UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY, Plaintiff, v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY, Defendants.	Civil Action No. 08-11364-GAO

DECLARATION OF CORYNNE MCSHERRY IN SUPPORT OF MOTION FOR RECONSIDERATION OF TEMPORARY RESTRAINING ORDER

I am an attorney with the Electronic Frontier Foundation, co-counsel for the Defendants Zack Anderson, RJ Ryan, and Allesandro Chiesa in the above-captioned matter. I have personal knowledge of the matters stated in this declaration. If called upon to do so, I am competent to testify to all matters set forth herein.

1. Attached hereto as Exhibit 1 is Hiawatha Bray, *T Card Has Security Flaw, Says Researcher*, Boston Globe, Mar. 6, 2008, downloaded August 17, 2008 from http://www.boston.com/business/articles/2008/03/06/t_card_has_security_flaw_says_researcher.

2. Attached hereto as Exhibit 2 is Marie Szaniszlo, *Research: Charlie Card is Far From Hack Proof*, Boston Herald, Mar. 6, 2008, downloaded August 17, 2008, from http://news.bostonherald.com/news/regional/general/view.bg?articleid=1078138.

3. Attached hereto as Exhibit 3 is Bruce Schneier, *Why Being Open About Security Makes Us All Safer in the Long Run,* The Guardian, Aug. 7, 2008, downloaded

August 17, 2008, from http://www.guardian.co.uk/technology/2008/aug/07/hacking.security.

4. Attached hereto as Exhibit 4 is *MIT Blocks Students from Revealing Fare Tips*, Boston Globe, Aug. 10, 2008, downloaded August 17, 2008 from http://www.boston.com/news/local/massachusetts/articles/2008/08/10/mbta_blocks_mit_students_from_revealing_fare_tips/.

5. Attached hereto at Exhibit 5 is Christopher Baxter, *MIT Students' Report Makes Security Recommendations,* Boston Globe, Aug. 12, 2008, downloaded August 17, 2008 from http://www.boston.com/news/education/higher/articles/2008/08/12/mit_students_report_makes_security_recommendations_to_t/.

6. Attached hereto as Exhibit 6 is George Hulme, *MBTA: Legally Shackling Security Researchers Rarely Works*, InformationWeek Security Weblog, Aug. 14, 2008, downloaded August 17, 2008, from http://www.informationweek.com/blog/main/archives/2008/08/mbta_legally_sh.html.

7. Attached hereto as Exhibit 7 is Marie Szaniszlo, *Board Member Demands MBTA Audit*, Boston Herald, Aug. 13, 2008, downloaded August 17, 2008 from http://news.bostonherald.com/news/regional/politics/view/2008_08_14_Board_member_demands_MBTA_audit/srvc=home&position=also.

8. Attached hereto as Exhibit 8 is Maddie Hanna, *Court Tells Students to Disclose Hacker Secrets in T Case*, Boston Globe, Aug. 14, 2008, downloaded August 17, 2008 from http://www.boston.com/news/local/articles/2008/08/15/court_tells_students_to_disclose_hacker_secrets_in_t_case/.

9. Attached hereto as Exhibit 9 is Boston Globe Editorial Board, *Hacking and Free Speech*, Boston Globe, Aug. 14, 2008, downloaded August 17, 2008 from

http://www.boston.com/bostonglobe/editorial_opinion/editorials/articles/2008/08/14/hacking_and_free_speech/?page=full.

10. Attached hereto as Exhibit 10 is KiMae Heussner, *Leading Computer Scientists Defend Student Hackers*, ABCnews.com, Aug. 14, 2008, downloaded on August 17, 2008 from http://www.abcnews.go.com/Technology/story?id=5581876&page=1

11. Attached hereto as Exhibit 11 is Marie Szanislow, *MIT Students Must Turn In Charlie Card Data Today*, Boston Herald, Aug. 15, 2008, downloaded on August 17, 2008 from http://news.bostonherald.com/news/regional/general/view/2008_08_15_MIT_students_must_turn_in_CharlieCard_data_today/.

12. Attached hereto as Exhibit 12 is Robert Caron, *Missed Opportunity On MBTA Security*, Letters to the Editor, Boston Globe, Aug. 16, 2008, downloaded Aug. 17, 2008 from http://www.boston.com/bostonglobe/editorial_opinion/letters/articles/2008/08/16/missed_opportunity_on_mbta_security/.

13. Attached hereto as Exhibit 13 is Harvey Silverglate, *National Security and Free Speech*, Boston Globe, August 16, 2008, downloaded August 17, 2008 from http://www.boston.com/bostonglobe/editorial_opinion/oped/articles/2008/08/16/national_security_and_free_speech/.

