THE CHRISTIAN SCIENCE MONITOR

Not so smart cards easily hacked

MIT students hack into Boston's transit system, highlighting security flaws in mass-transit cards.

***By Ben Arnoldy** – | Staff writer of The Christian Science Monitor*
***and Uri Friedman** – | Contributor to The Christian Science Monitor*
from the August 18, 2008 edition

Oakland, Calif.; and Boston - The recent hacking into Boston's mass transit system by three local university students underscores a much broader problem: More than a billion mass-transit fare cards and door-swipe badges worldwide have a security weakness.

That's due to a flaw revealed in a smart chip's design earlier this year. Other agencies that use the chip – from the London Tube to the Dutch government – have scrambled to adopt temporary countermeasures, says Karsten Nohl, the researcher who first uncovered the trouble. All their smart cards, he says, need to be shored up or replaced.

Three Massachusetts Institute of Technology students drove home this and other weaknesses in Boston's transit system when they claimed to have found a way to add money onto fare cards free of charge.

For now, a restraining order taken out by the Massachusetts Bay Transportation Authority (MBTA) stops the students from publicizing their work. But details are already leaking out. And their exploits come less than a year after Mr. Nohl's research had already pointed down one path to hacking such systems.

That's leaving some security experts to question the MBTA's efforts to maintain security through secrecy. "I'll predict for you that within a couple of months someone will reproduce the attack, whether or not the details were released," says Mike Davis, a senior security consultant with IOActive in San Francisco. "What these new hard-core attacks are starting to show us is that the obscurity we relied on to protect these systems are just assumptions people have made."

The MBTA spent $192 million upgrading its fare collection system in 2006, and picked a smart card system with the "Mifare Classic" chip. Mr. Nohl, now finishing his PhD at the University of Virginia, showed in December that this chip relied on a quickly crackable cipher whose only real strength turned out to be its secrecy.

"Now [MBTA officials] are trying to decide whether they should again replace everything with a third technology, or seek alternative means to combat fraud – one of which is to sue researchers," says Nohl.

Others have responded differently, he adds. London Tube officials developed a stopgap that could protect them until an upgrade becomes available. The Dutch government has dispatched security guards at key doorways once guarded only by smart cards using that technology.

However, only Boston's system has actually suffered a public hack.

Doing MBTA a good turn?

The MBTA cannot be sure that its security system is vulnerable until it has more detailed information from the MIT students, such as the report they submitted to their professor and the computer code they planned to reveal earlier this month at the DefCon hacker conference in Las Vegas, according to MBTA spokeswoman Lydia Rivera.

"If we get additional information, then we can actually make an informed and responsible decision on whether in fact their findings have merit," she says. "These students, along with the MIT staff and teachers overseeing them, have a responsibility to the public to share the information [with us] prior to making the information public or trying to make it public."

The students found flaws not included in Nohl's research and developed ways to add hundreds of dollars onto both the MBTA's new smart cards and its older-style paper tickets with magnetic strips.

As security researchers, they feel they are contributing to the public welfare by exposing critical vulnerabilities in the transit system. Transit authorities assessing their computerized systems need to sweat the details, says Zack Anderson, one of the students involved in the project.

"There are a lot of small intricacies that, if not done correctly, could result in systemwide failure," he says. "Some of the issues sometimes come down to fundamental mathematical errors like cryptography algorithms. That wouldn't be the MBTA's fault or the system integrator's fault. That would be the [fault of the] vender who sells the technology."

Mr. Anderson says the students did approach the MBTA about their findings before the conference.

Another court hearing takes place Tuesday, and researchers are warning that if the lawsuit succeeds it will poison future cooperation. "I think hackers will keep hacking, but they won't do responsible disclosure anymore," says Nohl.

Despite the legal wrangling, the cat is almost out of the bag anyway. A slide show presentation the students planned on giving at DefCon has already hit the Internet, even though they canceled the speech.

Back in March, newspapers including The Boston Globe and the Boston Herald widely publicized Nohl's findings.

MBTA's Ms. Rivera says she does not recollect those reports.

Nohl says the MBTA was aware of the vulnerabilities he outlined and that they considered implementing additional security measures. He adds that his Dutch colleagues will be publishing more explicit research on the chip's weakness in October.

"Once that paper is published, everybody can easily copy cards," he says.

John von Goeler at Scheidt & Bachmann, the system integrator for many US public transit systems including Boston's T, declined to comment.

Older system was weaker

Still, transit fare systems that don't use smart cards are often even weaker. Older-style subway tickets with magnetic stripes usually have no encryption, but they also tend to store value in a central computer rather than on the cards themselves. New York City's MetroCard doesn't even have that security.

"The monetary value of the card itself [is] stored on the magnetic stripe," says Joseph Battaglia, an electrical engineer who mapped most of the data fields on the MetroCard. "If a criminal wanted to proceed to continue the reverse-engineering effort in order to create their own cards, there would be absolutely nothing preventing them."

Nor is encryption used for highway toll collection, according to Nate Lawson, founder of the Oakland-based security consultancy Root Labs. He discovered that the Bay Area's FasTrak transponders could be tampered with remotely, even by people in nearby cars.

Adding encryption increases the costs. The MBTA could have chosen smart cards with strong cryptography, says Mr. Lawson, but since the fare cards are given out free of charge, the MBTA saved money upfront by choosing the much cheaper Mifare Classic chips.

The danger for weak systems like the MBTA's is that "somebody will take the attack and package it nicely," says Lawson.

Such systems can be sold to criminals who can then use it to churn out bogus cards to sell on the street. "Once it hits that level, that's when it costs the transit company a lot of money."

Find this article at:
http://www.csmonitor.com/2008/0819/p01s01-usgn.html

□ Check the box to include the list of links referenced in the article.