Privacy for Public Transportation*

Thomas S. Heydt-Benjamin, Hee-Jin Chae, Benessa Defend, and Kevin Fu

University of Massachusetts, Amherst, MA 01003, USA
{tshb, chae, defend, kevinfu}@cs.umass.edu

Abstract. We propose an application of recent advances in e-cash, anonymous credentials, and proxy re-encryption to the problem of privacy in public transit systems with electronic ticketing. We discuss some of the interesting features of transit ticketing as a problem domain, and provide an architecture sufficient for the needs of a typical metropolitan transit system. Our system maintains the security required by the transit authority and the user while significantly increasing passenger privacy. Our hybrid approach to ticketing allows use of passive RFID transponders as well as higher powered computing devices such as smartphones or PDAs. We demonstrate security and privacy features offered by our hybrid system that are unavailable in a homogeneous passive transponder architecture, and which are advantageous for users of passive as well as active devices.

1 Introduction

Public transportation ticketing systems must be able to handle large volumes of passenger transactions while providing the minimum possible impedance to travel. Therefore, it is hardly surprising that some of the world's busiest public transportation systems are at the forefront of electronic payment technology. Unfortunately, current systems have been designed such that passengers sacrifice privacy in order to take advantage of the convenience of electronic payment. Moreover, because of the inherent broadcast nature of RF, as systems migrate from contact based technologies like mag-stripe to contactless technologies there is increased risk to privacy and security [1,2,3,4,5].

The traditional passive RFID transponder is a severely resource constrained computing device. Manufacturing cost is usually a primary design criterion, resulting in transponders with little memory and processing power. Even in more expensive passive transponders, current technology limits the amount of memory and the complexity of the microprocessor that can fit into common form-factors. Furthermore, since passive transponders are powered by electrical induction from the reader's antenna, an RFID tag must power up, receive, process, and transmit within the brief time that a user holds the tag within the reader's electric field. Consequently, many of the security protocols that we would use for communication between other kinds of computers are inappropriate for the RFID plat-

* This research was partially supported by NSF CNS-052072 and a Ford Foundation Diversity Fellowship.

G. Danezis and P. Golle (Eds.): PET 2006, LNCS 4258, pp. 1–19, 2006.

form [6]. However, despite their resource constraints, cards with cryptographic co-processors are capable of executing carefully crafted protocols [7,8,9,10,11].

As the abilities of contactless smart cards have increased, new cryptographic primitives suitable for these resource constrained devices have been developed. Not only do recent contributions to the field of e-cash and anonymous credentials require much less memory, but the communications required for the zero-knowledge proofs are also greatly reduced [12,13,14]. The key management problem for a transit system involving hundreds of readers and hundreds of thousands of tickets has traditionally been difficult. We apply recent advances in re-encryption and re-signatures to place the burden of key management on the more powerful computers in the system, requiring the tickets to store only the public portion of a single highly secure key pair whose private portion can be protected in offline storage [15,16].

1.1 Background

In 2004, passengers took approximately 9 billion trips through public transportation systems in the United States [17]. Existing systems maintain a database of all transactions, associating them with the identities of passengers whenever possible, such as when a credit card is used in conjunction with the transit card [18,19,20]. If communication between a ticket and a transit authority is not properly secured, arbitrary third party adversaries might then have inappropriate access to user data. Many of the currently deployed systems are proprietary [21], and thus closed to scientific scrutiny. Recent historical examples, such as the black-box cryptanalysis of TI's major RFID security mechanism [22], reinforce that eschewing peer review often leads to insecure systems. Even if the RF communication in a transit system is secure, the user's data may still be at risk. The Washington D.C. Metro operated for years without a clearly defined privacy policy [23,24,25]. Until recently, users of this system had no legal protection preventing the sale or sharing of their data with third parties. Privacy preserving protocols are needed to protect this large volume of sensitive data.

The utility of privacy to the individual consumer is clear, however the very consumer data that we wish to protect has long been considered valuable to the transit authority. We feel that at a certain point organizations such as transit authorities may wish to scale back on the amount of consumer data they collect. They may come to view such information as a greater liability than an asset since they stand to loose both money and reputation if the data leaks to adversarial parties. Additionally, growing public unease about ubiquitous surveillance may lead to legislation, commercial pressure, or societal pressure forcing companies to adopt stronger privacy technologies. Ultimately a new equilibrium may be achieved in which systems may be designed to permit gathering of useful business data while reassuring the consumer by providing scientific guarantees that such data will be appropriately anonymized.

Many large transit systems are still in the process of choosing and implementing new ticket technologies. The San Francisco Bay Area Rapid Transit (BART) system, for example, had over 91 million passengers in 2004 [26] and is