boston.com

THIS STORY HAS BEEN FORMATTED FOR EASY PRINTING

boston.com

T card has security flaw, says researcher

The Boston Globe

Cracked code could lead to counterfeits, study team warns

By Hiawatha Bray, Globe Staff | March 6, 2008

A computer science student at the University of Virginia asserts that he has found a security flaw in the technology behind the Massachusetts Bay Transportation Authority's CharlieCard system.

German-born graduate student Karsten Nohl specializes in computer security. Nohl and two fellow security researchers in Germany say they've cracked the encryption scheme that protects the data on the card. The team warns that their breakthrough could be used to make counterfeit copies of the cards, which are used by commuters to pay for MBTA bus and subway rides.

"You could have thousands of cards and sell them in the underworld," said David Evans, an associate professor of computer science at the university, and Nohl's adviser. Nohl himself is on spring break and could not be reached.

The CharlieCard uses a Radio Frequency Identification, or RFID, chip. The card is pressed against a detector, which reads data from the chip and deducts the price of a subway or bus ride from the owner's account.

The T spent $192 million to introduce the CharlieCard in 2006. The system replaced cash and tokens.

A press release issued by the University of Virginia said Nohl's research team obtained the same kind of chip, then used abrasives to scrape away the chip layer by layer. By examining the chip circuitry, they were able to figure out the encryption algorithm it uses and found weaknesses that made it easy to break. Next, the team was able to use commercially available RFID readers to capture data from any RFID-equipped cards that came within range. They could then decrypt the data on those cards and copy them. Nohl said that his team needed only about $1,000 worth of equipment to dismantle the chip and crack the code.

Nohl said that the RFID chip they compromised, the MiFare Classic by NXP Semiconductors of the Netherlands, is the one used in London's subway system and in the MBTA CharlieCard. But MBTA spokesman Joe Pesaturo refused to confirm or deny this. "It's MBTA policy not to discuss security measures around its smart card technology," he said.

A 2004 policy analysis of the CharlieCard system produced by the Massachusetts Institute of Technology said that it would be based on MiFare technology.

NXP Semiconductors issued a statement saying that Nohl's team breached only one of several security features built into the MiFare Classic chip. "This does not breach the security of the overall system," the company said. "Even if one layer were to be compromised, other layers will stop the misuse."

Evans said it might be hard to solve the issue. "There are chips that have a much higher security level available," he said. "They cost more and it is not a trivial matter to upgrade the system."

Ari Juels, chief scientist and director of computer security company RSA Laboratories in Bedford, said that Nohl's research illustrates that there are serious security flaws in many smartcard applications. "The vulnerability is most certainly for real," Juels said.

Hiawatha Bray can be reached at bray@globe.com. ■