

# Behind the Headlines

Mifare hacking will not halt contactless ticketing for transportation systems.

By Jonathan Collin

Oct. 6, 2008—In March 2008, the Digital Security research group of Radboud University Nijmegen in the Netherlands announced that it had cloned and manipulated the contents of a contactless card using NXP’s Mifare Classic chip. In June, the same group claimed it had cloned a London Transport Oyster card, which employs the same technology, and used it to make trips on the system without paying. More than 16 million Oyster cards have been issued in the United Kingdom since the system was launched in 2003, with millions of people dependent on the contactless tickets to get them around the capital.

Both incidents resulted in news stories predicting major woes for contactless ticketing. Given the popularity of the Mifare Classic platform for transportation applications around the world—roughly 2 billion integrated circuits (ICs) have been shipped—we can expect to hear more of these stories. But while any breach of security is a concern, and the cloning of the Oyster card is no exception, a system’s security level is based on a number of checks, as well as design choices. One key choice is balancing technology costs with security requirements for each element of the system.

Transportation ticketing systems do not involve high-value sums when it comes to single trips—even in London! So Mifare—the lowest security level that NXP offers in its contactless portfolio and, accordingly, the lowest-priced IC it sells—makes sense. Ticketing systems employ more than just the entry/exit gates to ensure customers pay their fares. There are back-office checks that operate in real time, and Transport for London (TfL), the government body responsible for the citywide transportation system, maintains it can catch any cloned card at one of its gates within a few attempts.

TfL adopted contactless ticketing to help reduce fare evasion, but the automated system also gets people through the ticket barriers much faster than older magneticstripe tickets, and the reusable tickets reduce the cost and waste of issuing paper tickets for each trip. All told, that puts the benefits of Mifare ticketing systems ahead of any threat from cloning. In addition, Mifare Plus, with a new strengthened security encryption, is due by year’s end.

While the cracking of Mifare is unlikely to push any transportation operator to stop using or considering contactless ticketing, it may prompt a discussion about the future of contactless systems. Transportation companies are not particularly interested in printing and managing contactless tickets. If they could increase ticket security and offload ticket management to others, all the better.

**RELATED\_ARTICLES** The “others” are the banks and credit card companies that are promoting contactless credit and debit cards, such as MasterCard’s PayPass or Visa’s payWave. Transportation operators have the option to move from a closed payment system based on Mifare to one that accepts payments from those cards directly. Such a step could mean real benefits for commuters—but, so far, it’s the Mifare breach that makes the best headlines.

*Jonathan Collins, former RFID Journal European editor, is now a principal analyst with ABI Research. Based in London, his focus is on RFID and contactless commerce.*

Copyright ©2005 RFID Journal, Inc. All Rights Reserved