ACCESS CONTROL SYSTEM BASED ON RASPBERRY PI AND ANDROID SMARTPHONES

Jonay Suárez-Armas and Pino Caballero-Gil

Department of Computer Engineering and Systems,
University of La Laguna, Tenerife, Canary Islands, Spain

ABSTRACT

In venues where there are restricted access areas, access control systems that work by entering a code or with some extra element such as a card are used. This paper proposes an access control system based on controlling each restricted area using a Raspberry Pi with an NFC reader, in addition to using Android smartphones emulating an NFC tag as an identification method thanks to an application for these devices. The management of the system is performed through a web panel that also allows to view all the data. Moreover, the system is based on the role access control model. In order to protect the information exchanged between the different elements of the system, security mechanisms are used.

KEYWORDS

Security, Access control, NFC, Host-based Card Emulation

1. INTRODUCTION

For many years, physical security in different environments has been a matter of concern for people, and different alternatives have been sought to prevent the entry of unwanted people into certain places, such as homes, businesses or restricted areas within a building. With this aim, alarms and video surveillance systems have been installed in the most exposed places. If apart from detecting the intrusion of someone in an area, we want to prevent someone from entering, or that even some people can enter and not according to which zone, we talk about access control systems.

In large venues where there is a large number of people, like airports, it is not feasible to use simple keys to access the different areas, either because of the great number of copies of keys that would be circulating or because of the time it would take to request them. Therefore, access control systems are used in these places, which may have different methods of identification, such as the introduction of a number code, or even the introduction of a card in a reader. Another advantage of the access control system is to have a log with all access attempts, whether they have been allowed or not to pass.

In order to improve the current access control systems, this paper proposes a system based on the use of a Raspberry Pi for the control of each area and connected with a server that provides them with the necessary information about the access permissions that the users have in real time, each time a user tries to enter an area. In addition, the system is complemented by the use of Android

David C. Wyld et al. (Eds) : CNDC, DPPR, AIAA, WiMNET, ACITY - 2017
pp. 25– 32, 2017. © CS & IT-CSCP 2017 DOI : 10.5121/csit.2017.71603

smartphones as an identification device in each zone thanks to the NFC Host-based Card Emulation (HCE) mode [1], available for Android devices with version 4.4 or higher, and also thanks to an NFC reader that incorporates each Raspberry Pi.

The next section shows some related works. The details of the system architecture are explained in Section 3. Section 4 describes the designed applications while Section 5 exposes the security mechanisms used to protect the information exchanged between the elements of the system. Finally, a short conclusion closes the paper.

2. RELATED WORKS

Apart from access control systems that can be found in stores, there are different works that address this issue in order to try to design a good access control system with low-cost and usable. One of the trends that currently exists is to use low-cost minicomputers, such as Raspberry Pi or Arduino, to create small access control systems that can be installed in homes. In [2], the authors propose an access control system in which a Raspberry Pi is used to control the access to a house via the Internet, with the ability to view who wants to enter thanks to a camera and also to send a message through a small screen. In [3], a system security with Raspberry Pi has been designed, which is based on image recognition with extra functionalities, such as sending intrusion e-mails to the nearby police department or sending notifications via SMS. There are also works about access control that use an Arduino board with an NFC reader that allows reading NFC tags with the access credentials needed to access a zone [4] or even replace these tags with Android smartphones that are able to simulate an NFC card [5]. The NFC cards emulation on Android mobile phones [6] [7] is also a topic studied by different authors because of the advantages of being able to leave the cards at home and do different operations simply swiping the mobile phone to the reader, or even with an NFC-enabled smartwatch.

In access control systems, it is possible to use different identification methods. These methods can be classified into 3 groups: identification using something that is known, identification through something that is, identification using something that you have. The identification using something that is known is the most used method, since the passwords are in this group. In the second group, identification through something that is, fingerprint identification [8], identification using facial recognition [9] and identification based on iris analysis [10] are included. In the identification using something that you have is where the identification using NFC [11] cards fits in. To make a system stronger, it is possible to combine two identification methods of two different groups, for example the use of an NFC card together with the fingerprint. Authentication with NFC is also studied in some works [12] [13].

3. DESCRIPTION OF THE SYSTEM

The designed system is composed of some elements. The interconnection between them is in Fig. 1. The connection between the user's smartphones and the server is through the Internet, and the connection between the server and each Raspberry Pi is through Ethernet, or even through a Wireless LAN connection in areas without LAN connection.

