International Journal of Soft Computing 11 (1): 4-6, 2016
ISSN: 1816-9503

The Main Construction Principles of Access Control System Using Proximity Technology

[1]Zhukov Igor, [2]Mikhaylov Dmitry and [2]Dusha Igor
[1]Concern Radio-Electronic Technology, Ltd., Moscow, Russia
[2]MEPhI (Moscow Engineering Physics Institute), National Research Nuclear University, Kashirskoe Highway 31, 115409 Moscow, Russian Federation

Abstract: This study deals with the security issues linked with using contactless identifiers based on Radio Frequency Identification (RFID), providing controlled access, for example, into premises. Researchers, tell about the main problems occurring with the usage of such identifiers and disclose the basic methods of security increasing. The security level of many modern cards using RFID technologyis not significant. That is why this study includes the information about technical methods, organizational methods and cryptographic methods of information security.

Key words: Access control system, Radio Frequency Identification (RFID), contactless identifiers, proximity-card, security

INTRODUCTION

Nowadays Radio Frequency Identification (RFID) technology is very popular and it is used in different fields: science, technology and industry. A lot of scientific papers are devoted to achievements in RFID including Yang *et al.* (2013), Jadhav and Hamedi-Hagh (2011), Lee *et al.* (2011) and Wu *et al.* (2007).

At the present time, systems based on RFID play a very important role among access control systems. For example, Qiu *et al.* (2012) propose the way to improve the campus securities and obtain the personnel information and campus access control system. Al-Zewairi *et al.* (2011) tell about RFID access control systems without back-end database. Wu *et al.* (2010) present an access control system combining RFID-technology and face recognition based on neural network. Different ways to provide security are developed every day:

- Proximity cards (contactless access cards)
- Contactless smart-cards
- Mobile phones with NFC (Near Field Communication)

However, many systems remain vulnerable because RFID-cards can be cloned (Kasper *et al.*, 2011). Thus, it is necessary to analyze methods, improving protective properties of the system.

This study deals with the main principles that can be used to create on Access Control System (ACS) using Proximity technology.

ACCESS CONTROL SYSTEM

Nowadays proximity-cards are very popular in the market (Fig. 1) because they are used for remote (wireless) information exchanged. The proximity card can be active (card sends a signal) or passive (card reflects signals of a reader). In the first case, the card has its own power source. The main advantage of the proximity-cards is their practicality because they are hands-free and need no insertion in the reading device (Gebhart *et al.*, 2010; Lewis *et al.*, 2015).

However, the proximity-cards are not enough secure because an identifier can be easily copied (Bazakos *et al.*, 2005). It can be explained by the fact that the cards have been created not for objects authentication but for identification. Thus, security modules or encryption modules are not provided.

HID ProxCards II (Bazakos *et al.*, 2005) are thought to be safer then Em-Marine or Indala. It is necessary to understand that it is not actually true. All these cards provide the same functionality in information protection. Of cause, these identifiers are different andin some cases HID ProxCard II can be more reliable than Em-Marine or Indala. However, it does not mean that they are more secure. It does not matter for intruders what type of card (ProxCard II or Indala) is used in the system.

The next stage in RFID-cards evolution is encryption integration. Among analogs Milfare Classic has become the most popular product (Fig. 2). However, Crypto-1 Proprietary Cryptographic algorithm has been very weak

Corresponding Author: Zhukov Igor, Concern Radio-Electronic Technology, Ltd., Moscow, Russia

and was hacked after a while. Thus, these cards hinder malefactors to permeate to controlled territory but nevertheless they are not enough secure.

All identifiers described above hold about 90% of access control systems market. Thus, it is not very important what type of cards is used as identifiers. It is essential to provide additional logic for access control to increase security of the company. Let's consider the basic principles for ACS creation in details.

Some methods to prevent unauthorized access to the company (enterprise) are listed below. Any electronic ACS can use all these methods.

It is necessary to block the entrance to the Controlled Territory (CT) for the identifier which has been used by the other worker.

First, the intruder cannot use the identifier's clone. Secondly, if an unauthorized person enters the territory an operator will be informed in case an authorized person tries to use his real card.

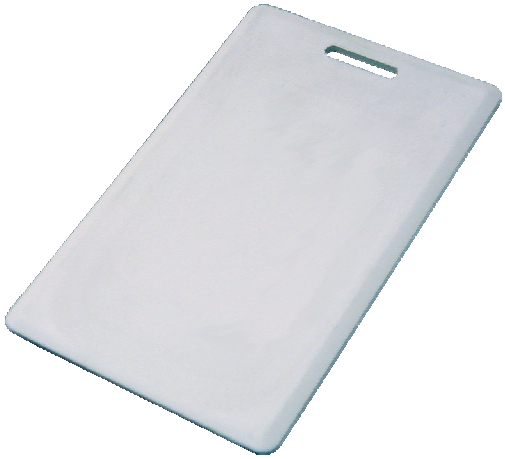

Fig. 1: General view of proximity-card

It is desirable to control not only the entrance to the controlled territory but the entrance-exit to/from any CT within the enterprise. We can consider this model multifrontier. Practical implementation of such method is simple and is not very expensive. However, it allows reducing the probability of unauthorized entrance to the controlled territory. A malefactor should find the identifier of a concrete person who has the access to CT.

