User Authentication Based on Contactless High and Ultra-High Frequency RFID Tags

Sebastian Janko, Barbara Klier, Filip Ptiček, Marko Pavelić, Marin Vuković
University of Zagreb
Faculty of Electrical Engineering and Computing
Unska 3, Zagreb, Croatia
{sebastian.janko, barbara.klier, filip.pticek, marko.pavelic, marin.vukovic}@fer.hr

***Abstract**. Internet of things is becoming a significant factor in modern society and terms like smart cities, smart homes and smart locks are more and more present on the consumer market. The paper focuses on smart locks that use contactless technologies for user authentication. Although nowadays locks typically use near-field communication for such purposes, we combine that technology with ultra-high frequency readers and tags. The paper proposes a system for user authentication and lock control based on the two radio frequency identification technologies. Both technologies are used in order to meet the requirements placed by the current state of technologies used at our Faculty. Finally, the paper discusses security issues and provides methods of protection against most common security vulnerabilities.*

Keywords. UHF, RFID, NFC, authentication, smart locks

1 Introduction

Internet of things is becoming a significant factor in modern society which is working towards connecting every object that we interact with on the Internet. Terms like smart TV, smart fridge, but also smart home and smart cities are becoming more and more present on the consumer market.

One of objects that everyone uses daily are locks, which have traditionally used mechanical lock and key for access. Access monitoring and logging, which are a must in some scenarios (e.g. warehouse, military, medicine, etc.) could be done only by humans or, more recently, surveillance cameras, also monitored by humans.

Smart locks have been on the market for some time now and are based on various technologies. For example, probably the most straightforward and very secure authentication method is used in biometric locks, where cameras or readers read fingerprints, retinas, perform face recognition and similar. However, due to privacy issues and inability to revoke biometric data, such devices are less and less used in areas other than those where high secure access control is needed.

With the development of radio frequency identification (RFID), user authentication with unique RFID tags became rather popular. First there were locks that relied on low frequency devices, in frequency range around 125kHz. Probably due to security and practicality issues (e.g. range, better resilience to interference), near-field communication (NFC) at 13.56 MHz is now the most popular technology for user identification and authentication.

However, in this paper we propose a system for user authentication based on ultra-high frequency (UHF) RFID, which is typically used for asset tracking, logistics and similar purposes. This is because there is an existing system for employee attendance tracking on the Faculty of Electrical Engineering and Computing based on UHF RFID, and all employees already have unique UHF based tags. In that sense, the idea is to use existing tags for user authentication and lock control. Furthermore, our Faculty students have their student cards that are NFC enabled, and the idea is also to grant them access to specific doors/locks.

Therefore, we propose a system for user authentication that can read both UHF and NFC tags, authenticate the users and provide lock control and access monitoring. The system is managed by a central control point where each unique user identifier, whether it is implemented by UHF or NFC, can be assigned to specific locks within the Faculty.

The rest of the paper is organised as follows. Section 2 describes the proposed system for user authentication consisting of the UHF and NFC readers and central web application for user management and reader control. Section 3 discusses common security vulnerabilities applicable to the proposed system and gives information on how to lower or remove the risks of breaches. Finally, section 4 concludes the paper and gives guidelines for further work on developing the proposed system.

2 System for user authentication by using high and ultra-high frequency RFID tags

The proposed system is physically and logically divided into two building blocks:

- hardware and software that runs the readers, placed on the controlled doors
- web application on a virtualized server that manages the users, their identifiers and controls the readers

The following sections explains the details about each component.

2.1. NFC and UHF Readers

The system consists of ultra-high (UHF) and high frequency (NFC) readers which allow two different types of authentication. The UHF tags are used by the employees of the Faculty of Electrical Engineering and Computing University of Zagreb, while the NFC tags are used by the Faculty students. Along with the readers, the system uses a Raspberry Pi computer to communicate with the readers and with the internal server. The tags and readers conform to the latest ISO/IEC 18000 and EPC standards and for HF and UHF systems (ISO/IEC 18000-6, 2013), (ISO/IEC 18000-3, 2010), (ISO/IEC 14443-4:2018**).**

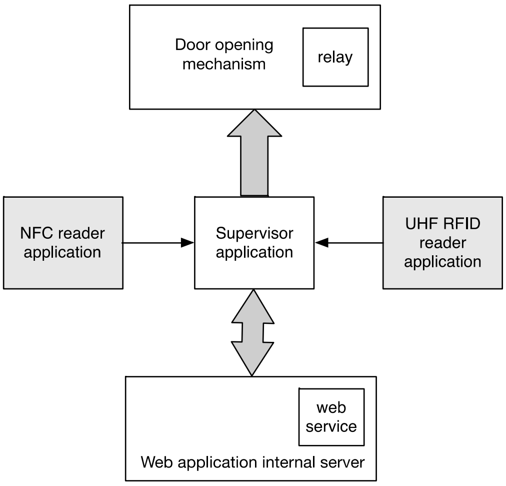


Figure 1 - System architecture

The UHF reader is connected to the Raspberry Pi with a USB cable and they communicate via serial interface. The whole architecture can be seen on Figure 1. The communication is handled by a Python script on the computer and consists of sending packets to the reader and parsing packets received from the reader. The reader's protocol is documented within the reader's documentation. The protocol packets which are made of hexadecimal digits. As seen in Table 1 and Table 2, every packet consists of several fields which define a packet.

