Ticketing Systems for Smart Public Transportation: Tools at the User Side

Antoni Martínez-Ballesté(✉), Nicolás Villalobos, Edgar Batista,
Pablo López-Aguilar, and Agusti Solanas

School of Engineering, Universitat Rovira i Virgili, 43007 Tarragona, Spain
antoni.martinez@urv.cat

Abstract. Smart transportation systems are an integral part of the smart cities of tomorrow. With the proliferation of miniaturised sensors, IoT devices and 5G communication technologies, plenty of opportunities are yet to be developed to make transport systems more convenient, from the user side, and more cost-efficient and sustainable from the service providers side. Among the many actors involved in this domain, ticketing systems are paramount to access public transportation, such as trains, metros or buses. However, these systems must cope with a number of strong security and privacy requirements. This article overviews the current landscape of tools for a secure deployment of the user side of ticketing systems in public transportation.

Keywords: Smart transportation · Ticketing systems · Security · Lightweight cryptography · Smart card

1 Introduction

In today's society, the transportation of people and the problems it entails are gaining importance. Despite the effect of the COVID-19 pandemic on the popularisation of teleworking, commuting and its effects on large urban areas are still an issue. Apart from collapses and delays that workers may suffer due to the traffic or accidents, the mass movement of vehicles is a problem for the environment. Large cities and metropolitan areas are betting on public transportation (or mass transit) to the detriment of private automobiles. Moreover, metropolitan and regional governments are putting efforts into integrating transportation means into a multimodal transport system.

Ticketing systems are a linchpin in the success of mass transit. These consist of two parts: (i) the *user* side (*e.g.* the tickets for using the transportation system) and (ii) the *service* side (*i.e.* ticket machines, turnstiles...). At the user side, transportation tickets have evolved from printed cards (controlled by ticket inspectors) and magnetic stripe cards (typically read and written at turnstiles), to smart cards and smartphone apps (*i.e.* mobile ticketing), including the electronic purchase of tickets: users can currently buy tickets in advance through

R. Berta and A. De Gloria (Eds.): ApplePies 2022, LNEE 1036, pp. 229–234, 2023.
https://doi.org/10.1007/978-3-031-30333-3_30

websites or apps, import them into digital wallets or even print them. In state-of-art *smart ticketing* systems, user tickets are stored in the chip of a smart card, or in a smartphone app. Such systems clearly benefit the environment and do not suffer from read/write errors, as in the case of magnetic stripe cards. In addition, they naturally fit into multimodal transportation since, in general, allow passengers to seamlessly hop on and off buses, trains, bicycles, and the like. On the whole, smart ticketing aims at encouraging people to use public transportation because of its convenience: *i.e.* does away with the need for cash, can decrease the time it takes to board transport, and, all in all, play a key role in emerging models, *e.g.* Mobility as a Service (MaaS) [1].

1.1 Security, Privacy and Ticketing Systems

Fare collection is a crucial aspect of ticketing systems, which must fulfil some security requirements [4], namely: *integrity* (*i.e.* tickets shall not be manipulated and its verification should be possible by all parties), *unforgeability* (*i.e.* tickets can only be issued by authorised authorities), and *non-overspending.* In addition, ticketing systems must also cope with *fairness* (*i.e.* if a user presents a valid ticket, the service provider shall provide the service linked to that specific ticket), *portability*, *flexibility* (*i.e.* allow the use of tickets in different transport means within the same city) and *availability.*

Certainly, modern ticketing systems must be designed, developed and deployed considering security of systems, networks and the information. Moreover, the privacy of users (*i.e.*, location tracking, transportation habits...) must be tackled to mitigate the Big Brother effect. In order to achieve such deployments and the aforementioned properties, cryptographic tools are needed. Nevertheless, the constrained resources in some of the actors involved in the ticketing system must be considered.

1.2 Contribution and Plan of the Paper

In this paper we overview the techniques and tools currently available in the user side of smart ticketing systems. The rest of the paper is organised as follows. Section 2 introduces the actors involved: smart cards and cryptographic protocols, Sect. 3 reviews outstanding current proposals and, finally, Sect. 4 concludes the paper. Addressing a general approach to security (DDoS attacks, physical layer attacks, countermeasures, etc.) and privacy aspects is out of the scope of the paper.

2 Tools at the User Side

In this section we address the elements that play a key role in the user side of a smart ticketing system, *i.e.* fare collection and ticketing validation.

