Mobile Access Control System Based on RFID Tags and Facial Information

Kostiantyn Khabarlak  
Dnipro University of Technology  
Ukraine  
habarlack@gmail.com

Larysa Koriashkina  
Dnipro University of Technology  
Ukraine

Abstract

Better access control system security comes at a higher price. It many cases the price is too high for small companies, leaving them vulnerable with cheap and insecure systems. In this work we introduce an alternative access control scheme, which improves access control security while lowering the cost. In the proposed model, passive RFID tags are mounted near a turnstile or a smart door. Tag reading and programming is done via NFC chip directly on the users smartphone. To enhance security, together with smartphone-based authorization we require the user to provide his photograph while entering a secure gate. The photograph is then displayed on a monitoring dashboard side-by-side with the registration picture, so that the two can be matched against each other. The developed client-server application offers administrative system used to configure gate access policies and monitor entrances with filters by access time, user and gate. Also, we propose a mobile application that allows gate registration and serves as a door unlock key. The suggested access control model reduces installation costs required, while maintaining good security. The system is fully wireless and uses cheap autonomous RFID-tags as its main component. We hope, that the proposed system architecture will find its application in small to medium-sized companies.

Keywords: Access Control System, RFID Tags, NFC, Mobile Access Control, Security, Person Identification.

1. Introduction

Many of the modern enterprises use turnstiles or smart doors with access card scanners, where RFID cards are used predominantly. To provide extra security guarantees schools and universities also employ such systems as they are cheap and easy to use. In the same time, such systems have a serious drawback, namely the card can be easily lost, which means an intruder can access the enterprise unnoticed. This in turn may cause critical consequences such as an accident, sensitive information loss, etc. Installing video surveillance cameras may be a partial solution, which enables detection of an intruder in retrospect. However, storing video surveillance data for a long time may take a lot of disk space. The most efficient yet expensive approach to solving the problem is an installation of expensive biometric systems recognizing face or fingerprint (the latter can be recognized via the terminal or directly on a special access control card).

Using smartphone’s NFC chip for secure authentication sees an ever-increasing interest. In this paper, we describe a novel access control scheme, which doesn’t use card scanner and offers higher security guarantees when entering a gateway without needing video surveillance cameras.

2. Review of existing approaches

To begin with, let us describe existing commercial systems, which control the access by the means of a personal identifier. Company [1] proposes systems based on using plastic cards or fingerprint. Manufacturer [2] features a more advanced set of products including virtual mobile cards (NFC-based), bank credit card authentication or biometric systems (fingerprint or facial recognition). A comprehensive list of currently available commercial products is presented in [3]. These can be categorized in

1. Products supporting only classical plastic card id.
2. Products that additionally include support for NFC or Bluetooth Low Energy (if NFC is not available).
3. Biometric systems.

Unique identifier in NFC-compatible systems (point 2 above) is granted either via a global server for all clients (in

---

This article has been published in the peer-reviewed journal. Citation: K. Khabarlak, L. Koriashkina. Mobile Access Control System Based on RFID Tags and Facial Information. Bulletin of National Technical University “KhPI”. Series: System Analysis, Control and Information Technologies, vol. 2, no. 4, pp. 69–74, 2020. DOI: 10.20998/2079-0023.2020.02.12
this case a regular fee is taken) or for free based on a unique id of a smartphone (IMEI) or a SIM-card (IMSI). Identifier can be blocked if requested. Wherein, there may arise at least two cases of unauthorized access to the enterprise, that are impossible to track down: 1) after having lost the mobile device and before locking its id; 2) in case of intentional transfer of a smartphone to third parties. That is to say that such systems are quite vulnerable on its own.

Let us also highlight some of the more advanced systems. In [4] authors note a growing interest in access cards that have an extra level of security. For instance, multi-technology cards that offer embedded fingerprint scanner together with a standard passive RFID tag. To supply the scanner, these cards also have an ultra slim battery. Surely, this comes with a higher price.