Table 1. Request packet form

Len	Adr	Cmd	Data[]	LSB-CRC16	MSB-CRC16

Request packet consists of the following fields:

- `Len` – packet's length
- `Adr` – reader's address
- `Cmd` – command identifier
- `Data[]` – data array, command specific
- `LSB-CRC16` – least significant byte of the CRC16 algorithm
- `MSB-CRC16` – most significant byte of the CRC16 algorithm

Table 2. Response packet form

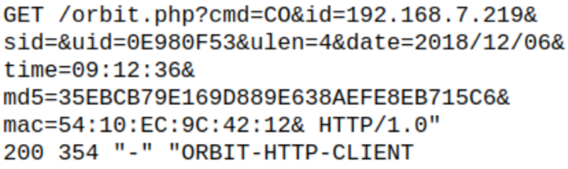
Len	Adr	reCmd	Status	Data[]	LSB-CRC16	MSB-CRC16

Response packet consists of the following fields:

- `Len` – packet's length
- `Adr` – reader's address
- `reCmd` – command identifier
- `Status` – request command's execution status
- `Data[]` – data array, command specific
- `LSB-CRC16` – least significant byte of the CRC16 algorithm
- `MSB-CRC16` – most significant byte of the CRC16 algorithm

The packets sent to the reader are packets that request the content of EPC and TID memory on tags (GS1, 2013). The packets received from the reader contain that data which is then parsed in Python. After extracting the data from the packets, the data is sent to a supervisor application, also written in Python. The supervisor application consists of a web server with one endpoint. The script which interfaces with the UHF reader sends the TID to the supervisor through an HTTP POST request. The request contains JSON data – the type of the reader (UHF or NFC) and the ID of the tag.

The NFC reader is powered via Power over Ethernet interface and also uses it to communicate over the network with the Raspberry Pi. The NFC reader is a standalone HTTP web client. Raspberry Pi is running a Python web server which receives HTTP requests from the reader upon card detection. Information containing the unique identifier (UID) is sent in the URL of the HTTP request. Example of a HTTP request sent by the NFC reader is shown on Figure 2.



```
GET /orbit.php?cmd=CO&id=192.168.7.219&
sid=&uid=0E980F53&ulen=4&date=2018/12/06&
time=09:12:36&
md5=35EBCB79E169D889E638AEFE8EB715C6&
mac=54:10:EC:9C:42:12& HTTP/1.0"
200 354 "-" "ORBIT-HTTP-CLIENT
```

Figure 2 – HTTP GET request

The web server parses the URL to extract the UID and sends it to the supervisor through an HTTP POST request. The request contains JSON data - the type of the reader (NFC) and the UID of the NFC tag.

The supervisor application then sends this same data to an application on an internal server which checks the data against a database.

The door opening mechanism which we are interfacing is a system which can open sliding doors using an electric motor and a computer controlling the motor. The system has an interface which can be connected to a relay. The computer controlling the relay then controls the motor and the state of the sliding door.

After the application on the internal server checks the database, it returns an HTTP status code. This code can be 200 OK or 401 Unauthorized. If the code returned is 200 OK, the supervisor application triggers the relay connected to the Raspberry Pi which is connected to the door opening mechanism used to open the sliding door.

2.2. User management and reader control web application

The web application consists of an administration service, database and a graphic web interface for accessing the application and database, shown in Figure 3. The administration service queries the database for needed information and approves access. The database stores the readers, tags and users. The web interface allows reading of all existing data in the database and entering new data.

The administration service readerHandler is a connection between the readers and database and approves access to the door. With the database, it is the back-end part of the system.

When the tag is pressed against the reader and access is requested, the reader sends an HTTP POST request for access to the service. The service receives the data in the body of the POST request, processes the request, queries the database for the necessary information, and responds with HTTP 200 (OK) if access is approved, or HTTP 401 (Unauthorized) if access is denied.

The database stores all the administrators that can access the application, all the tags that are allowed to open the gate, and readers. They are uniquely identified by an *ID*. That secures that only appropriate tags can open their respective gates.

