2009 Fourth International Conference on Systems and Networks Communications

A Decentralized RFID Authentication Solution for Embedded Systems

Joel J. P. C. Rodrigues^{1,2}, Fábio D. Beirão^{2}, and Binod Vaidya^{1}
^{1}Instituto de Telecomunicações, Portugal
^{2}Department of Informatics, University of Beira Interior
Covilhã, Portugal
joeljr@ieee.org; fdbeirao@ubi.pt; bnvaidya@co.it.pt

*Abstract***— Radio Frequency Identification (RFID) and biometric technologies are promising technologies and are already widely used in applications such as building access controls. User authentication is an important mechanism for preventing unauthorized access. Even though we can use different user authentication mechanisms, using single kind of user authentication mechanism may not provide perfect reliable authentication because each of this mechanism has some disadvantages. In this paper, in order to obtain higher degree of security, we propose a decentralized authentication solution for embedded systems that combines both token-based and biometric-based authentication mechanisms. Our proposed solution is implemented and validated. We have obtained results confirming that the proposed solution provides better authentication.**

Keywords- RFID; Security; Biometric; Fingerprint system; Embedded Systems

I. INTRODUCTION

Radio Frequency Identification (RFID) [1] is a contactless technology used to identify or / and authenticate remote objects or persons, through a radio frequency channel using devices called RFID readers and RFID tags. This technology is one of the most promising of this decade and is already widely used in applications such as access cards, transportation passes, payment cards, and passports.

RFID technology thus races on at a pace that surpasses our ability to control it. The same ease-of-use and pervasiveness that makes RFID technology so revolutionary offers less-then-ethical characters unprecedented opportunities for theft, covert tracking, and behavioral profiling. However, without the appropriate control solutions, attackers can perform unauthorized tag reading. Snooping is possible by eavesdropping on tag/reader communications. Furthermore, adversaries can also manipulate RFID-based systems by either cloning RFID tags, modifying existing tag data, or by preventing RFID tags from being read in the first place.

Authentication is the process of positively verifying the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to the building or resources in the system. The authenticating entity accomplishes positive verification by matching some short-form indicator of identity, such as a shared secret that has been prearranged during enrollment or registration for authorized users.

The most ancient and basic forms of authentication are the traditional keys, where only the bearer of the key can have access. However, these mechanisms are not suitable for many environments such as modern building access control system. Major disadvantages of traditional key systems are that temporary staff or visitors have difficulty in the access and traditional keys can be easily duplicated by adversaries.

Information Technology (IT) has changed and enriched our lives in many ways. With the IT development, authentication and authorization have changed a lot. In any modern enterprise regardless of its size, a need for employee authentication is always in high priority. Whether it is for a building access control or system access control, every employee needs to authenticate himself.

For instance, in a typical building access control, many services may operate with the Mifare structure [2], that is, every card contains the information corresponding to the services its owner has access to: each sector, excluding the first one, refers to a service allowed to the card's owner; the specific data of each service are stored independently, that is, the user's data and reading/writing keys of a sector are chosen by the appropriate service provider.

One of the security challenges in the organization is handling with access for visitors or temporary employees – people with temporary access.

This paper presents a secure way for people (long-term and short-term employees and visitors) to authenticate themselves that can be used for a building access control.

There are three well-known user authentication mechanisms that allow a user to authenticate himself, within a certain degree of certainty: something he knows (knowledge-based, using for instance a password or a PIN), something he owns (token-based, using for instance a key card) or something he is (biometric-based, using a unique and recognizable biometric feature) [3].

While these three paradigms of authentication all provide certainty to a certain level, none of them can provide per-se a reliable authentication. In this regard, we can point out several disadvantages of such mechanisms. In case of knowledge-based mechanism, a password can be eavesdropped, thus allowing some third party to authenticate as a legitimate user; whereas in case of token-based mechanism, a token can be stolen, raising the same problem. Finally in case of biometric-based mechanism, a biometric feature can be mistaken by the system. For instance, disadvantage of biometric security using facial image is that

978-0-7695-3775-7/09 $26.00 © 2009 IEEE
DOI 10.1109/ICSNC.2009.65

the face can easily be disguised or even obstructed by hair, glasses, hats, etc. Similarly, capturing the iris of some individuals can be quite difficult which is the main disadvantage of such biometric security. An iris can easily be covered with eyelashes, contact lenses, eyelids or even reflections from the cornea.

