


EXHIBIT 1

The Tech

Established 1881

ONLINE EDITION

Volume 128 >> Issue 30 : Friday, August 8, 2008

PDF of This Issue 

CORRECTION TO THIS ARTICLE:

The Saturday, Aug. 9 Web update "Students' Subway Talk Canceled by Court Order" inaccurately stated that software used to analyze the MBTA's CharlieCard was made available online and was removed after legal action. The software had not been placed online, according to Zackary M. Anderson '09, one of the students whose talk was canceled. (This article has been revised to reflect this correction.)

WEB UPDATE

Students' Subway Security Talk Canceled by Court Order

By Michael McGraw-Herdeg and Marissa Vogt

STAFF REPORTERS

August 8, 2008

Three MIT students will not be presenting their security research at the annual DEF CON hacker convention this weekend because of a temporary restraining order filed by the Massachusetts Bay Transportation Authority on Friday afternoon. The students — legally represented by the Electronic Frontier Foundation, a nonprofit advocacy group — are appealing the order.

Zackary M. Anderson '09, Russell J. Ryan '09, and Alessandro Chiesa '09 planned to present research on Sunday that would have shown how the MBTA's CharlieTicket could be reprogrammed to contain up to \$655.36 using a \$200 magnetic stripe writer. The students would also have



MARISSA VOGT—THE TECH

(from left) Alessandro Chiesa '09, Russell J. Ryan '09, and Zackary M. Anderson '09 appear at a press conference held by the Electronic Frontier Foundation to discuss their canceled presentation titled "The Anatomy of a Subway Hack." The presentation, which would have been held Sunday at the 2008 DEF CON hacker convention, was pulled because of a temporary restraining order filed by the Massachusetts Bay Transportation Authority.

discussed the CharlieCard. According to a vulnerability assessment written by the students for the MBTA, the CharlieCard can be read wirelessly and also stores information about its balance on the card.

Article Tools

The MBTA's complaint says that they intend to sue the students on several charges. In "Count III: Conversion," the complaint alleges that "the MIT Undergrads exerted dominion over MBTA's property by traveling on the MBTA lines without paying fares." But Anderson said in an e-mail that "we never rode the T for free." Anderson said that

at Saturday's hearing, the MBTA alleged they anticipated a loss of more than \$5,000 in fares because of the students' research. EFF attorney Marcia Hofmann said that the EFF would represent the students defending against the subpoena, but that the EFF would rethink its support of the students if the MBTA files further suits. (The EFF has no staff attorneys licensed to practice in Massachusetts.)

The CharlieTicket vulnerabilities were discovered in the spring by a team of four 6.857 (Computer and Network Security) students working on a final project, but the MBTA was not notified. Three of the students are those named in the MBTA's suit. The fourth student, Samuel G. McVeety G, did not participate in the DEF CON presentation preparation, Anderson said, and was not named in the MBTA's complaint. Anderson, Ryan, and Chiesa continued to research the CharlieCard and they submitted their findings to DEF CON.

Though the presentation itself has been canceled, the presentation slides and confidential vulnerability report the students wrote for the MBTA are now widely available online. Still unavailable is some key information that would complete the attack and let people copy transit cards or add money to their CharlieTickets. It is unclear whether the students had managed to copy or edit the content of the CharlieCard, but their presentation included a detailed discussion of weaknesses in the card's encryption.

According to the presentation, the students wrote software to generate and analyze cards like the CharlieCard to crack encryption keys on those cards, and they wrote software to read and duplicate cards like the CharlieCard. That software was to have been put online days ago, but the students did not put it on a Web site advertised in their presentation, Anderson said. Researchers around the world have studied for several years the MIFARE Classic card, used by the CharlieCard, London's Oyster card, and the Dutch public transit system.

For court documents and a copy of the presentation, which was distributed to all DEF CON attendees, see <http://www-tech.mit.edu/V128/N30/subway/>.

Lawsuit surprised students

The lawsuit surprised many DEF CON attendees, who are accustomed to relatively cordial relations with software companies who are informed of security holes. It also surprised the students, who said they had until then gotten positive reactions from the MBTA.

The lawsuit was filed late Friday afternoon, just two days before the presentation. But MBTA officials had been aware of the talk since at least July 30, when a vendor told them about a description of the talk online at defcon.org. The students had also been in contact with the MBTA since July 31 through Ronald L. Rivest, the professor who had overseen their 6.857 project. Rivest could not immediately be reached for comment.

On Monday, Aug. 4, MBTA representatives met with Rivest, the three students, and an MIT staff attorney to discuss the planned presentation. Anderson said that the students met in order to tell MBTA representatives information about the vulnerabilities which they did not intend to disclose publicly. As a result of that meeting, the students wrote a confidential report for the MBTA explaining the vulnerabilities they had discovered. Leaving the Monday meeting, the students felt that the issue had been resolved based on verbal comments and that they would not face legal action, Anderson said.