The front-end of the system is a web interface that is a graphic user interface for accessing the application and data. After a secure login, an administrator can view other existing administrators, tags and readers. All data is displayed using DataTables and jQuery. The data is formatted, searchable and paginated.

Adding new data is supported via a PHP form, which then validates the data and saves it in the database, which is then viewable in the list of users, tags or readers.

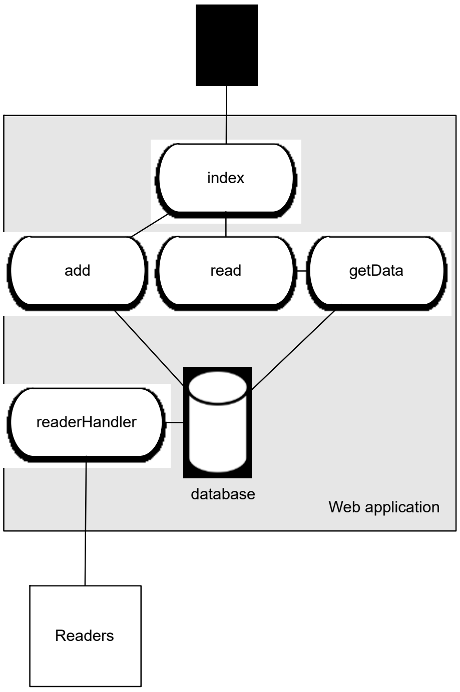


Figure 3 - Architecture of user management and reader control web application

By hovering over the respective buttons, a dropdown menu appears, giving access to view data or add new data.

3 Security analysis of the proposed system

As with every locking system, security should be a central concern of the system in order to prevent unauthorized access. When discussing security, we can analyse the following aspects:

- Physical security of the lock hardware and web server
- RFID and NFC security
- Communication security, between locks and web server
- Web security and user data protection
- Reliability of the system

3.1 Physical security

The readers are distributed across our Faculty, so physical security is an important aspect of the proposed system, since an attacker could try to gain physical access to a part of the system.

Readers are enclosed within special housings which would indicate unauthorized opening. Furthermore, each reader/door is covered by a security camera so it is our opinion that it would be fairly easy to detect unauthorized access to the equipment.

The server is placed in a server room with other servers from our Faculty, that is monitored at all times, so we also estimate the risk of such a breach as being low.

3.2 RFID and NFC security

On the RFID side there is a possibility of attacks such as sniffing the communication between tags and readers, interference in communication, which is a kind of denial of service attack, manipulation of tag data and finally the destruction of tags (Thornton, 2006). Attacks on RFID tags are not common and are hard to perform because the tag's memory has very limited memory space. However, there have been cases of malware and SQL injection attacks on RFID tags (Kirk, 2006) (Ollmann, 2013).

However, cloning tags is a common attack and possibly difficult to protect against. Regarding NFC, we are currently using Mifare 1K which can be cloned, but the idea is to migrate to Mifare Desfire and Ultralight in the following years. However, the entrances covered by NFC are meant for students so virtually all students of our Faculty can have the access to these entrances, making the need for cloning less profitable. When looking at UHF tags, an attacker needs a cloning device in the proximity of a tag. The built-in protection for such attacks is a unique tag ID which is written by manufacturer and cannot be overwritten. More complex way of protecting against cloning attacks is writing a timestamp on the tag every time the tag communicates with a reader. The same timestamp is written in the database alongside the tag ID. On every authentication attempt, the timestamp in the database is checked against the timestamp on the tag. In case an attacker clones a tag, there will be two identical tags. If the attacker then tries to authenticate, he will succeed, and a new timestamp will be written on his tag and in the database. When the user tries to authenticate, he will be denied entrance which will mean an attacker got access with his tag. In case an attacker clones a tag, but the user of that tag authenticates first, the attacker's tag timestamp will be outdated, and he will not have access anymore.

To sniff and replay communication between a tag and a reader, the attacker needs a sniffing device in close proximity of the reader or a very powerful device to sniff from greater distances. In any case, after the communication has been recorded, the attacker can perform a replay attack where the recorded communication is replayed back to the reader without the need for a tag. However, this attack, especially the replay part, requires specialized equipment and knowledge and it is our opinion that the probability of such an attack is low, especially due to other controls such as security cameras, analysis of entrances within the system etc.

3.3 Communication security

Attacks on the communication channel would consist of inserting a sniffing device in the channel (man-in-the-middle attack). As the proposed system uses Ethernet cables to communicate with the internal server, it is more secure than system which use wireless protocols because they are easier to sniff. If an attacker managed to perform a man-in-the-middle attack, he would be able to see all data sent to the internal server in plain text as the system does not have any sort of cryptographic protocol like TLS. As this system does not protect critical infrastructure, it can allow unencrypted communication with the internal server.