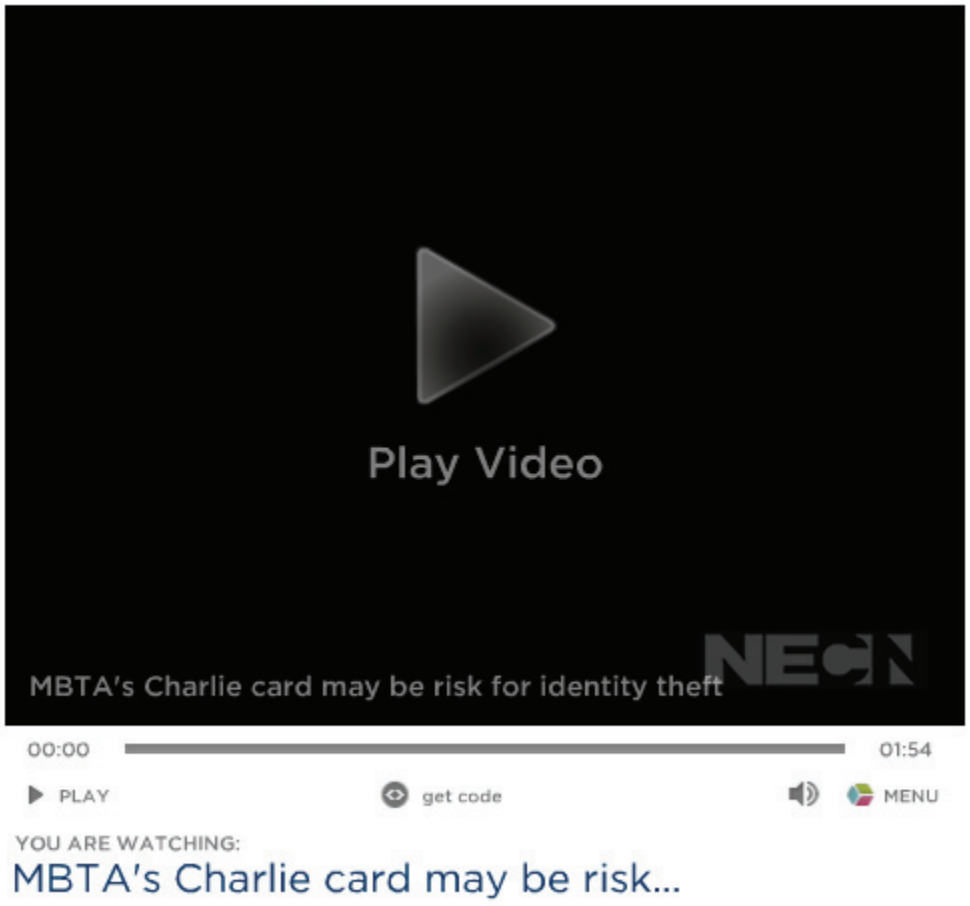
14. Attached hereto as Exhibit 14 is Ben Arnoldy and Uri Friedman, *Not So Smart Cards Easily Hacked*, Christian Science Monitor, August 18, 2008, downloaded August 18, 2008 from http://www.csmonitor.com/2008/0819/p01s01-usgn.html.

Signed under penalty of perjury this 18th day of August 2008 in San Francisco, California.

__/s/_____
Corynne McSherry, Esq.

boston.com

THIS STORY HAS BEEN FORMATTED FOR EASY PRINTING



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. ■

Research: CharlieCard is far from hack-proof

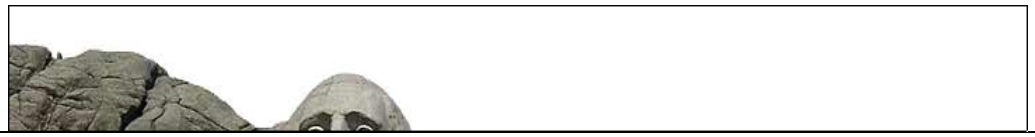
By Marie Szaniszlo | Thursday, March 6, 2008 | http://www.bostonherald.com | Local Coverage

New research by a University of Virginia graduate student shows that “smart cards” like the CharlieCard may be vulnerable to cyber thieves, who potentially could steal fares or sell counterfeits.

The incentive for theft could increase if state officials proceed with plans to allow commuters to use a CharlieCard not only to ride the T, but also to pay Mass Pike tolls and access government-run parking facilities, with funds being automatically withdrawn from their bank account.

Related Articles:

MIT students must turn in CharlieCard data today
/news/regional/general/view.bg?articleid=1113095



guardian.co.uk

Why being open about security makes us all safer in the long run

Bruce Schneier
The Guardian, Thursday August 7 2008

London's Oyster card has been cracked, and the final details will become public in October. NXP Semiconductors, the Philips spin-off that makes the system, lost a court battle to prevent the researchers from publishing. People might be able to use this information to ride for free, but the sky won't be falling. And the publication of this serious vulnerability actually makes us all safer in the long run.

