Multimodal Electronic Access Control System Using Digital Identity for Enabling Authorized Physical Access to Premises

Matej Rabzelj, Tjaša Jereb, Aljaž Martinčič, Andrej Kos

University of Ljubljana
Faculty of Electrical Engineering
Tržaška cesta 25, 1000 Ljubljana
E-mail: matej.rabzelj@ltfe.org, tjasa.jereb@ltfe.org, aljaz.martincic@ltfe.org, andrej.kos@fe.uni-lj.si

Abstract

With the advancement of consumer electronics and expansion of connectivity technologies, more and more devices are connected to the cloud. These include smart home appliances such as smart lights, home video systems and most importantly – smart locks. However, installation of an EAC (electronic access control) system should consider a number of security and usability aspects. This paper presents the developed EAC system which enables multimodal context-based authentication and provides access to the Student council's office at the Faculty of electrical engineering. It describes the integration of hardware mechanism and it's connection to the cloud, as well as the authorization process to ensure controlled access. Finally, it explains the importance of interaction design and overviews the security aspects of different modalities.

1 Introduction

Premises locked by means of electronic access control (EAC) offer enhanced physical security due to centralized monitoring and access logging systems. The most common type of physical EAC is role-based, where access to parts of premises is determined by the user's role in an organization [1]. Replacement of standard keys with EAC systems minimizes difficulties in case of their loss, as there is no need to replace the entire lock and keys of other users. Instead, restricting the access goes only as far as denying permissions for an individual electronic key [1]. Their usage is not exclusive to office buildings, as nowadays, a wide array of smart access solutions are presented through a trend of smart houses, introducing keyless entry to simple households and regular customers. Changes towards easier access are also visible in the car industry. While most car manufacturers already introduced key-less entry as a part of their basic equipment, some went even a step further, developing the new Digital key standard which will enable any smartphone or smartwatch to act as a digital car key [2].

The access control to the majority of cabinets, laboratories and offices at the University of Ljubljana, Faculty of electrical engineering is realised with an electronic system unlocked by appropriate RFID (radio-frequency identification) cards or keys. To open the door with this solution, one must approach the key next to the keypad near the door. Amongst premises with this system is the Student council's office on the ground floor of the faculty. Each year a newly elected set of students gains access to the office, leading to issuance of a new set of keys at the beginning of each mandate. These keys – while functional – bring some inconveniences. Starting with key programming which requires a time-consuming manual entry of each name using a dedicated control program. Then, when entering and exiting the office frequently, keys might be forgotten inside, leaving the user locked out. Furthermore, in case a key is lost, the access has to be manually revoked. These are only some aspects of a much wider challenge of designing a secure access control system while offering a seamless user experience.

To achieve their functionality, EAC systems make use of various technologies ranging from simple RFID tags to complex biometric scanning solutions [3]. However, the exact choice of authentication method typically represents a tradeoff between a system's security and users' convenience. Nevertheless, multiple modalities of interaction may be implemented to increase the solution's versatility and satisfy different use cases.

Therefore, our solution proposes the use of the already established digital university identity database to provide premises access control with the following modalities of interaction:

- voice-invoked access control,
- geolocation-based access control,
- proximity-based access control;

2 System Architecture

The developed EAC system consists of three main functional building blocks:

- a user-facing (mobile) client component for enabling various modalities of invocation,
- an authentication proxy for authentication against University of Ljubljana's remote identity directory,
- an electromechanical part comprised of physically secured components for latching action control;

An overview diagram of these modules and their interconnected interfaces is depicted in Figure 1. The configuration of components on the diagram follows the logical flow of an unlocking action - starting with the user intent at the top and resulting in mechanical action at the bottom of the figure.

The user who intends to access locked premises can interface with one of our four developed client applications. These provide the ability to control the door lock with both iOS and Android-based mobile terminals. Besides the touch input, these mobile applications can also be invoked using a corresponding Siri voice command or an on-location NFC (near field communication) tag. Aside from providing entry for themselves, users inside the building may also respond to incoming visitors without having to reach for their mobile phones or a remote doorbell switch. Instead, the unlocking mechanism may be activated using voice control provided by the Amazon Alexa device with a custom invocation command or using web and desktop applications.

