Demo: WISP-based Access Control Combining Electronic and Mechanical Authentication

Yuanchao Shu
State Key Laboratory of Industrial Control Technology
Zhejiang University, China
ycshu@zju.edu.cn

Fachang Jiang
State Key Laboratory of Industrial Control Technology
Zhejiang University, China
fcjiang@zju.edu.cn

Zhiyu Dai
State Key Laboratory of Industrial Control Technology
Zhejiang University, China
derek88@zju.edu.cn

Jiming Chen
State Key Laboratory of Industrial Control Technology
Zhejiang University, China
jmchen@iipc.zju.edu.cn

Yu Gu
Singapore University of Technology and Design
Singapore
jasongu@sutd.edu.sg

Tian He
Dept. of Computer Science and Engineering
University of Minnesota, USA
tianhe@cs.umn.edu

Abstract

To bridge the gap between insufficiency of existing proximity authentication solutions and the increasing demand of high security guarantee for access control systems, we develope a WISP-based access control system combing electronic and mechanical authentication methods. In our authentication, encryption complexity is changeable and trusted users can share privileges with each other. During experiments, our system has achieved 95% authentication accuracy rate with up to 3 different users.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design

General Terms

Design, Experimentation, Performance, Security

Keywords

WISP, Sensor Networks, Authentication, Access Control

1 Introduction

Access control systems can be divided into two broad categories based on their underlying physical identification mechanisms. The first category based on mechanical matching includes keys and combination locks. However, due to physical constraints of mechanical matching systems, they are not secure enough for critical infrastructures. If a key is lost, access control to a designated space can be easily breached.

The other category of authentication for access control systems is electronic authentication including barcode, magnetic stripe, biometrics and etc. Compared with mechanical ones, the electronic proximity authentication such as smart card offers much more convenience and flexibility for both administrators and users of access control systems. However, it still suffers from similar loss of keys problem. Anyone who carries the card will be granted the access and the security of the system still can be compromised. Although various biometric authentication mechanisms have been introduced for further security enhancement, such methods as fingerprint, iris and voice recognitions have high infrastructure cost and cannot be transferred among trusted users.

This work was supported in part by NSFC No. 60974122 and SUTD-ZJU Collaboration Grant SUTD-ZJU/RES/03/2011.

SenSys'11, November 1–4, 2011, Seattle, WA, USA.
ACM 978-1-4503-0718-5/11/11

2 Authentication Method

The authentication system we design attempts to combine the best of both mechanical matching and electronic proximity authentication methods. The main idea of our system design is shown in Figure 1. A similar architecture is used in [1] for access control system description. Similar to mechanical matching methods, access control system users have to perform a series of predefined actions which are sensed and picked up by sensors integrated on access cards. Then the sensory data as well as encoded identification information on the card is sent to the network server through access control clients for authentication.

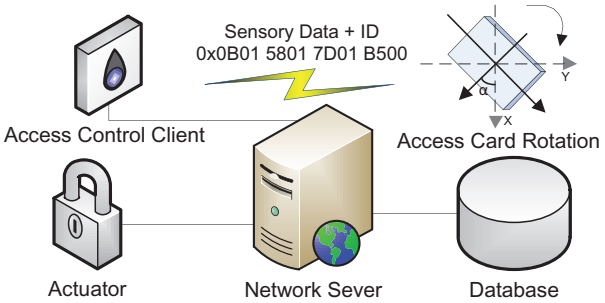

Figure 1. System Function Diagram

In our proposed system, we integrate accelerometers onto access cards for action detection. During rotations, we can determine the attitude of the accelerometer in a two-dimensional plane. Firstly in our authentication process, users have to perform a series of predefined rotations. Then the sensory data of accelerometer as well as the onboard ID information is encoded together into electronic product code (EPC) and sent to the network server. If both sensory data and

Table 1. KEY SPACE BETWEEN DIFFERENT k AND n

	$n=4, k=3$	$n=4, k=8$	$n=8, k=8$
Key Space	864	6718464	1.18×10^{10}

identification information match a valid record in the authentication database, the network server instruments the actuator and grants the card holder the access to the system. In this way, even an unauthorized personnel possessed an authentic access card or duplicated it illegally, as long as the card holder does not know how to generate the correct sensory data, he or she still cannot access the system thus the security of the system is successfully preserved.

In order to meet the need of security levels in different scenarios, one complete authentication consists of several basic rotations. Different number of basic rotations and granularities of recognition lead to a much larger key space and an adjustable encryption complexity. Table 1 summarizes possible key space for two-dimensional rotations with different number of basic rotation k and granularity of recognition n. From the table, we can see with just such simple rotations, key space can be significantly enlarged and therefore increases the security level of systems.