Next, let’s consider research of promising combined RFID and biometric systems. Patent [5] contains a description of a biometric system, in which RFID tag holders are also verified via a standalone facial recognition system. This allows to solve additional problems of access control systems like:

1. Buddy badging, when one person logs two badges, while only one actually enters the gate.

2. Tailgating, when several people enter while using the same badge.

Let any access violation occur, the door will be locked and a special lighting stack will alert the guards to intrude. A similar system with a different alerting method is proposed by [6] for access control in university hostels.

To sum it up, all of the above-mentioned systems have either almost no defense against card transfer (e.g., classical or NFC-based systems) or have a high price (e.g., biometric systems including combined systems).

### 3. Mobile access control system model

In this work we propose to turn the classical access control scheme “upside-down”. Firstly, instead of a RFID card scanner, which has to be connected to a computer, we propose using passive RFID tags similar to those found in today’s plastic cards. The tag will placed near the door and will store the door id and some extra information. RFID tags can store enough data for our system and are much cheaper. Secondly, instead of plastic cards we suggest employing user’s smartphone. By holding the device near the passive tag, the proposed access control application will be automatically started. All information about gate location will read from the tag. Also, to avoid the need of a standalone video surveillance camera installation, we require the user to take a photograph on his frontal camera. After that information from the tag joined with the user data is sent to the server via a corporate Wi-Fi network. The information includes: gate information, user id and photograph. In Fig. 1 we present a comparison of typical access control system (shown in Fig. 1a) and the one we propose (Fig. 1b).

As can be seen from the figure, the proposed system doesn’t need camera or RFID scanner installation. Furthermore, no wiring is required as all of the communication is done using smartphone’s Wi-Fi connection.

#### 3.1. Adding tags to the system

As is known, RFID (Radio Frequency Identification) tag is a device that can store a small amount of data, usually below 888 bytes (while there exist modifications with higher memory capacity, they are rate). The tags are classified into active and passive. Active tags contain an embedded energy source (battery). Their advantage is high acting distance (up to 100m). Passive tags are used in intercoms, biometric passports, contactless credit cards and classical access control systems. Such tags are cheaper than active, but can work only on a short distance ranging from several centimeters to meters depending on a standard and working frequency. As in passive tags the microchip has no built-in power source, an electromagnetic coil is installed instead. A device for reading and programming the tag (including a smartphone) creates electromagnetic field inducting a current in the tag by the Faraday’s law [6].

Smartphones contain the so-called NFC chip (Near Field Communication) to read and program RFID tags. It should be noted, that not all of the existing tags on the market are compatible with NFC. Three main tag types, supporting NFC include: MIFARE Classic®, MIFARE Ultralight® and NTAG®. The latter two have the best support among mobile devices [7], and NTAG has the largest capacity. That is why in our product we have decided to use NTAG tags and support two its main modifications: NTAG213 (144 bytes) and NTAG216 (888 bytes) [8]. Besides the writable memory, the tag also contains serial number, an option to enable write password protection and an irreversible switch to read-only mode.

In our system tag programming is supposed to happen on a device of an enterprise security administrator with a use of a special account. The first step is to fill data about the gate to which the tag is going to be attached. The data includes unique gate name and its location. In response to tag registration request, server generates unique unsigned integer id for the gate, which together with the server identifier is written on the tag. In order to avoid data rewrite by third party applications or intentional data corruption, further tag programming is protected via a password (as we have described earlier, this capability is built into the chosen RFID tag standards). The password is global for the given organization and is automatically sent from the server. To complete the gate registration process, the administrator...
Figure 1. Access control system schemes comparison. In contrast to the conventional system (a), the proposed system (b) doesn’t require standalone camera or wires to connect to the door. Passive RFID tag is used instead of RFID reader. All communication is performed via the user’s smartphone.

should bring the device to the tag at a distance of 1-3 cm for the programming to take place. Finally, the administrator needs to setup user access policies for the registered tag in a special server-side administrative application (which we will describe in the next section).