Mobile clients and web application require users to log in prior to their first use, while Alexa requires the user to be present within its audible range. Login credentials are accepted in the form of username and password, which are securely conveyed to the authentication proxy server in exchange for a session token. This eliminates the need to store sensitive data on the device or in the cloud and only stores the time-constrained token instead. After initial authentication the application allows for fingerprint-assisted and geolocation-based unlocking. These methods provide some elementary restrictions, such as geofencing, to limit the application's functionality outside of the building's vicinity.

Further upstream, a LEMP stack (Linux, Nginx, MariaDB, PHP-FPM) middleware with secure API (application programming interface) endpoints serves as an authentication and session management gateway. It features multiple virtual network interfaces providing firewalled internet connectivity and communication with the University of Ljubljana's AD (Active Directory) server and the on-premise microcomputer module. At the forefront, Nginx performs TLS (transport layer security) termination of incoming requests, while the PHP OpenLDAP implementation escapes and authenticates the provided client credentials against the central AD server. Assuming success, the retrieved user data is further compared against local filters enforcing conditional access. Matching records from the unified authentication procedure then generate a pseudo-random session key, which is written to the MariaDB storage and returned to the client. All subsequent incoming requests with included session token are then compared against existing records and either forwarded to the server's command and control component or dropped if invalid. Lastly, the command and control module uses a virtual private network to communicate with the on-site microcomputer.

Contrary to the extensive list of software components, the on-premise electromechanical installation is rather uncomplicated. It consists of a preinstalled electric door latch (lock), mechanical relay, and an SBC (single board computer). The latter severely aids the prototyping process, as it offers on-board Ethernet connectivity and direct programmatic control of its GPIO (general purpose input and output) ports. It accepts network requests from the control module and issues executable scripts that activate the mechanical unlocking action. The whole installation is enclosed in a locked network cabinet and remains compatible with the preinstalled RFID EAC system.

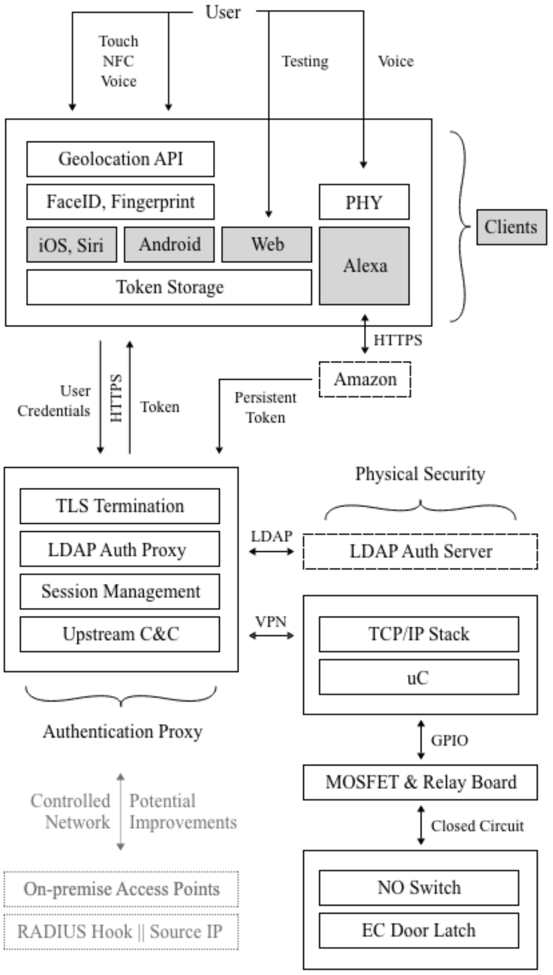

Figure 1: System architecture diagram depicting a typical request flow through different clients and various software and hardware components.

3 Interaction Design

During the mobile development, our efforts were aimed towards creating a very streamlined operation experience. Therefore, the application interface was designed to serve one core purpose – granting physical access in a rapid and secure manner. This approach severely aids the overall user experience and aims to position the touch-based smartphone unlocking mechanism near the existing RFID keycards in terms of convenience. Accordingly, two different interface design proposals were developed – one employing a tap-based unlocking system and another relying on a swiping unlock gesture. Each proposal was implemented on one of the mobile platforms as a rudimentary approach towards A/B testing, neglecting the platform dissimilarities and relying on user familiarity instead. Selected views of mobile interfaces are depicted in Figure 2 and Figure 3.

