Providing Location Privacy in Automated Fare Collection Systems
(extended abstract)

Levente Buttyán Tamás Holczer István Vajda
Laboratory of Cryptography and Systems Security (CrySyS)
Department of Telecommunications
Budapest University of Technology and Economics, Hungary
{buttyan, holczer, vajda}@crysys.hu

1. Introduction

In many big cities around the world, public transport operators (PTOs) have introduced automated fare collection (AFC) systems, which greatly facilitate the collection and management of transactional data in their public transport systems. The benefits to the PTOs are clear: based on the fine grained data gathered on the usage of their services, they can optimize their transport systems, which may result in great savings, and thus, higher profit.

AFC systems offer some benefits to the passengers too. For instance, they can enable the deployment of dynamic pricing schemes, which may be advantageous for passengers. But AFC systems also present serious privacy risks. The problem stems from the fact that electronic tickets have unique and fixed identifiers. Besides making the processing of transactional data easier for the PTO, unique and fixed identifiers are also the basis for many fraud detection and prevention techniques (e.g., blacklists).

Unique and fixed ticket identifiers lead to at least two privacy problems. First, if the PTO can link particular tickets to particular persons, then it can track the whereabouts of some passengers. This could be possible, because many tickets (especially those for long term usage) may have some personal data associated with them, such as discounting rights (granted for students, elderly people, or disabled persons). By pulling together these personal data and the traces of the ticket observed in the past, the PTO may identify links between particular tickets and particular persons with high probability.

Second, in many modern AFC systems, tickets are implemented on contactless smart cards. These cards execute their transactions with card readers (e.g., a ticket validating device) through wireless channels. Although the nominal range of typical contactless smart cards used in public transport applications is only a few centimeters, it has recently been demonstrated in [4] that they can be eavesdropped from a larger distance of a few meters. Hence, it is possible to install eavesdropping equipment in an unnoticeable way at places of transactions (e.g., at the entrance of metro stations), and collect transactional data, including the unique and fixed card identifers, for later off-line analysis.

In this abstract, we address the second problem. Solutions to the first problem would require to substantially change the way AFC systems are engineered today, and PTOs would likely be reluctant to invest in that. On the other hand, the solutions that we propose for the second problem require changes only at the lowest layer of the AFC system architecture (i.e., in the protocols used between the contactless smart cards and the card readers), and they do not affect the higher layers (i.e., back-end processing).

2. Design criteria

In order to propose viable solutions to the problem described above, one needs to understand the operation of AFC systems. Here, we focus on the usage of contactless smart cards.

Smart cards are tiny computers that can store data and perform computations, including cryptographic operations. In addition to this, contactless smart cards can communicate wirelessly with card reader devices through an RF interface. In AFC systems, contactless smart cards store electronic tickets and execute ticketing transactions with card reader devices. Transactions are usually protected cryptographically. However, due to performance reasons, only symmetric key cryptographic algorithms, such as DES, are supported by smart cards (at least on the RF interface). Each card has its own symmetric key, which is created from the card identifier and a master key. This allows for card readers to store only the master key, and re-generate the card's key locally in each transaction once the card has identified itself. This is very useful, because many card readers are off-line, thus, they cannot obtain card keys from a server.

Based on this brief description, we can identify the following design criteria:

- The solution should be based on symmetric key cryptography. Thus, the simple approach of encrypting identification messages with the public key of the PTO is excluded.
- Cards should not store global secrets, because in that case a single compromised card would compromise the whole system. Thus, the simple approach of having a common group key shared by every card and card reader is excluded.
- The solution should not rely on state kept in the back-end system, because off-line card readers cannot access this state in a timely manner.
- There is a strict upper bound on transaction execution times, in order to avoid long queues of waiting passengers.

3. Proposed solutions

Key-tree based approach: The problem of using symmetric key encryption to hide the identity of a smart card during identification is that the card reader does not know which symmetric key it should use to decrypt the encrypted identity. The reader may try to generate possible card keys until one of them properly decrypts the encrypted identity, but this would increase the execution time if there are many cards in the system.

Recently, Molnar and Wagner proposed an elegant solution to this problem in the context of RFID systems [3]. Their solution is based on the concept of key-trees. We propose to adopt the key-tree based approach for private identification of smart cards in AFC systems, together with the optimization technique proposed in [1] that allows the PTO to determine the parameters of the key-tree such that the highest level of privacy is ensured while still respecting a given upper bound on the execution time.

One-time identifiers: Our second solution is based on one-time identifiers (OTIs). In each transaction, an OTI is created by the card reader and passed to the card in an encrypted form using the session key of the transaction or the card key itself. Thus, only the card can obtain the OTI. The card then uses this OTI to identify itself in the next transaction.

Due to the requirement of avoiding to keep state in the back-end system, the OTI cannot be a simple index in a table of real card identifiers, but it should be self-contained. This means that the card reader should be able to recover the card's identifier from the OTI. An easy way to achieve this is to generate the OTI by encrypting the card's identifier and some random element with a master key. Then, each card reader can decrypt any OTI to obtain the card's identifier. The random element is needed to ensure that OTIs generated from the same card identifier are unlinkable.

4. Conclusion

In this extended abstract, we identified privacy problems in AFC systems, and sketched two solutions. The full paper [2] contains more detailed descriptions. Our solutions require that the protocols currently used between the smart cards and the card readers are changed. However, once the card reader determined the real card identifier, everything can work in the same way as in today's AFC systems.

5. Acknowledgement

The work presented in this extended abstract has partially been supported by the Hungarian Scientific Research Fund (T046664) and the Mobile Innovation Center (www.mik.bme.hu). The first author has been further supported by the Hungarian Ministry of Education (BÖ2003/70).

References

[1] L. Buttyán, T. Holczer, and I. Vajda. Optimal Key-Trees for Tree-Based Private Authentication. Under submission, March 2006.

[2] L. Buttyán, T. Holczer, and I. Vajda. Location privacy in Automated Fare Collection systems. Technical Report. BME CrySyS Lab, April 2006.

[3] D. Molnar and D. Wagner. Privacy and security in library RFID: issues, practices, and architectures. In *Proceedings of ACM CCS*, 2004.

[4] K. Zetter. Feds rethinking RFID passport. *Wired News*, 26 April 2005.