Here's the story. Every Oyster card has a radio-frequency identification chip that communicates with readers mounted on the ticket barrier. That chip, the "Mifare Classic" chip, is used in hundreds of other transport systems as well — Boston, Los Angeles, Brisbane, Oslo, Amsterdam, Taipei, Shanghai, Rio de Janeiro — and as an access pass in thousands of companies, schools, hospitals, and government buildings around Britain and the rest of the world.

The security of Mifare Classic is terrible. This is not an exaggeration; it's kindergarten cryptography. Anyone with any security experience would be embarrassed to put his name to the design. NXP attempted to deal with this embarrassment by keeping the design secret.

The group that broke Mifare Classic is from Radboud University Nijmegen in the Netherlands. They demonstrated the attack by riding the Underground for free, and by breaking into a building. Their two papers (one is already online) will be published at two conferences this autumn.

The second paper is the one that NXP sued over. They called disclosure of the attack "irresponsible," warned that it will cause "immense damages," and claimed that it "will jeopardize the security of assets protected with systems incorporating the Mifare IC." The Dutch court would have none of it: "Damage to NXP is not the result of the publication of the article but of the production and sale of a chip that appears to have shortcomings."

Exactly right. More generally, the notion that secrecy supports security is inherently flawed. Whenever you see an organization claiming that design secrecy is necessary for security — in ID cards, in voting machines, in airport security — it invariably means that its security is lousy and it has no choice but to hide it. Any competent cryptographer would have designed Mifare's security with an open and public design.

Secrecy is fragile. Mifare's security was based on the belief that no one would discover how it worked; that's why NXP had to muzzle the Dutch

researchers. But that's just wrong. Reverse-engineering isn't hard. Other researchers had already exposed Mifare's lousy security. A Chinese company even sells a compatible chip. Is there any doubt that the bad guys already know about this, or will soon enough?

Publication of this attack might be expensive for NXP and its customers, but it's good for security overall. Companies will only design security as good as their customers know to ask for. NXP's security was so bad because customers didn't know how to evaluate security: either they don't know what questions to ask, or didn't know enough to distrust the marketing answers they were given. This court ruling encourages companies to build security properly rather than relying on shoddy design and secrecy, and discourages them from promising security based on their ability to threaten researchers.

It's unclear how this break will affect Transport for London. Cloning takes only a few seconds, and the thief only has to brush up against someone carrying a legitimate Oyster card. But it requires an RFID reader and a small piece of software which, while feasible for a techie, are too complicated for the average fare dodger. The police are likely to quickly arrest anyone who tries to sell cloned cards on any scale. TfL promises to turn off any cloned cards within 24 hours, but that will hurt the innocent victim who had his card cloned more than the thief.

The vulnerability is far more serious to the companies that use Mifare Classic as an access pass. It would be very interesting to know how NXP presented the system's security to them.

And while these attacks only pertain to the Mifare Classic chip, it makes me suspicious of the entire product line. NXP sells a more secure chip and has another on the way, but given the number of basic cryptography mistakes NXP made with Mifare Classic, one has to wonder whether the "more secure" versions will be sufficiently so.

• *Bruce Schneier is a security technologist and author: schneier.com/blog*

boston.com

THIS STORY HAS BEEN FORMATTED FOR EASY PRINTING

MBTA blocks MIT students from revealing fare tips

Associated Press

August 10, 2008

BOSTON --The Massachusetts Bay Transportation Authority is suing three MIT students who say they've found security flaws in the T's automated fare system.

The three planned to make their findings public at a Las Vegas computer hacker conference, but the MBTA was granted a court injunction barring them from revealing what they found about the CharlieCard and CharlieTicket system.

The MBTA alleges in court documents that the three claimed to have circumvented the security protocols of the ticketing system, according to the Boston Sunday Globe. The suit claims the three offered free subway rides for life to people over the Internet.

The suit also named MIT as a defendant.

Lawyers for the three did not return phone calls to the Globe.

Information from: The Boston Globe, http://www.boston.com/globe ■

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. ■

InformationWeek's Security Weblog

Topics: Security

- E-mail this page
- | Print this page
- | BOOKMARK

MBTA: Legally Shackling Security Researchers Rarely Works

Posted by **George Hulme**, **Aug 14, 2008 05:18 PM**

As many security and technology followers know, three MIT students had planned on presenting their findings on a number of vulnerabilities they found in the Massachusetts Bay Transportation Authority's CharlieTicket and CharlieCard payment cards at last week's Defcon conference. That was, until a gag order was put in place to keep them quiet. Today, a federal judge in Boston let the temporary restraining order stand. And so this Saga of Stupidity continues.