Thus, in order to achieve a higher level of security, companies can use the combination of above-mentioned authentication paradigms, thus can create more trustworthy user authentication mechanism.

In this paper, we propose a decentralized authentication solution for embedded system that combines both token-based and biometric-based authentication mechanisms. This allows us to overcome the issue of increasing number of false positives, as the user processes a token with a template of his biometric feature, thus making the match a 1:1 match, which is the most reliable way to match a biometric feature. This solution is very easy to use and easily can be embedded in a decentralized system.

The rest of this paper is organized as follows. Section II presents the related work. Section III describes the design and realization of the system Section III describes proposed system construction, whereas Section IV presents implementation and validation. Finally, Section V concludes and presents the future work.

II. Related Work

Nowadays, there are many commercially available user authentication solutions using contactless card and a biometric feature. This section reviews the available approaches, where the solution proposed in this paper gathered contributions.

The miPASS Bio Series [4] offer a security solution by combining fingerprint scanning technology and encryption for secure user verification and authentication. In this solution, card holder's access control data and fingerprint template is encoded directly into the memory chip of the miPASS card, which is secured with encryption keys protecting the card holder's information from being compromised. And the Bio Series reads the cardholder's data from the memory chip of a miPASS card and only transmits to a door controller once a valid finger has been presented. As authentication is performed locally within the Bio Series reader, it does not require reference to a centralized database, thus improving performance by minimizing verification time and eliminating privacy concerns.

Futronic's FS25 USB2.0 Fingerprint Mifare Card Reader/Writer [5] can be used as standalone fingerprint matcher. Under the control of PC via USB interface, it can capture a fingerprint image, extract the minutiae (fingerprint characteristics) and then store to its internal memory. The stored fingerprint can be used to match with a freshly captured fingerprint and only the matching result will be sent to PC. So FS25 can do "Match On Device". Its internal memory can store up 100 fingerprints.

In the paper [6], the authors have proposed RFID (Radio Frequency Identification) biometric system for personal certification to communicate between machine-to-machine. This system stores extracted feature vectors from a facial image to each tag and performs a comparison and interpretation when facial image is inputted. The most prominent disadvantage of such biometric security is that the face can easily be disguised or even obstructed by hair, glasses, hats, etc. This reduces the reliability of such biometric security to a great extent. We believe that it is quite easy to deploy a system with fingerprint rather than a system with facial image.

Next section describes the proposed solution and identifies the system key issues in detail.

III. Proposed System

This section depicts the proposed system focusing on its main components and describes the hardware used on system construction. A comparison with existing solutions is also included.

A. System Construction

The main idea of this project is to construct a decentralized (central database and server independent) system for user authentication that can be used for the building access control.

As mentioned earlier, this can be accomplished through three different mechanisms: knowledge-based authentication, token-based authentication and ID-based.

The ordinary automatic access control systems normally use a card (RFID or smartcard) [7] to identify the employees. These systems can be easily deceived because the employee can be separated from the card and registration may be made by other person.

In biometric technology, users do not have to memorize any codes, neither to carry any token. Biometric systems are more reliable because their characteristics cannot easily be duplicated, lost, or stolen [8].

Being the most stable biometric characteristics, fingerprint authentication [9] can be used to prevent unauthorized physical access to the building or logical access to the system. Fingerprint authentication has the several advantages over the traditional password, smart card, token, etc, in terms of security and convenience. Main advantages are the following: fingerprint cannot be stolen by others; it would not be forgotten; and it is with the user/owner all the time.

In this project, two of the above authentication methods are combined: token-based and ID-based authentications. This is accomplished by using RFID capable cards and a biometric feature, fingerprints. The proposed configuration is shown in Figure 1.