2.1 Smart Cards

Plain old bank cards had to be swiped through a POS (Point of Sale) so the data embedded in the magnetic stripe could be read. Later, chips were introduced and, currently, thanks to NFC (*Near Field Communication*, which evolved from RFID, *i.e.* radio-frequency identification), the physical contact between card and reader is not required. The use of smart card technology has expanded to a variety of fields beyond payments, *e.g.* transportation ticketing systems. *Contactless smart card* communications are ruled by the ISO/IEC 14443 standard which is divided into four main sections: physical characteristics; initialisation and anti-collision; transmission protocol; radio frequency power and signal interface. Regarding the latter, cards must operate at 13.56 MHz frequency and support communication range up to 10 cm. Two deployments under the aforementioned standard are recalled next:

- **MIFARE** is a proprietary technology owned by NXP Semiconductors. Their smart cards are based on ISO/IEC 14443. MIFARE Classic (launched in 1994) introduced a proprietary encryption algorithm and authentication protocol called Crypto1. MIFARE Ultralight and DESFire were developed to protect data at low cost. The latter was designed for multi-application smart card solutions in access, loyalty program, payments, as well as public transportation. After some security flaws were found [5], it was superseded by MIFARE DESFire EV1.
- **FeliCa** is a proprietary technology created by Sony, which has become the standard smart ticketing system in Japan. It also conforms to ISO/IEC 14443.

Smart card ecosystems' security is assessed following the ISO/IEC 15408 *Common Criteria for Information Technology Security Evaluation*, which assigns the smart card platform a *Evaluation Assurance Level* (EAL). MIFARE DESFire last version achieved EAL5+ level, whereas FeliCa achieved EAL6+, which means high levels of formal verification and testing. Manufacturers' websites publish documentation that focuses on the security of the communication between the reader and the card.

2.2 Smart Card Emulation

Since NFC technology is steadily being embedded into smartphones, these devices can communicate through this technology with other NFC devices, *e.g.* another smartphone to share files, a POS to make payments or ticket validators to collect fares. Initially, the secure data related to payments (*e.g.* the credit card information) had to be stored in the so-called *Secure Element* (SE) in the smartphone: a tamper-resistant microprocessor-based element, typically the SIM card or a secure chip.

As an alternative, *Host Card Emulation* (HCE) emulates the SE, allowing the smartphone to act as a smart card from the contactless reader perspective, without the presence of an actual smart card or SE. Telecom providers and smartphone manufacturers control the access to the SE chip, thus limiting what systems could make use of it. With HCE there is a change in the paradigm: it is open to integration with other applications such as storing transport passes and holding multiple cards and wallets. Both technologies allowed major companies in the smartphone market to enable payments using not only smartphones but also other devices like smart watches (*e.g.* Apple Pay, Samsung Pay, Google Pay). However, using HCE entails some security concerns [8] and, hence, the use of cryptography and secure communication protocols and techniques like *tokenisation* (in a nutshell, no real sensitive payment data but a surrogate value is stored on the smartphone) must be considered [2]. Nevertheless, in the public transportation arena, smartphone apps entirely replacing smart cards is quite unrealistic: not everyone has a smartphone and occasional users like tourists may be refrained from installing apps due to unexpected roaming costs.

2.3 Lightweight Cryptography

Traditional cryptographic algorithms were designed for desktop and server environments where processing power and energy consumption were not a concern. With the rise of the IoT and embedded systems, the necessity arises to explore lightweight cryptography (LWC) algorithms that consider a number of aspects, namely power consumption, latency (how long it takes to perform a task), throughput (the rate the plaintext is processed by the algorithm) and resources (in terms of *Gate Equivalences*, GE).

NIST, the USA's National Institute of Standards and Technology, considers an 80-bit key length to be the minimum for lightweight cryptography. For enhanced security, 112-bit and longer are recommended. Also, according to ISO/IEC standardization, a lightweight cipher should have a GE value between 1000 and 2000. Some of the most outstanding LWC are PRESENT, which is designed from the well-known Advanced Encryption Standard (AES), CLEFIA, Enocoro and Trivium, which are included in the ISO/IEC 29192 standard. Refer to [7] for a comprehensive description of LWC protocols.

However, all in all, the AES using 128 bit keys has been shown to be suitable to resource constrained devices [3]. Due to its importance as standard, this flavour of AES is the *de facto* protocol used in real frameworks and settings: the aforementioned MIFARE DESFire, MIFARE Plus, MIFARE Ultralight and FeliCa rely on this protocol instead of implementing other LWC proposals. Some of these proposals also consider DES and 3DES; however, since these protocols have been found to be weak, NIST has deprecated their use.

3 Current Smart Ticketing Proposals

In this section, we address some example proposals for smart ticketing in public transportation which are currently in use. Some of their promoting organisations founded the *Smart Ticketing Alliance* (STA), who considers "essential that public authorities and users can be confident in the quality of contactless communication between contactless readers and fare media" [6].