At around the time that they delivered their five-page vulnerability assessment report on Friday afternoon, the three students learned that the MBTA had filed a complaint in Massachusetts District Court. The students were not provided notice until the MBTA had already sent lawyers to the court to file the complaint, said Kurt Opsahl, a senior staff attorney for the Electronic Frontier Foundation.

The students worked with EFF staff throughout Friday night to prepare a response. "We haven't slept since Thursday," Anderson said Saturday afternoon. EFF attorneys participated in a Saturday morning hearing via teleconference.

On Saturday afternoon, Judge Douglas P. Woodlock issued an order prohibiting the students and "all persons in active concert or participation with any of them" from "providing program, information, software code, or command that would assist another in any material way to circumvent or otherwise attack the security of the Fare Media System." Most of the information about the vulnerabilities were publicized by the MBTA's inclusion of the presentation slides and the vulnerability assessment report in their complaint, available online.

A temporary restraining order is issued when a judge believes a future lawsuit is likely to succeed on its merits, that the restraint will prevent an irreparable harm, that the order will not irreparably harm the restrained party, and that the public interest weighs in favor of the restraint. A detailed explanation of the judge's reasoning was presented orally at the hearing; an audio recording was made by the court but is not yet available.

"The court's order is an illegal prior restraint on legitimate academic research in violation of the First Amendment," Jennifer Granickpeech, an EFF representative, said in a press release issued by the EFF. Nevertheless, the students cancelled their talk on the EFF's advice. "We disagree with the ruling," but they intend to follow it, Opsahl said. Opsahl said that the court's ruling was based on a misinterpretation of the Computer Fraud and Abuse Act.

The complaint lists Anderson, Ryan, and Chiesa as defendants, as well as Rivest, MIT, President Susan J. Hockfield, Chancellor Phillip L. Clay PhD '75, and the MIT Corporation. Opsahl said that only the three students were treated as defendants by the courts. "We can't comment on pending litigation," said Pamela D. Serfes, an MIT News Office representative.

MIT lawyers were helpful but did not represent the students. "We have aligned interests, but they're not representing us," Anderson said.

Representatives of the MBTA were not available for comment.

Responsible disclosure?

The students did not successfully talk with the MBTA about the problems they discovered until July 31, only 10 days before the research was to be proposed. (They tried to contact the MBTA through Rivest about a week earlier, but he did not get in touch until July 31.) Computer security researchers traditionally tell companies about problems they find, give them some time to correct the problems, and only then disclose the vulnerabilities in public, in a process called "responsible disclosure" within the community.

Security expert Phil Zimmerman said that traditionally researchers give at least a month after notification before they disclose a vulnerability in a software system. In hardware systems such as the MBTA's magnetic-stripe and RFID card system, where fixing the vulnerability could possibly take more time, researchers usually offer more time, he said. "If it was me, I would've tried to give them more time to fix it," Zimmerman said. But, he said, "public disclosure is a good thing," because intense public scrutiny can help force people to fix systems.

Should security researchers explore systems which could be critical to security, like public transportation? Well, Zimmerman said, "try not to do anything that involves hiring a criminal defense lawyer."

When an important problem has been discovered with little time until it is publicly announced, Zimmerman said, an organization like the MBTA should fix it immediately. Because lawsuits generally result in security vulnerabilities becoming even more visible, the MBTA should "be thinking a lot about engineering right now and not litigation," in

terms of loss mitigation, he said. If the system is irreparably broken, Zimmerman said, the MBTA might consider switching back to an older form of subway authentication: tokens.

"It's very easy to fix," said Brenno de Winter, a Dutch journalist and security analyst. "In the Netherlands, we've got a system that works. It's called paper," he said.

Dan Kaminsky, a security researcher who recently discovered a serious vulnerability in the domain name system underlying the Internet, said that the students' disclosure could have been handled more gracefully. But the MBTA also responded inappropriately, he said, by suing the students instead of just asking for time.

Many computer software vendors are accustomed to learning of security vulnerabilities from researchers in the responsible disclosure model, Kaminsky said. "You can expect cooperation from software vendors in a way that you could not expect six years ago," Kaminsky said. But the MBTA is not a software company, Kaminsky noted. They may never have before encountered people interested in testing their security for free, a common occurrence outside of the software realm, Kaminsky said. This was an unpredictable "first-contact scenario," he said.

"If your goal is to limit discussion, this [restraining order] is not the way," Kaminsky said. "Suppressing talks in a culture that values freedom of speech just highlights the speech you're trying to suppress."

Patrick Cruce contributed to the reporting of this article.