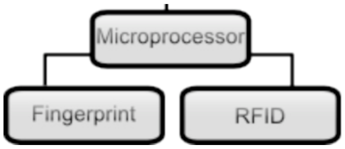


Figure 1. Proposed system configuration.

For this purpose, we have used a programmable microprocessor – Peripheral Interface Controller PIC24, Mifare card reader and fingerprint reader.

B. *Hardware Used*

The main components used to build the above-mentioned solution were carefully selected in order to attain the expected results, and they are identified and described below. Each main component of the system may easily identified in Figure 4.

The microcontroller we used is a MicroChip [10] PIC24 (PIC24FJ128GA010). PIC24 devices are designed as general purpose microcontrollers which has following features hardware MAC (multiply-accumulate), barrel shifting, bit reversal, (16x16)-bit multiplication and other DSP operations, hardware support for loop indexing, and direct memory access.

We used a Microchip Explorer 16 Development Board populated with a PIC24 microcontroller as the basis for this project, which allows an easier communication and power supply.

Since the keen interest toward contactless technology, many smart card manufacturers developed low-cost RFID products such as Mifare chips.

For the Mifare device, we have used a GemAlto [11] Prox-C2 (formerly known as GemAlto GemEasyLink300). The Prox–C2 is small contactless proximity card reader/writers having a built-in reader/writer and an internal antenna. They are used for any contactless applications such as access control, transportation, identity, banking services and vending machines etc. These devices have a reading range up to 4cm.

In case of the biometric reader, we have used a Suprema [12] UniFinger SFM3010FC. The UniFinger modules provide complete fingerprint solutions by incorporating fingerprint sensor interface and embedded fingerprint recognition algorithm into a half business card sized module.

As UniFinger modules are autonomous, they are easy to integrate in an embedded solution. The modules can store more than thousands of fingerprints in its internal memory and provides a full features of biometric functions. They have proven to be extremely reliable and produce a very satisfactory matching mechanism.

Also, Suprema UniFinger is modular enough to allow us to replace the fingerprint reader itself on-the-fly. This allows us to implement the appropriate reader to each scenario where we wish to implement our solution. Hypothetically, if an optical fingerprint sensor is not providing a satisfactory recognition, we can quickly replace it with a swipe sensor, or a thermal sensor.

C. *Comparison with existing solutions*

The miPASS Bio Series [4] and Futronic's FS25 [5] are examples of the existing solutions for user authentication and access control. However, miPASS Bio Series do not support a feature of optional cards. In case of our proposed solution, we have additional feature of optional cards, thus providing an easier utilization of the service.

Furthermore, due to the modularity of this proposed system, we can easily replace the fingerprint reader module by another sensor, such as a swipe or a thermal sensor. This allows the implementation of our proposed solution in a vast range of scenarios. It is also important because some places are more susceptible to finger deterioration.

Regarding Futronic's FS25 system [5], as it requires a USB2.0 connection to a personal computer (for power and to match 'OK' signal), it is quite inconvenient to use. In comparison with this approach, the proposed solution is power independent, using two common AC transformers to power all the devices and providing a logical signal for the correct match.

IV. Implementation and Validation

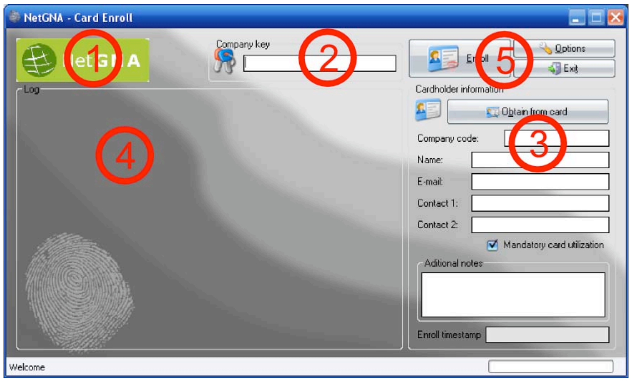
The methodology used to test and validate the proposal is based in a prototype. The above-describe hardware was used to create to perform the complete user authentication in a given embedded system. This section addresses the prototype implementation and corresponding solution validation.