- **ITSO**[1] (*Integrated Transport Smart card Organisation*) is a non-profit organization in the UK, whose specification became the national standard to regulate the interoperability of tickets across public transport operators in that country. Its ecosystem includes smart cards, the POS and the back-office processing system, which provides key management facilities in a secure datacenter, manages lifecycle cryptographic keys, etc. It makes use of AES encryption and MIFARE smart cards. Founding member of STA.
- **Calypso**[2] is an open global security standard proposed by transport operators which operates through contactless smart cards or contactless compatible devices and has been successfully implemented in 25 countries, for instance, it deploys the Paris Navigo public transportation system and others in Portugal, Italy, Mexico, Belgium, Morocco, and Israel. The specification relies on a central system, which tracks transactions, a reloading system that allows to top up cards and adds tickets to them, a validating system that grants access to transport services, and optional devices for controlling purposes such as an inspector checking a passenger has a valid ticket. Regarding cryptography, it also uses AES. Founding member of STA.
- **CiPurse**[3] is another open security standard for public transportation proposed by OSPT (*Open Standard for Public Transportation* alliance), which proposes vendor neutrality and interoperability across vendor systems. It also makes use of AES, and supports payment media such as contactless cards, wearables, whether using SE or HCE. It is used in several countries like Ecuador, Brazil or South Korea.
- **CEPAS** (*Contactless E-Payment Application Standard*) is a Singaporean standard for electronic money stored in a smart card, which proposed the use of 3DES (after an amendment, AES was adopted) and is also intended for public transportation ticketing. It is deployed in the Singapore EZ-Link transportation system.

Other deployments in real settings are not based on the aforementioned frameworks, but make use of standard smart card technologies, for instance the Hong Kong's Octopus and Tokyo's Suica use the FeliCa smart card platform. The New York metro card and Madrid's transportation system make use of MIFARE smart cards. Moreover, some public transportation systems have introduced the use of smartphone apps. Notable examples include: Hong Kong's Octopus, London's Oyster, Japan's Suica, and Singapore's EZ-Link. Finally, note that this list is not exhaustive, since there is an increasing number of smart ticketing systems being enabled [9].

4 Conclusions

The future of smart ticketing has already started and will provide several advantages not only to consumers, but also to transport operators, and all citizens liv-

[1] https://www.itso.org.uk.

[2] https://calypsostandard.net.

[3] https://www.osptalliance.org/cipurse-specifications.

ing in large cities. To this end, in this article we have described the advantages brought by the use of smart ticketing for both passengers and the environment. However, to develop this technology under the concept of "security by design" remains mandatory to guarantee, among other objectives, the integrity, unforgeability, portability and availability of the information. Although dosens of LWC encryption systems are ready to be adopted in ticketing systems, standards make use on the well-known AES-128 encryption. In addition, the gradual implementation of ticketing applications in smartphones would be a positive step towards a more efficient transportation system, although HCE systems still have to be matured from the security perspective. Future work will focus on validating the suitability of LWC in future smart ticketing systems, as well as the study of interoperability between transport providers.

Acknowledgments. This work is supported by the Government of Catalonia under grant 2020PANDE00103 (ACTUA), by URV's Institut de Ciències de l'Educació under grant 07GI2119, by MCIN/AEI/10.13039/501100011033 and "ERDF A way of making Europe" under grant RTI2018-095499-B-C32 (IoTrain), by Agència de Gestió d'Ajuts Universitaris i de Recerca under grants 2017-SGR-896, and by Universitat Rovira i Virgili with project 2021PFR-URV-118.

References

1. Butler, L., Yigitcanlar, T., Paz, A.: Barriers and risks of Mobility-as-a-Service (MaaS) adoption in cities: a systematic review of the literature. Cities **109**, 103036 (2021)
2. Europay Visa Mastercard: Payment Tokenisation. https://www.emvco.com/emv-technologies/payment-tokenisation/. Accessed 12 June 2022
3. Lara-Niño, C.A., Morales-Sandoval, M., Díaz-Pérez, A.: An evaluation of AES and present ciphers for lightweight cryptography on smartphones. In: International Conference on Electronics, Communications and Computers, pp. 87–93 (2016)
4. Mut-Puigserver, M., Payeras-Capellà, M.M., Ferrer-Gomila, J.L., Vives-Guasch, A., Castellà-Roca, J.: A survey of electronic ticketing applied to transport. Comput. Secur. **31**(8), 925–939 (2012)
5. Oswald, D., Paar, C.: Breaking Mifare DESFire MF3ICD40: power analysis and templates in the real world. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 207–222. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-23951-9_14
6. Smart Ticketing Alliance. https://www.smart-ticketing.org. Accessed 11 June 2022
7. Thakor, V.A., Razzaque, M.A., Khandaker, M.R.A.: Lightweight cryptography algorithms for resource-constrained IoT devices: a review, comparison and research opportunities. IEEE Access **9**, 28177–28193 (2021)
8. Umar, A., Mayes, K., Markantonakis, K.: Performance variation in host-based card emulation compared to a hardware security element. In: 1st Conference on Mobile and Secure Services, pp. 1–6 (2015)
9. Union Internationale des Transports Publics (UITP): Demystifying ticketing and payment in public transport. Technical report, UITP, Brussels, Belgium, November 2020