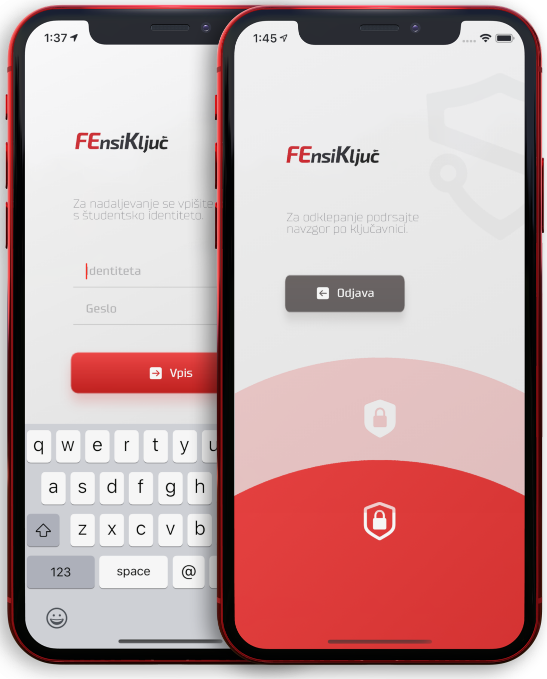
1:37
FEnsiKljuč
Za nadaljevanje se vpišite s študentsko identiteto.
Identiteta
Geslo
Vpis
q w e r t y u
a s d f g h
z x c v b
123
space
@
1:45
FEnsiKljuč
Za odklepanje podrsajte navzgor po ključavnici.
Odjava

Figure 2: Mobile client interface on iOS operating system displaying a large surface area for a ”swipe to unlock” gesture. The unlocking action also features audible and haptic feedback to aid user experience.

Despite different interface compositions, both applications follow the same crucial design patterns. They use the red color from the University of Ljubljana’s emblem to establish a visually relating appearance and color-code their primary functions. The interfaces adapt to different screen sizes and resolutions to always position the primary action widgets within a natural resting position of a user’s thumb. The geolocation-conditioned availability of login and unlock actions are color-coded along with matching symbols or text.

The iOS application, however, provides a much larger surface area for the touch-start event, making it easier to operate while walking as it does not require the user to keep eyes on the screen. It also provides audible and haptic feedback upon the successful unlock action, aiding the user in case of a silent latching mechanism. Contrary, its Android counterpart only offers feedback in form of a toast message but provides additional invocation mechanisms. Namely, it allows for direct invocation of the unlock intent from the system launcher menu and the immediate application exit upon the command execution. The latter nearly transforms the application into a home screen widget, allowing for a very transparent operation.

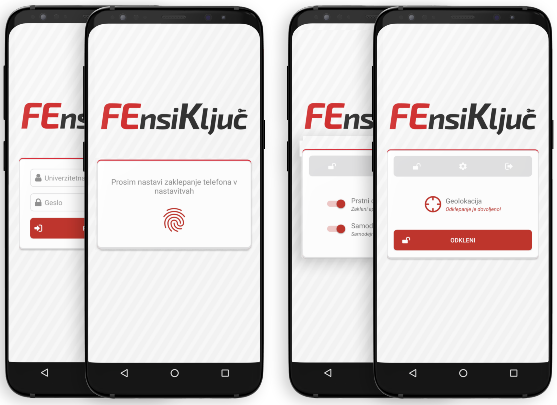

Figure 3: Android interface features a smaller primary action surface positioned within a natural resting position of a user’s thumb. However, the application also offers several configuration options, including direct unlocking from home screen and fingerprint-based unlock protection.

Besides manually launching smartphone applications, their invocation using Siri voice commands on iOS and NFC detection on Android was also implemented. To enable the latter, a NFC tag with a password protected memory was placed outside of the office. Its scanning with an Android smartphone allows for activation of background unlock actions implemented in the mobile application.

Additionally, voice invocation of the unlock controller was realized using Amazon Alexa. This required a different approach, as Alexa only provides users with a voice-operated interface. Its invocation is therefore only possible from inside the office where the Echo Dot resides. In order to enable its smart home functionality an intermediary device emulation server was installed in local network, bridging the communication between Alexa and SBC. This allowed the use of natural language to control access to premises.

