label information are also displayed.

If the Password detected to be a weak password, users can also rewrite the EPC and USER tag information.



超高频弱口令测试程序

EPC信息：
123456781234567812345678

USER信息：
B001A002A003A004A005A006A007A0091111111111111111

```
执行情况：改写信息成功
EPC:   123456781234567812345678
USER:  B001A002A003A004A005A006A007A0091111111111111111
```

Figure 7. Rewrite the label information

Set a password that could be deciphered after 733 times of tests, and through repeated testing to decipher the password for the average time Time_PWD_Once.

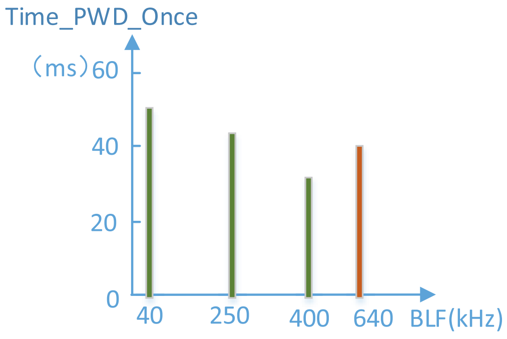


Figure 8. BLF's Effect to Time_PWD_Once

As shown in Figure 8, when Gen2BLF = 640kHz, the test result is Time_PWD_Once=[33.713~40ms], but it is not stable that sometimes it's unable to crack the password. So it is recommended that Gen2BLF = 400kHz as it could also get a pretty good and stable result.

V. DISCUSSION AND CONCLUSION

The above analysis illustrates that the electronic tag's password can be cracked, especially for simple weak password which can be cracked in a relatively short period of time.

As the UHF RFID technology fits for application projects in large quantity, therefore, even if the password is set to a slightly complex, but if you use the same password for so many tags, it can still be cracked by this cracker in distributed operation mechanism by using multiple UHF password strength crackers simultaneously. Once the password is deciphered, it indicates that the RFID network security management system will collapse.

In addition, in order to achieve reliable reading of electronic tags, the interrogator needs to increase radio power, but this time it is easy to cause electromagnetic interference. so it's needed to design a hardware structure that the tag can be placed in a closed magnetic field measurement environment.

For convenience, a weighted value of evaluation should be set, for example, "1" for the right. On the basis of this, users could know how to judge the strength coefficient of passwords.

In this paper the technology of the UHF RFID password strength is explored. Please don't do anything illegal activities. Remind you of not using weak passwords in important projects. Incidentally, this paper not only suggests the industry to upgrade the level of security when using password .At the same time, the author has designed a method to solve the security problem in the whole tag initialization and practical application.

REFERENCES

[1] EPCglobal Inc., "EPC radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz -960 MHz version 1.4", 2008.

[2] T. L. Lim and T. Li, "Addressing the weakness in a lightweight RFID Tag-Reader mutual authentication scheme", in Proceedings of the IEEE Int'l Global Communications Conference (GLOBECOM) '07, pp. 5963, Nov 2007.

[3] S. Karthikeyan, M. Nesterenko, "RFID security without extensive cryptography", in Proceedings of the 3rd ACM Workshop on Security ofAd Hoc and Sensor Networks, pp. 63-67, 2005.

[4] Tianci Liu, Lei Yang, Qiongzheng Lin, Yi Guo, "Anchor-free backscatter positioning for RFID tags with high accuracy",2013.

[5] Ertl, J.Plos, T.Feldhofer, M.Felber and N.Henzen, "A security-enhanced UHF RFID tag chip" ,Digital System Design (DSD), 2013 Euromicro Conference , 2013 : 705 - 712.

[6] L Leinweber, F G Wolff and C Papachristou. "A minimal protocol with public key cryptography for identification and privacy in RFID tags[C] "//International Symposium on Signals , Circuits and Systems, 2009(ISSCS 2009), 2009 : 1-4.

[7] M. H. Habibi and M. Gardeshi, "Cryptanalysis and improvement on a new RFID mutual authentication protocol compatible with EPC standard," in ICISC 2011, 2011, pp. 49-54.

[8] S.A. Weis, S.E. Sarma, R.L. Rivest and D.W. Engels, "Security and Privacy Aspects of Low- cost Radio Frequency Identification Systems",Security in Pervasive Computing 2003, LNCS, vol. 2802, pp 201212,Springer, 2004.

[9] P. Peris-Lopez, et al., "Cryptanalysis of a novel authentication protocol conforming to EPC-CIG2 standard", in Proceedings ofInt'l Conference on RFID Security (RFIDSec) '07, Jul 2007.