The server is the centre element and is the brain of the system. It contains all the data needed to manage the access to the restricted areas, and the web panel of management is lodged in it. This element is connected with the other elements of the system in order to give them the necessary information.

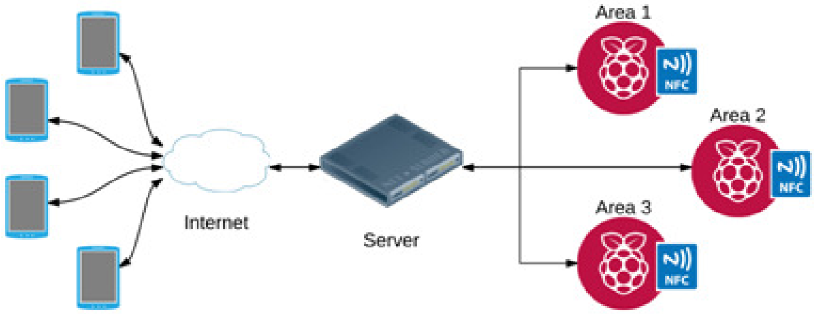

Figure 1. System architecture scheme

Another essential element of the designed access control system is what we will call area control subsystem, because it is composed of different elements managed by a Raspberry Pi. In each restricted area, there will be an area control subsystem. This subsystem consists of a Raspberry Pi together with an NFC reader (MFRC522), a 16x2 LCD display to indicate some information to the users, a green LED to indicate that access has been allowed and a red LED to indicate otherwise, a camera to capture images of people who have accessed the different areas, and a relay that allows the connection of the Raspberry Pi with the door opening system of the controlled area. In Fig. 2, the connection scheme of the Raspberry Pi with the different elements that make up the area control subsystem is shown.

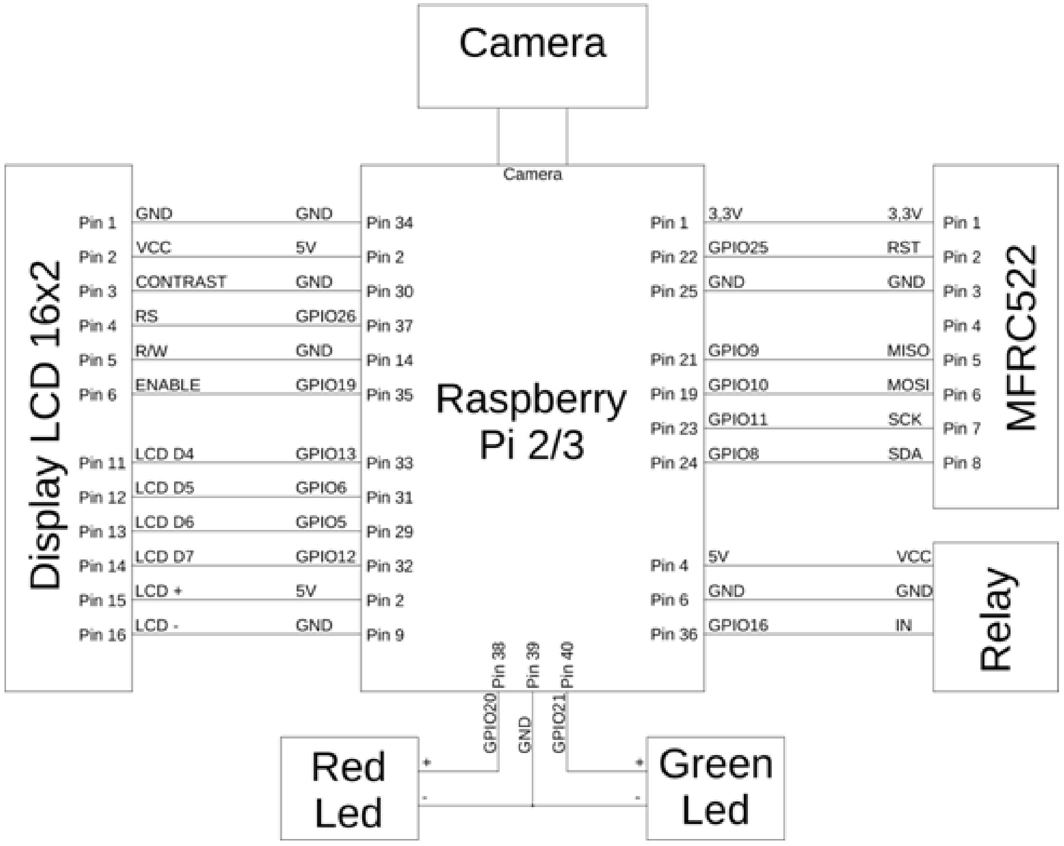

Figure 2. Raspberry Pi connection scheme

The last point of the system is composed of the users' own mobile phones. These Android smartphones are NFC-enabled and they have a version of Android 4.4 or higher, from which the NFC Host-based Card Emulation (HCE) tag emulation mode is available, which allows to emulate an NFC tag on the mobile device, so by bringing the phone closer to an NFC reader, the user requests to access an area. To do this, each of these phones will have an application installed that allows you to connect to the system server to gather the necessary information and then to be able to be identified in each restricted area.