The Peripheral Interface Controller (PIC) device was programmed in C language. All communications with the Mifare and Fingerprint devices is done through RS-232 serial interface. As this PIC only provides one serial connection, we created a new RS-232 serial interface and inserted it in the expansion slot available on PIC.

We have integrated both Suprema's UniFinger protocol and GemAlto's GBP protocol in our solution. All these implementations are done both in the PIC software and in the enrollment software developed in C#. A snapshot of the enrollment software is presented in Figure 2. This application software allows the configuration and control of each card profile and also performs card enrollment.

As may be seen in Figure 2, there are several features supported by the enrollment software, which are as follows:

1. Company's logo – can be personalized, from company to company.
2. Company's passphrase for generating the Mifare secret keys.
3. Personal information can be stored inside the Mifare card. We can provide information such as: Company ID, Name, email ID, two contacts, and additional notes. Here we can also specify if this is an obligatory card.
4. This is the log zone, where the system informs the user about its' status and asks him to take actions such as place finger in reader, place Mifare card close to the reader.
5. In this section, the Enroll, Quit and Options buttons are available. Inside Options menu, there is an option to recover the Mifare card – if possible – in case it was damaged while enrolling.



☑ Mandatory card utilization

Figure 2. Snapshot of the Enrollment software.

In this solution, when a card is enrolled, a user can specify whether its use is mandatory or optional. This is used to create two profiles: visitor or employee. It is assumed that visitor profile must use fingerprint reader each time uses the system. For an employee profile, after the first successful matching, the system stores the fingerprint template inside the Suprema fingerprint module, so the card-holder may authenticate using only his enrolled fingerprint. However, for the temporary visitor profile, fingerprint template is not stored inside the fingerprint module, following the system requirements.

Figure 3 illustrates the flow diagram with the operation of the system implementation. From the Figure 3, it can be seen that both the Mifare and fingerprint devices are in infinite loops (guarded by inside watchdogs). The Mifare device constantly reads and waits for a valid card (if the keys registered in the device match the ones in the card, it is considered valid) and reads the enrolled fingerprint.

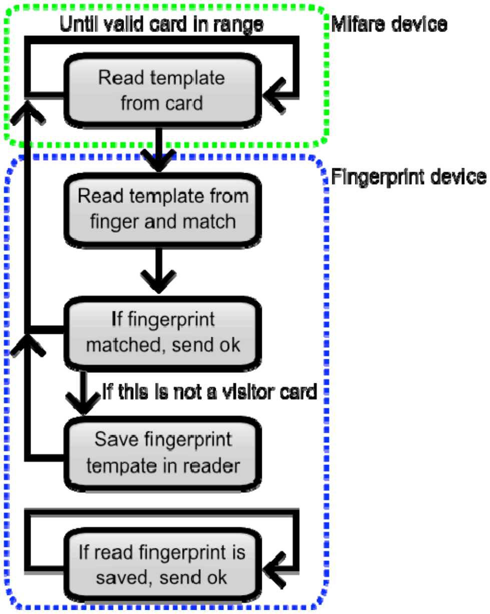

Until valid card in range
Mifare device
Read template from card
Fingerprint device
Read template from finger and match
If fingerprint matched, send ok
If this is not a visitor card
Save fingerprint tempate in reader
If read fingerprint is saved, send ok

Figure 3. Operation of the System implementation.

After reading the fingerprint, the microcontroller PIC24 sends it to the Mifare device for matching. When fingerprint template matches, this device also sends the final Ok. The matching algorithm is Suprema's proprietary. If the microcontroller PIC24 receives the information that the fingerprint was successfully matched, it checks whether this card has a visitor profile or not. If the card's profile is optional, then the microprocessor re-sends the template to Suprema's device, requesting its registration into its internal memory. This allows for the fingerprint device to match any read fingerprint against those on its memory.

Figure 4 shows the complete solution of user authentication mechanism using both contactless card reader and fingerprint reader. As may be seen, Figure 4 presents the above-described main components: (1) GemAlto Mifare reader and Mifare card; (2) Suprema Fingerprint device and fingerprint reader; and (3) Microcontroller Board.

