MIT students' report makes security recommendations to T

The Boston Globe

MBTA chief faults school on response

By Christopher Baxter, Globe Correspondent and Hiawatha Bray, Globe Staff | August 12, 2008

A report provided to the MBTA by three MIT students recommends that the agency implement an auditing system to detect tickets with forged encryption codes, create a central repository to store the current value of cards, and improve physical security measures in stations across Boston.

The vulnerability assessment, a confidential document that researchers said was not part of any public presentation, was included in filings after the Massachusetts Bay Transportation Authority sued Friday in federal court. A judge granted a temporary order blocking the students from publicly discussing how to hack the CharlieCard and CharlieTicket system to ride the T for free.

"There have been claims in the past that have been made against our card or other cards, and, happily, they've all been able to be dismissed or dealt with," said Daniel A. Grabauskas, general manager of the Massachusetts Bay Transportation Authority. "I'm confident it will be the same thing here."

Grabauskas lauded the judge's decision and said he was disappointed by the actions of the students and what he described as a less-than-zealous response from the Massachusetts Institute of Technology. MIT declined to comment on the pending litigation.

The MBTA sued after learning that MIT students Zack Anderson, R.J. Ryan, and Alessandro Chiesa planned to present their findings Sunday at the DEFCON hacker convention in Las Vegas. The temporary order is valid for 10 days. Then the T must prove that the students' research poses such a risk that an extended injunction is necessary. The T is also seeking unspecified financial damages, according to court papers.

"It's not a light step for a judge to grant this action, and it speaks to the strength of our arguments and the merits of our position," Grabauskas said.

But Marcia Hofmann - staff lawyer for the Electronic Frontier Foundation, a nonprofit representing the students - called the decision a "dangerous precedent for security researchers," which could potentially discourage the investigation and improvement of technology across the country.

"That certainly would discourage security researchers from discussing their work and sharing information that might ultimately make systems more secure," Hofmann said.

Anderson, a Los Angeles native and senior electrical engineering and computer science major, said the research started as a project in a network security class. He said the group was upfront with the MBTA, provided all the information it requested, and intended to help fix problems, rather than create more.

"We planned all along not to reveal the full details about what we had found," Anderson said. "We basically gave some information, but nothing that would enable someone to defraud the MBTA at all."

But Grabauskas said that the students did not disclose all their research and that he was concerned about what information not included in the written presentation might have been discussed at the conference.

Despite the agency's efforts to keep the information under wraps, much of the technology and vulnerabilities of the CharlieCard and CharlieTicket were detailed in court filings.

Regular MBTA riders usually obtain a CharlieCard, a hard plastic card that contains a Radio Frequency Identification 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. Passengers can also use a paper CharlieTicket, which has a magnetic strip that stores the data. The report states that both cards can be cloned or forged.

The students' report says the CharlieTicket has four main problems: Value is stored on the card, not in a central MBTA database; anyone that has a card can read and write it with low-cost technology; a cryptographic signature algorithm is not used on the data to prevent forgeries; and MBTA networks do not have any centralized card verification system.

The CharlieCard has some level of security through encryption, according to the report, but it can be duplicated.

"They've made claims that they've been able to in some way understand part of the code," Grabauskas said. "What we're doing is simply trying to figure out whether or not there is anything to their claims."

Karsten Nohl, a German researcher who was one of the first to crack the CharlieCard's security, said he has been comparing notes with the MIT team and hopes to come to Boston to meet them.

He may also give a public demonstration of the CharlieCard security flaw by purchasing a card and showing how to clone it, he said. ■