3.1. Role access control model

To improve the granting of permissions, the system is based on the roles access control model [14], in which permissions are not granted to each user, but assigned to a role, and then roles are assigned to system users.

This is an advantage, since it is not necessary to manually assign the permissions to each user, so that if a series of permissions are repeated for several users, they are only assigned once to a role, and then the created role is assigned to the corresponding users. In addition, it is possible to assign several roles to a user, so it is not necessary to modify a role that affects several users, but you can create a new one that will be complemented with those already assigned.

To avoid permissions conflicts, in the designed system permissions are not denied, because by default users do not have any permissions. In this way, when assigning several roles to a user the system does not have to decide whether to allow or deny an access, since all of them would be positive permissions.

4. APPLICATIONS

Three applications have been designed to make up the system: server application, Raspberry Pi application, and Android application.

The web application hosted on the server is in charge of the control of the system, and could be divided into two parts. On the one hand, there is the application in charge of communications with other elements of the system to provide them with the information they need at any time, especially the information of permissions of users each time an access attempt occurs. On the other hand, there is the web panel that allows administrators to perform different system configurations (user creation, role creation, role and permissions assignment) and monitor the access attempts of each area.

The application of Raspberry Pi is responsible for making the communication with the server every time a user approaches his mobile phone to try to access a controlled area. In that communication, it queries if said user has permission to access said zone. It is also responsible for operating the NFC reader, opening the door if necessary and controlling the other elements that are connected.

The application installed in the mobile phones of the users is responsible for establishing NFC communication with the Raspberry Pi of each controlled area. In addition, it connects to the server through an Internet connection to request the access credentials that are sent through NFC when a user tries to access a restricted zone. For security reasons, NFC communication only occurs if the device is unlocked, preventing another person from accessing an unauthorized area using a third-party phone. Through this application it is also possible to view your own access logs.

4.1. Operation

The typical operation mode is divided into several steps (see Fig. 3):

1. From the management web panel, users must be created in the system so that they can get identification data from their Android mobile phones.

2. To assign corresponding permissions to the users created previously. On the one hand, permissions to enter the web panel for reading data or even to modify it will be assigned, and on the other hand restricted areas access permissions will be assigned. The permissions assignment is based on the role access control model previously mentioned.

3. In the Android application, every user must introduce their username and password to get the identification data and to be able to use the system.

4. The mobile phone is set in emulation tag mode and is ready to establish a communication with the NFC readers of each area.

5. Swiping the smartphone by an NFC reader, the system checks if the user has permission to access the corresponding area.

6. The door is opened if the user is authorized.

7. The access attempt is registered and saved in database whether the user could access or not to the restricted area. The data recorded on each attempt are: date and time, user, user's photo, area, and if access has been allowed or denied.