It is essential to regulate employee's entering to the controlled territory in accordance with the working time. This practice is widespread. It is often used in software and hardware for unauthorized access protection. The employee should discuss additional working time with their superior (authority). This method combined with methods 1 and 2 gives almost complex protection against identifier cloning. Time frame which can be used by the intruder is greatly decreased.

It is necessary to use two-factor authentication in strategically important objects. The optimal variant is biometric authentication. And even if the card is cloned it is impractical to copy biometrical features and access the territory without revealing yourself. Let's list methods linked with cryptographic features and system setting with reference to RFID-identifiers.

Diversification of keys: It allows greatly increasing system security. An intruder will be able to read/write only one card. Data copying to the new card will not give any results. The system will not identify this card (other keys will be used).

Additional data encryption: It is not reliable to use integrated system protection if a card contains private information. It is especially true for Milfare Classic cards. It is necessary to use additional data encryption and record encrypted data on the card: "Never record unencrypted data".

		Byte number within a block															
Sector	Block	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Description
15	3	Key A						Access bits				Key B						Sector trailer 15
	2																	Data
	1																	Data
	0																	Data
:	:																	
1	3	Key A						Access bits				Key B						Sector trailer 15
	2																	Data
	1																	Data
	0																	Data
0	3	Key A						Access bits				Key B						Sector trailer 0
	2																	Data
	1																	Data
	0	Manufacturer data																Manufacture block

Fig. 2: Milfare classic 1k memory structure

Counter ambiguity: A counter on a card should not be obvious. It is possible to protect the system by sorting that can be submitted as transactions or linked with any additional data.

Blacklist: This rule can be named as a "gold" one. A system should keep a log of transactions. It allows detection of "suspicious" cards and putting them into the blacklist. Attempts to emulate the card will be detected with the help of log of transaction as well.

Elements of randomness: It often happens that all ID cards lie in a certain range. Thus, the intruder can restore all cards of the system with the help of the information about only one card. This is linked with the rule 3.

It is also necessary to notice some organizational requirements. The company staff should know that it is unacceptable to give a personal card to someone else. What is more, it is recommended to give all authorized users an opportunity to buy covers protecting against unauthorized access.

CONCLUSION

Thus, security issues linked with using contactless identifiers based on RFID-technology are presented in this study. Of cause, an enterprise can reach the higher level of protection. However, considered rules are enough simple to implement. They are effective to prevent most of unauthorized attempts to enter the controlled territory or premises. Other methods are more expensive or cannot provide an adequate level of security.

REFERENCES

Al-Zewairi, M., J. Alqatawna and O. Al-Kadi, 2011. Privacy and security for RFID access control systems: RFID access control systems without back-end database. Proceedings of the IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies, December 6-8, 2011, Amman, pp: 1-6.

Bazakos, M.E., Y. Ma and A.H. Johnson, 2005. Fast access control technology solutions (FACTS). Proceedings of the IEEE Conference on Advanced Video and Signal Based Surveillance, September 15-16, 2005, Minneapolis, MN., USA., pp: 312-317.

Gebhart, M., J. Bruckbauer and M. Gossar, 2010. Chip impedance characterization for contactless proximity personal cards. Proceedings of the 7th International Symposium on Communication Systems Networks and Digital Signal Processing, July 21-22, 2010, Newcastle upon Tyne, pp: 826-830.

Jadhav, G.N. and S. Hamedi-Hagh, 2011. UHF class-4 active two-way RFID tag for a hybrid RFID-based system. Proceedings of the IEEE International RF and Microwave Conference (RFM), December 12-14, 2011, Seremban, Negeri Sembilan, pp: 337-342.

Kasper, T., I. von Maurich, D. Oswald and C. Paar, 2011. Cloning cryptographic RFID Cards for 25$. http://www.proxmark.org/files/Documents/13.56%20MHz%20-%20MIFARE%20DESFire/Cloning_Cryptographic_RFID_Cards_for_25USD-WISSEC_2010.pdf.

Lee, M.H., C.Y. Yao and H.C. Liu, 2011. Passive tag for multi-carrier rfid systems. Proceedings of the IEEE 17th International Conference on Parallel and Distributed Systems, December 7-9, 2011, Tainan, pp: 872-876.

Lewis, A.M., G. Baldini and J.M. Chareau, 2015. Apodization method for standard load modulation amplitude measurement on proximity integrated circuit cards. Trans. Instrumentation Measurement, 64: 170-183.

Qiu, Y., J. Chen and Q. Zhu, 2012. Campus access control system based on RFID. Proceedings of the IEEE 3rd International Conference on Software Engineering and Service Science, June 22-24, 2012, Beijing, pp: 407-410.

Wu, D.L., W.W. Ng, P.P. Chan, H.L. Ding, B.Z. Jing and D.S. Yeung, 2010. Access control by RFID and face recognition based on neural network. Proceedings of the International Conference on Machine Learning and Cybernetics, Volume 2, July 11-14, 2010, Qingdao, pp: 675-680.

Wu, V., M. Montanari, N. Vaidya and R. Campbell, 2007. Distributed RFID tag storage infrastructures. University of Illinois at Urbana, Champaign, IL., USA.

Yang, P., W. Wu, M. Moniri and C.C. Chibelushi, 2013. Efficient object localization using sparsely distributed passive RFID tags. IEEE Trans. Ind. Electr., 60: 5914-5924.