The data written to the tag is stored in a special binary format called NDEF (NFC Data Exchange Format). On Android this binary format is implemented via a special NdefMessage message type, containing a set of data records, called NdefRecord [9]. In our system we write the following information to the tag:

1. Server global unique identifier (server GUID), which is used to verify user organization. It should be noted that a distinctive feature of GUID generation is its high randomness, meaning that collisions (generations of the same GUID) are nearly impossible [10].

2. Unsigned integer, representing gate id inside the organization.

3. A special Android Application Record (AAR) [9] used to launch the application instantly, when the device is held near the tag. The only requirement is that the device should be unlocked.

4. A similar record for iOS devices, containing the so-called Universal Link.

The calculation of each field’s size is shown in Table 1. Overall 120 bytes are written to the tag in our application. Thus, each of the considered RFID tag standards has enough memory for the developed system.

Note, that Apple smartphones did not contain NFC chip for a long time [7]. Even after its appearance the use of NFC chip was limited to Apple Pay functionality only. Currently, NFC APIs are being rapidly added to the Apple iOS operating system. Since iOS 11.0 it has become possible to read RFID tags, and iOS 13.0 has introduced a tag write capability [11]. New devices also feature background tag reading support [12]. That is the feature mostly analogous to the AAR. In contrast to Android, the application is not launched automatically, but a notification is presented to the user, inviting to launch it. As we have already mentioned, the iOS launch record is written in Universal Link format [13]. Thereby, all of the functionality required by our system is available on both mobile platforms.

3.2. Server-side control system

The main instrument for the company’s security administrator is a server-side control panel, implemented in a form of a web-site. Administrative account is needed to access the panel. In there the administrator can add a new user and register its smartphone. To complete the process, users first, last names, and photograph are required. It should be noted, that it is the administrator’s responsibility to guarantee the correctness of the entered data. Additionally, gate access policies can be configured in the panel.

To setup gate access policies, the tags must be first registered via the mobile application (as it was previously described). Then the administrator can select the tag to configure from a drop-down list. Add, view or edit operations are permitted. Gate access configuration panel is shown in Fig. 2. To enhance the security, each access record should have an expiration date set, after which the access will be
Table 1. Data written on the RFID tag.

| Content                        | Size (bytes) | Description                                      |
|--------------------------------|--------------|--------------------------------------------------|
| Server ID                      | 16           | GUID                                             |
| Secure gate ID                 | 4            | Unsigned integer                                 |
| Android Application Record     | 42           | Depends on application name length               |
| iOS Universal Link             | 58           | Depends on application name length               |
| Overall                        | 120          |                                                  |

Figure 2. Gate access configuration panel. The gate to be configured is selected on the left. List of users that have (or had) access to the gate are shown on the right. User name, access status, access expiration date and photograph are displayed.

After the initial setup, the main panel that we expect to be used is the monitoring panel (shown in Fig. 3). A number of monitoring features are proposed:

1. An ability to view access records in real time or by time filter (for example, during or outside the working hours).

2. Filter by the tag to which an access attempt has been made.

3. Filter by user.

4. An option to display denied accesses only.

Each of the filters can be left empty if need. In future we suggest extending the system with mobile face recognition based on research presented in [14], [15].

3.3. Backend and third-party services integration

Along with the above-described user-facing parts, we have a server backend used to communicate with the mobile application via REST API. Also, we have implemented a SignalR [16] endpoint for third-party services integration. SignalR provides a feed to access control events, and is designed for mobile and web integrations. In our system we do not propose turnstile or smart door systems, so we expect the end-users to be able to quickly adapt their existing systems via the provided API. We hope that the API provided will allow for a seamless implementation of our system into existing infrastructure.

4. Conclusion

Access control client-server application has been presented in the paper, which includes:

1. Administrative system to configure gate access poli-
Figure 3. Monitoring tab of the proposed access control system. Access list filters by time, gate, person or access status are configured on the left. Corresponding user accesses are shown on the right. The following information is presented: user’s name, registration photo and picture taken at the gate, gate name, access time and status.