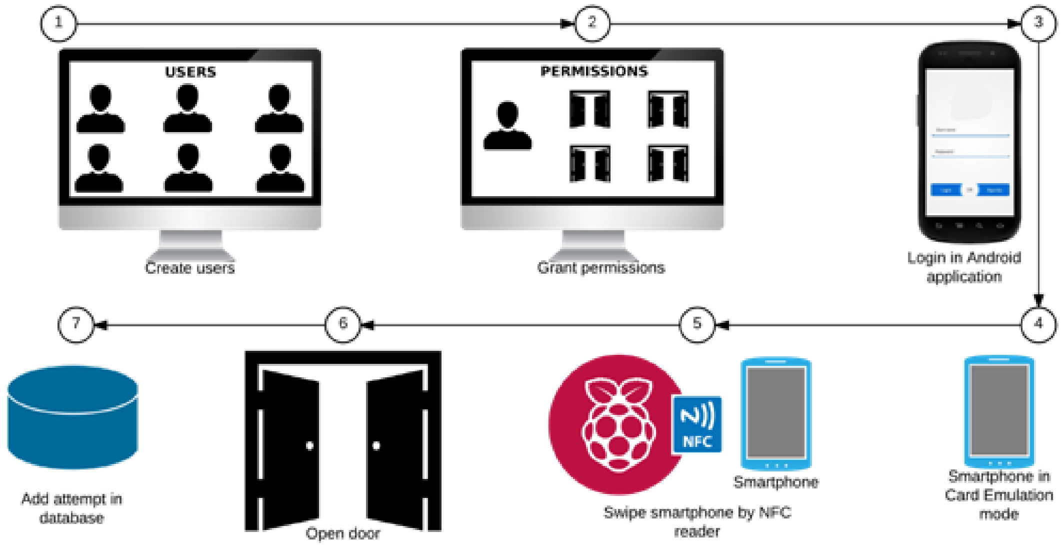

Figure 3. Operation mode

5. SECURITY

An access control system is a platform dedicated to the physical security of a venue, so the logical security is an essential part of the system. For this reason, the corresponding security mechanisms are used to protect each part of the designed system. In Fig. 4 the mechanisms chosen in each part are shown.

First, the communications between the server and the web application that manages and monitors the system, are protected by the use of HTTPS. This protocol is also used to protect the exchange of information between the server and the Raspberry Pi of each restricted area.

On the other hand, is the information that is sent between the server and the mobile application, generally to request to the server the identification data for the access control system. That information is encrypted with 256-bit Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode. In addition, the encryption key used in AES is previously agreed between the server and the smartphone using the Elliptic Curve Diffie-Hellman (ECDH) key agreement algorithm. This agreement is carried out by exchanging the public keys between these two parties through an insecure channel, such as the Internet, and applying in each part the operations corresponding to the ECDH algorithm we obtain on both sides the key that will be used to encrypt with AES.

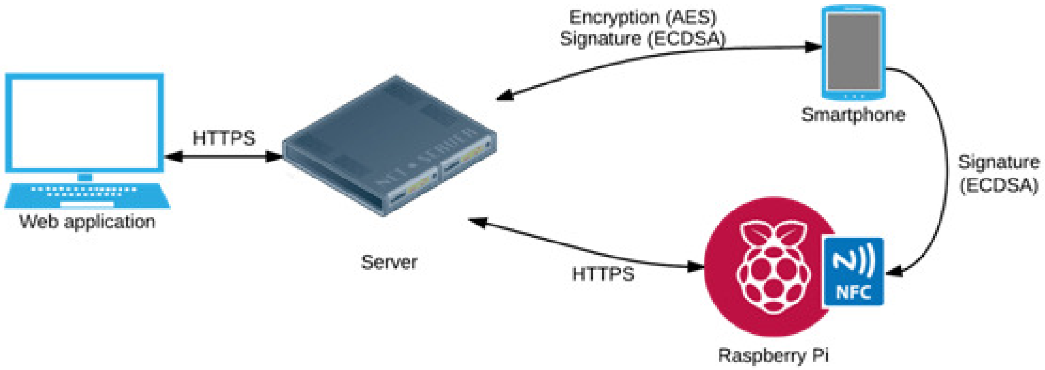

Figure 4. Security scheme

Moreover, the information exchanged between the server and smartphone is digitally signed in order to verify that the information received is correct and also comes from the entity that is expected. For this purpose, Elliptic Curve Digital Signature Algorithm (ECDSA) is used. The use of these two algorithms, provides the system with confidentiality, integrity and authenticity, since the information travels signed and encrypted. The latter involves maintaining a logical order in applying these security algorithms. First, the information is signed and then encrypted, which means that on the other side you first have to decrypt the information and finally verify it before using it or performing any operation with it.

Finally, in order to avoid possible attacks that NFC technology is exposed [15], NFC communications between smartphones and Raspberry Pi also apply security methods. In this case, the information sent from the smartphone to the Raspberry Pi is signed, and then it is verified before using it. For this purpose, the ECDSA digital signature algorithm is also used.

6. CONCLUSIONS

The proposed access control system improves current systems in cost and functionalities thanks to the use of Raspberry Pi as a controller in each restricted area. One of the main advantages of this system compared to those that can be found in stores is the flexibility to add new functionalities and different forms of identification, as well as different sensors that allow to obtain some kind of relevant information. Besides, the use of smartphones in each area as a method of identification is here proposed to replace keys or cards.

Moreover, it is possible to control remote zones in which an Ethernet connection is not available using a wireless network connection because Raspberry Pi has a wireless network interface.