For the validation of our user authentication solution, we have created several user profiles for both permanent users (employees) and temporary users (visitors). Exhaustive experiments were performed on both permanent users as well as temporary users. The experiment results show that our user authentication solution works perfectly for both profiles. In this regard, our proposed user authentication solution provides higher level of security, which can be used in many applications such as building access controls.

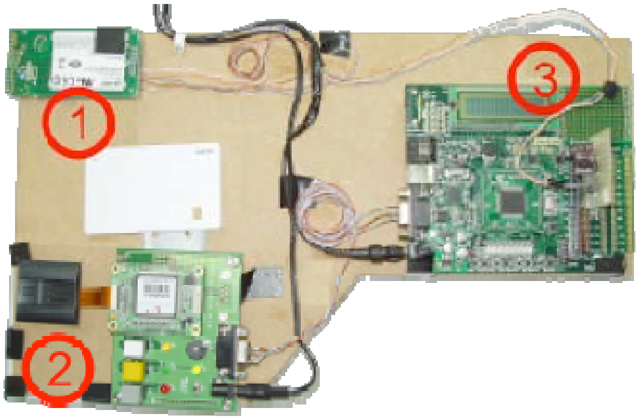


Figure 4. Complete User Authentication Solution

V. Conclusion and Future Work

Even though three well-known user authentication mechanisms such as knowledge-based authentication, token-based authentication and ID-based can be used to authenticate user himself/herself, none of them can provide complete reliable authentication. To achieve a higher security level, the combination of well-known authentication mechanisms can be used such that we can construct better and more trust worthy authentication solution.

This paper proposed a decentralized authentication solution for embedded system that combines both token-based and biometric-based authentication mechanisms. We have implemented and validated the solution with several user profiles. The obtained results demonstrate that our solution provides high level of security.

Nevertheless, there are still some security issues to be addressed, as in the current implementation, any company card send an 'OK' signal in every reader the company mounted. As we have reserved about 100Bytes in the Mifare card, it would be possible to implement Mifare-only authentication in some company sections, due to the low cost of the Mifare readers.

In the future, we will enhance our solution to provide more restricted access control mechanism.

ACKNOWLEDGMENTS

Part of this work has been supported by the *Instituto de Telecomunicações*, Next Generation Networks and Applications Group (NetGNA), Portugal, and by the Euro-NF Network of Excellence from the Seventh Framework Programme of EU.

REFERENCES

[1] Tristram Carlisle, "Radio Frequency Identification - RFID…Coming of Age," Information Technology Association of America (ITAA), June 2004.

[2] MIFARE. net, http://mifare.net. Accessed in May 2009.

[3] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proceedings of the IEEE, vol. 91, No. 12, Dec. 2003.

[4] The miPASS Bio-X Series, http://www.bqtsolutions.co.uk/suite-of-security-products/mipass-access-devices/mipass-bio-x-series.html. Accessed in April 2009.

[5] Futronic's FS25 USB2.0 Fingerprint Mifare Card Reader/Writer, http://www.futronic-tech.com/product_fs25.html. Accessed in April 2009.

[6] JY Lee, MK Jeong, YH Kim, and DS Kang, "An Implementation of the Personal Authentication System for USN", Advanced Intelligent Computing Theories and Applications. With Aspects of Contemporary Intelligent Computing Techniques, CCIS, Vol. 2, 2007, pp 771-778.

[7] A Qaiser and SA Khan, "Automation of time and attendance using RFID systems," 2nd International Conference on Emerging Technologies, 2006.

[8] MKH Leung, ACM Fong, and SC Hui, "Palmprint verification for controlling access to shared computing resources," IEEE Pervasive Computing, 2007.

[9] Y Gil, D Ahn, S Pan, and Y Chung, "Access control system with high level security using fingerprints," Proc of the 32nd Applied Imagery Pattern Recognition Workshop (AIRP'03), 2003.

[10] MicroChip PIC24 microcontroller, http://www.microchip.com. Accessed in April 2009.

[11] GemAlto Prox-C2, http://www.gemalto.com. Accessed in April 2009.

[12] Suprema UniFinger, http://www.supremainc.com. Accessed in May 2009.