2. Monitoring system with filters by access time, user and RFID-tagged gate.

3. Mobile application made to register gates and that serves as a key to unlock the doors.

The implementation of the developed system will allow to lower the cost of access control systems in schools, universities and enterprises by replacing stationary RFID scanner with a cheap tag, and also by avoiding video surveillance camera installation. The camera is not required as the user takes a photograph on his mobile phone when unlocking the door.

We hope, that the proposed application will make a contribution to the development of more secure and less expensive access control systems.

We see an implementation of a mobile face recognition system as one of the next steps to enhance the proposed application.

References

[1] (2020). “Data Protection. Access Control. Working Time Tracking (in Russian),” [Online]. Available: http://www.ualock.kiev.ua/index.htm (visited on 10/20/2020).

[2] (2020). “Perco security systems (in Russian),” [Online]. Available: https://www.perco.ru/ (visited on 10/20/2020).

[3] (2018). “Mobile Access. Using smartphone in access control systems (in Russian),” [Online]. Available: https://habr.com/ru/company/intems/blog/433872/ (visited on 10/12/2020).

[4] (2020). “Access Control Cards (in Russian),” [Online]. Available: http://www.techportal.ru/glossary/karti-kontrolya-dostupa.html (visited on 10/12/2020).

[5] K. Kail, C. Williams, and R. Kail, “Access control system with RFID and biometric facial recognition,” U.S. Patent 11 790 385, Nov. 1, 2007.

[6] U. B. Farooq, M. ul Hasan, M. Amar, A. Hanif, and M. U. Asad, “RFID based security and access control system,” International journal of engineering and technology, vol. 6, no. 4, pp. 309–314, 2014. DOI: 10.7763/IJET.2014.V6.718.

[7] (2020). “NFC compatibility,” [Online]. Available: https://www.shopnfc.com/en/content/7-nfc-compatibility (visited on 10/12/2020).
[8] (2020). “NFC tag specs – tag NFC,” [Online]. Available: https://www.tagnfc.com/en/info/11-nfc-tags-specs (visited on 10/12/2020).

[9] (2020). “NFC basics,” [Online]. Available: https://developer.android.com/guide/topics/connectivity/nfc/nfc (visited on 10/12/2020).

[10] (2020). “What is GUID?” [Online]. Available: http://guid.one/guid (visited on 11/24/2020).

[11] (2020). “Core NFC — Apple Developer Documentation,” [Online]. Available: https://developer.apple.com/documentation/corenfc (visited on 10/23/2020).

[12] (2020). “Adding support for background tag reading — Apple Developer Documentation,” [Online]. Available: https://developer.apple.com/documentation/corenfc/adding_support_for_background_tag_reading (visited on 10/23/2020).

[13] (2020). “Allowing apps and websites to link to your content — Apple Developer Documentation,” [Online]. Available: https://developer.apple.com/documentation/xcode/allowing_apps_and_websites_to_link_to_your_content (visited on 10/23/2020).

[14] K. Khabarlak and L. Koriashkina, “Fast Facial Landmark Detection and Applications: A Survey,” Journal of Computer Science and Technology, vol. 22, no. 1, pp. 12–41, Apr. 2022. DOI: 10.24215/16666038.22.e02. [Online]. Available: https://journal.info.unlp.edu.ar/JCST/article/view/1972.

[15] K. Khabarlak, “Face Detection on Mobile: Five Implementations and Analysis,” CoRR, vol. abs/2205.05572, 2022. DOI: 10.48550/arXiv.2205.05572. arXiv: 2205.05572. [Online]. Available: https://doi.org/10.48550/arXiv.2205.05572.

[16] (2020). “Real-time ASP.NET with SignalR — .NET,” [Online]. Available: https://dotnet.microsoft.com/apps/aspnet/signalr (visited on 10/23/2020).