Apart from using Android phones, it is also intended to be able to use iPhone as an identification method, but unfortunately NFC technology is not open to iOS developers.

In the future, cameras connected to the Raspberry Pi will be used to perform video surveillance and to do motion detection tasks using fuzzy logic.

In addition to identification by using smartphones emulating an NFC card, fingerprint identification will be added to provide a higher level of security for the most critical areas. In this way, these two methods will be combined, having to pass both to access the controlled area.

To check the effectiveness of the system, it will be implemented and tested in a real environment. When it is in operation, tests will be carried out to obtain data on its performance. Attacks will also be launched to identify weak points in the security of the system and then correct them.

ACKNOWLEDGEMENTS

Research supported by the Spanish Ministry of Economy and Competitiveness, the European FEDER Fund, and the CajaCanarias Foundation, under Projects TEC2014-54110-R, RTC-2014-1648-8, MTM2015-69138-REDT and DIG02-INSITU.

REFERENCES

[1] “Host-based Card Emulation,” Android Developers, 03-May-2017. [Online]. Available: https://developer.android.com/guide/topics/connectivity/nfc/hce.html. [Accessed: 04-Nov-2017].

[2] M. N. Chowdhury, M. S. Nooman, and S. Sarker, "Access Control of Door and Home Security by Raspberry Pi Through Internet," International Journal of Scientific and Engineering Research, vol. 4, pp. 550–558, 2013.

[3] R. Manjunatha and R. Nagaraja, “Home Security System and Door Access Control Based on Face Recognition,” International Research Journal of Engineering and Technology (IRJET), 2017.

[4] M. W. D. Saravia, “Access control system using NFC and Arduino,” 2015 IEEE Thirty Fifth Central American and Panama Convention (CONCAPAN XXXV), pp. 1–6, 2015.

[5] R. S. Basyari, S. M. Nasution, and B. Dirgantara, “Implementation of host card emulation mode over Android smartphone as alternative ISO 14443A for Arduino NFC shield,” 2015 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC), pp. 160–165, 2015.

[6] N. Saparkhojayev, A. Nurtayev, and G. Seydaliyeva, “NFC-based Access Control and Management System Using Smartphones as Keys,” International Journal of Applied Engineering Research, vol. 11, no. 8, pp. 5519–5522, 2016.

[7] N. Saparkhojayev, A. Dauitbayeva, A. Nurtayev, and G. Baimenshina, “NFC-enabled access control and management system,” 2014 International Conference on Web and Open Access to Learning (ICWOAL), pp. 1–4, 2014.

[8] S. Shigematsu, H. Morimura, Y. Tanabe, T. Adachi, and K. Machida, “A single-chip fingerprint sensor and identifier,” IEEE Journal of Solid-State Circuits, vol. 34, no. 12, pp. 1852–1859, 1999.

[9] J. S. Coffin and D. Ingram, “Facial recognition system for security access and identification,” Nov. 23 1999, US Patent 5,991,429.

[10] J. G. Daugman, "Biometric personal identification system based on iris analysis," Mar. 1 1994, US Patent 5,291,560.

[11] V. Sharma, P. Gusain and P. Kumar, "Near field communication," Conference on Advances in Communication and Control Systems 2013 (CA2S 2013), vol. 248001, 2013.

[12] M. Q. Saeed and C. D. Walter, "Off-line NFC Tag Authentication," Internet Technology and Secured Transactions, 2012 International Conference for IEEE (ICITST-2012), pp. 730–735, 2012.

[13] H. Lee, W.-C. Hong, C.-H. Kao, and C.-M. Cheng, "A User-Friendly Authentication Solution Using NFC Card Emulation on Android," 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 271–278, 2014.

[14] D. Ferraiolo, J. Cugini, and D. R. Kuhn, "Role Based Access Control: Features and Motivation," In Proceedings of 11th annual computer security application conference, 1995.

[15] E. Haselsteiner and K. Breitfuß, "Security in near field communication (NFC)," In Workshop on RFID security, pp. 12–14, 2006.

AUTHORS

Jonay Suárez-Armas is a Computer Engineer graduated at the University of La Laguna in 2016, and currently is a Master Student in Mobile Application Development and member of CryptULL, the cryptology group of the University of La Laguna. He has participated in different conferences and is the author of several papers.

Pino Caballero-Gil is a Full Professor of Computer Science and Artificial Intelligence at the University of La Laguna, Spain, where she leads the CryptULL research group on Cryptology. Her major research interests are in secure mobile applications, stream ciphers, strong identification, cryptographic protocols, vehicular networks and security in wireless networks.