However, the readers and server are contained within a VPN so an attacker would need to have physical access to the infrastructure in order to sniff the traffic. Furthermore, TLS will be implemented for securing the communication in the production level system.

3.4 Web security and user data protection

On the server side, the system can face denial of service attacks and other attacks common to servers and web applications. Broken authentication, access control and sensitive data exposure are the main concerns with the proposed web application.

Broken Authentication often happens because authentication and session control functions are implemented wrong, allowing attackers to violate passwords, keys, token sessions or to exploit other implementation failures to temporarily or permanently take over identities of other users. This is addressed by the use of strong generated session tokens that change periodically with each user login. The possibility of stealing a session token is limited since the system is working in a VPN without access to the Internet and only limited number of users (administrators and managers) have access to the system.

Broken Access Control is setting incorrect limits on what authorized users are allowed to do. Attacks can use these disadvantages to access unauthorized functionality and / or data such as accessing other users accounts, reviewing sensitive files, changing data other users and change access rights. Access control was accomplished by the careful use of roles. Each page verifies whether the user is logged in and whether his/her account has the privilege to access its contents.

Sensitive Data Exposure such as financial data, health care data, and personal information happens when attackers steal or modify such poorly protected data to perform card fraud, identity theft or other crimes. Sensitive data can be compromised if stored or transferred without extra protection and requires special precautions when interacting with the browser. Regarding the proposed system, it stores RFID identifiers and history of user access, alongside with authentication credentials. Passwords are sucred using hash function with salt, in order to lower the possibility of dictionary attacks. The same is the case with user tag identifiers. However, user access logs are not encrypted and this will be a part of the future work.

3.5 Reliability of the system

When examining any locking system, it is obvious that it should be as reliable as possible. All the doors covered by the proposed system are also equipped with standard, mechanical, locks that provide redundancy in case the proposed system fails.

Regarding the reliability of the proposed system, if it should fail completely, the users would be able to use existing mechanical locks. If a part of the system fails, e.g. a single lock, users would also be able to use existing keys. Only problem would emerge if the NFC locks failed, since the students do not have additional keys. In that case, the doors would be inaccessible from outside of the Faculty. In this sense, all the doors can be opened from the inside; this is a must in cases of power outage, fire or similar situations.

4 Conclusion

The proposed system for user authentication based on contactless high and ultra-high frequency RFID tags can be used by both the employees and students of the Faculty. Both the use of UHF and NFC readers removes the need to introduce new technologies because of systems that are already in use in the Faculty.

Access control using RFID UHF and NFC tags proves to be more practical than the standard mechanical locks due to several facts. The most notable fact is that access permissions can be granted dynamically for each user RFID tag. This removes the need for exchanging keys, as is the case currently on our Faculty. Furthermore, using these type of locks results in ability to monitor access history at all times, which might prove to be valuable in cases of missing equipment or similar situations. Finally, all of our employees and students already have UHF (employees) and NFC (students) tags. This removes the need for issuing new tags to users and makes it more simple to migrate to the proposed system.

As with any locking system, security should be specifically addressed. The use of different modules that communicate with other different types of security measures must be implemented. For user management there is a login system for administrators to prevent unauthorized access to the database. The communication between the tag readers and the web application is limited to the system VPN, and is not currently encrypted, which might enable sniffing if the attacker had physical access to the infrastructure. This is currently covered by housing the readers and coverage of the security cameras throughout the Faculty.

When discussing future work, several issues emerge. First, security should be hardened further, in terms of encrypting communication and using more secure NFC cards. Additionally, an expert system that monitors the regularity of access should be implemented in order to indicate potential unauthorized access, cloned tags, or other types of breaches.

References

*ISO/IEC 18000-6: Information technology -- Radio frequency identification for item management -- Part 6: Parameters for air interface communications at 860 MHz to 960 MHz General (*2013)

ISO/IEC 18000-3: Information technology -- Radio frequency identification for item management -- Part 3: Parameters for air interface communications at 13,56 MHz (2010)

ISO/IEC 14443-4: Cards and security devices for personal identification -- Contactless proximity objects -- Part 4: Transmission protocol (2018)

GS1: EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID: Specification for RFID Air Interface Protocol for Communications at 860 MHz – 960 MHz. (2013)

Thornton, Frank & Haines, Brad et al. (2006): RFID Security: Protect the Supply Chain, first edition, Syngress Publishing, 2006.

Kirk, J. (2006): RFID tags vulnerable to viruses, study says, 15 March 2006, feeds.computerworld.com/article/2561797/rfid-tags-vulnerable-to-viruses-study-says.html, 8 July 2019

Ollmann, O. (2013), SQL Injection in the Wild, 25 March 2013, www.circleid.com/posts/20130325_sql_injection_in_the_wild, 8 July 2019