Different from existing authentication methods such as combining RFID and an additional keypad near the reader, our method could be adopted with minor modification of existing infrastructure. In fact, since sensory data and ID information are gathered into EPC, lots of work on authentication protocol and communication encryption in RFID system can be easily adopted into our authentication method, and therefore several security vulnerabilities such as replay attack and eavesdropping can also be well solved.

3 System Description

The prototype system we built consists of three parts including WISP-based access cards, access control clients and the server interface.

Access cards used in our system is built based on the Intel Wireless Identification and Sensing Platform (WISPs)[2]. WISP is a fully-passive ultra high frequency (UHF) RFID tag which integrates an processor and several low-power sensors such as accelerometer. Through WISP's antenna, the signal from standard UHF RFID readers can be used for both communication and powering the entire WISP. Due to the space constraint of cards, we reshaped the antenna of traditional WISP and optimized it under the licensed RFID frequency band in China. Figure 2 shows the comparison between our WISP-based access card and the original WISP.

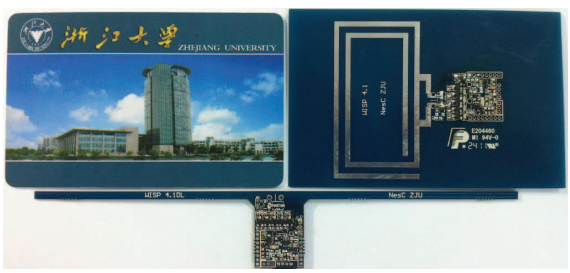

Figure 2. WISP-based Access Card vs. Original WISP

To further improve the communication quality between access card and RFID reader, we orthogonally placed 2 WISPs onto one card. In this way, two different orientated antennae ensure a more stable power supply and data transmission for our system. Data from two different accelerometers are complementary and consolidated for authentication. In our experiments, 50 complex rotations under each number of basic rotations k are designated to 3 volunteers (abbreviated as VLT in Table 2). Accuracy rates of authentication for each volunteer are reported in Table 2. Through experiments, we found the probability of simultaneous sensory data loss is reduced relative to that with only single accelerometer and average accuracy rates of all three columns are higher than 95%.

Table 2. ACCURACY RATE vs. DIFFERENT VOLUNTEERS WITH DUAL ACCELEROMETERS ($n=4$)

	k=1	k=2	k=3	k=4	k=5
VLT #1	100%	100%	94.0%	94.0%	96.0%
VLT #2	100%	94.0%	96.0%	100%	98.0%
VLT #3	98.0%	96.0%	94.0%	96.0%	98.0%

We use an Impinj Speedway Reader IPJ-R1000 as access control client. It powers the whole WISP-based access card and provides network connectivity between the card and the backend authentication network server.

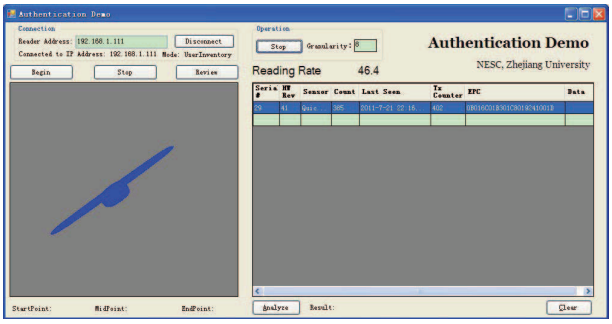

Figure 3. Authentication User Interface

Figure 3 shows the user interface of our system. Network interface of it is based on an open source of Impinj Reader Application [1]. During rotation process, realtime attitudes of access card are shown in the left part and communication details are listed in the right. Moreover, the demo GUI can reconstruct the whole rotation process and most importantly, we can obtain the matching result of sensory data user generated with records in the authentication database.

4 References

[1] I. Daradimos, K. Papadopoulos, I. Stavrakas, M. Kaitsa, T. Kontogiannis, and D. Triantis. A physical access control system that utilizes existing networking and computer infrastructure. *IEEE EUROCON*, September 2007.

[2] A. P. Sample, D. J. Yeager, P. S. Powledge, A. V. Mamishev, and J. R. Smith. Design of an RFID-based battery-free programmable sensing platform. *IEEE Trans. on Inst. and Meas.*, 57:2608–2615, November 2008.

[1] http://wisp.wikispaces.com/reader+application