4 System Security

Our development approach considered the separation of concerns (SoC) principle in terms of software as well as hardware components. The modular design provided flexibility in terms of system installation and ensured the physical security of critical parts. Further, the authentication proxy server and the SBC both store private key files for OpenVPN authentication and TLS termination, as well as session and database information on the fully encrypted storage. This configuration prevents possible data exfiltration attacks on the physical media. Besides storage, all participating networks and interfaces are packet-filtered, rate-limited, and directly addressed by IP, evading potential DNS poisoning attacks. All system connections, login attempts, and executed mechanical actions are logged to provide an authorization history catalog.

Despite our efforts, several security weaknesses were identified and changes and updates for their mitigation were proposed. While DMA side channel and cold boot encryption attacks [4] on the authentication infrastructure are highly unlikely due to tight security measures, client terminal devices remain largely unprotected. Most notably, the system's geolocation-conditioned access is based on the information directly provided by the client devices. The latter should not be trusted as a reputable source of information, as they remain outside of our direct control. While such attack does not permit unauthorized access, mobile application users may modify their mobile systems to provide mock location data, falsely indicating their geographical position and allowing the premises to be unlocked remotely. Such settings are rather easily accessible in form of a software toggle on Android platforms, but may also be enabled on rooted (jailbroken) iOS devices or by using a compromised external GPS module or a GPS signal spoofer (e.g. using a software-defined radio - SDR) [5]. Moreover, mobile client security features such as fingerprint authentication and token storage all rely on their vendor implementations. In case the terminal device gets stolen, and an exploitable vulnerability exists, an attacker might be able to hijack active, time-constrained session keys.

Therefore, our security propositions include a migration to a network-based terminal localization method or source IP-based local access restrictions. On IP networks, these could range from simple firewall policies to RADIUS authentication hooks on eduroam networks, utilizing the same digital university identity and confirming the user presence on-site. However, all of the above options require direct control over the on-premise network, potentially sacrifice user convenience and possibly even introduce new attack vectors (e.g. a RADIUS evil twin attack).

Lastly, possible attacks on voice recognition hardware - Amazon's Echo Dot - were evaluated. While the device is securely installed inside the gated area, an attacker within a direct line of sight (e.g. from an elevated nearby building) could use a novel laser-based audio injection attacks on voice-controllable systems utilizing integrated MEMS (micro-electro-mechanical systems) microphones [6]. Although a cheaper (albeit more conspicuous) version of voice-based attack could also include a loud voice recording projected through door slit using a directional loudspeaker to activate the Echo Dot.

5 Conclusion

Electronic access control is undeniably a fundamental part of most commercial premises and smart homes. Its use has many advantages, such as revokable control and authorization log compared to the classic approach of sharing a common key. With the use of a wide range of standard options ranging from RFID installation to biometric scanners, additional methods, such as voice assistants and mobile and desktop applications enable users with new methods of authentication. However, each such novelty potentially instigates new security risks that have to be taken into consideration during the development and implementation these solutions.

Our solution addresses the problem of RFID key possession and enables context-based authentication using smartphone or voice-activation instead. Further, it simplifies privilege management operations by utilizing a pre-existing user database particularly suited for academic environment. Based on limited user feedback, these additions represent a significant improvement in terms of access convenience, as well as user experience by tackling repetitive daily tasks with gamification. However, the long-term reliability and security of our solution remain to be continuously evaluated. The first system assessment primarily indicated the requirement for transition to a network-based geolocalization, as well as inclusion of support for smart wearable devices to further aid user convenience.

References

[1] A. C. Caputo, "Digital video surveillance and security (second edition)," [Accessed 03.09.2020]. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780124200425000113

[2] "Car connectivity consortium – digital key task group 2019," [Accessed 03.09.2020]. [Online]. Available: www.trustonic.com/events/car-connectivity-consortium-digital-key-task-group-2019

[3] W. Deutsch, "An introduction to electronic access control systems," [Online; accessed 6.7.2020]. [Online]. Available: https://www.thebalancesmb.com/introduction-to-electronic-access-control-394578

[4] J. Longo, E. De Mulder, D. Page, and M. Tunstall, "SoC it to EM: ElectroMagnetic side-channel attacks on a complex system-on-chip," pp. 620–640.

[5] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," p. 75. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2046707.2046719

[6] T. Sugawara, D. Genkin, B. Cyr, S. Rampazzi, and K. Fu, "Light commands: Laser-based audio injection attacks on voice-controllable systems."