The hearing held in Boston today was to decide if it was OK for the MIT students to talk about the bevy of vulnerabilities they found in the Boston T. And let me tell you, if Russell Ryan, Zack Anderson, and Alessandro Chesa's presentation slides are an accurate indication of the state of security in the city's transportation system, one of the important questions remaining is why hasn't the Boston T been pwned long, long ago. We're talking about a system rife with all kinds of vulnerabilities. In fact, it may very well already have been compromised.

Part of their scheduled talk, Anatomy of a Subway Hack, would have provided details in how it's possible to generate stored-value fare cards, reverse engineer magstripes, and tap into the fare vendor network. And I think it's reasonable to assume others already have figured some of this out.

Because U.S. District Judge George O'Toole has decided not to decide until next Tuesday, this story may not move forward until Aug. 19.

The problem of trying to solve security vulnerabilities like this through the legal stifling of speech are manifold. Like the fact that it does nothing to solve the underlying security problems, and steals energy away from actually mitigating the problem. Chris Wysopal summed it up very well in his Zero In A Bit blog at VeraCode:

> "Security problems go away by mandating independent security testing before a product is accepted, not by trying to get security researchers to be quiet. This is a good example of how the reactive approach doesn't work. The flaws are still in the system and suing researchers has just shined a bright light on them."

Wysopal is right, and if the energy used to stifle the MIT students from publishing their research had been used to test the payment systems before it was deployed, you'd be reading about something else right now. So if you're upset at these researchers for finding these flaws, your anger is misplaced: it should be directed at the authorities for buying such a sheep of a system.

The idiocy of this all, especially now, is that the student's PowerPoint presentation was given to the thousands of Defcon attendees, and a 5-page vulnerability analysis already has become public. Not to forget, as ZDNet's Richard Koman noted earlier, that the MBTA, in its legal compliant, put a 30-page confidential report written by the students into the public record.

« Detecting Counterfeit Cisco Equipment | Main | Energy-Efficient Ethernet In The Data Center »

Discuss This

2 message(s). Last at: Aug 15, 2008 10:45:45 AM

p.s. I forwarded this like to my eastcoast inlaws. Some of them live in Boston.

So what you are saying is that if I track down which U.S. District Court has Judge O'Toole I can then run down the case and read the entire 30 page explaination of how to ride the subway for free? If I lived in Boston or any other city that used products from the same vendor I would be a travellin' man. Awsome!

Add Your Comment:

Post as user

Please login or register here for a free Techweb account to post

Post as guest

Name

Important Note: This comment area is NOT intended for commercial messages or solicitations of business.

Please enter the word you see below

Submit Comment

Board member demands MBTA audit

By Marie Szaniszlo | Thursday, August 14, 2008 | http://www.bostonherald.com | Local Politics

Photo by Herald (file)

A member of the MBTA's board of directors yesterday waged an all-out assault on the agency's general manager, demanding an audit and saying she had lost confidence in him and in the safety and security of the T.

At a board meeting, Janice Loux cited a series of incidents that had occurred on Daniel A. Grabauskas' watch, from a fatal Green Line accident in May to three MIT students' claims that the CharlieCard, the T's automated fare collection system, is vulnerable to hackers.

"I have grave concerns today," Loux said, "and I have lost confidence in the general manager."

Bernard Cohen, the board's chairman and the state's transportation secretary, said he had asked Grabauskas to review the T's safety record and procedures after the Green Line trainwreck that left 24-year-old operator Terrese Edmonds dead.

"I have confidence in the safety of the MBTA system," Cohen said. "We can all do better in this area. No accident is acceptable . . . But the general public should feel safe riding the MBTA."

But Loux called for an outside audit, noting that safety was not the only issue.

The T gave a no-bid contract for CharlieCard services to a former government employee, she said. And, in addition to finding security problems with the CharlieCard, MIT undergrads Zack Anderson, R.J. Ryan and Alessandro Chiesa also claim to have found unlocked turnstile control boxes, control and surveillance rooms left unattended and keys left in unlocked boxes in public areas, Loux noted.

"This reaffirms my concerns about safety and security," she said.

The board will decide the scope of any audit in the coming weeks before deciding whether to proceed with one.

In the meantime, lawyers for the MBTA are due in court this morning to try to block the MIT students from releasing any information that could jeopardize the T's fare collection system.

"We just want to make very clear that we're not interested in quashing anyone's First Amendment rights," Grabauskas said, declining to respond to Loux's criticisms. "All we're really asking is that the court bar the release of any nonpublic information that might adversely affect the CharlieCard's security."

Article URL: http://www.bostonherald.com/news/regional/politics/view.bg?articleid=1112940

Related Articles:

MBTA worker nabbed in 'drop-box' scheme
/news/regional/general/view.bg?articleid=1113522

Critics rail over MBTA raises
/news/regional/politics/view.bg?articleid=1113247

MIT students must turn in CharlieCard data today
/news/regional/general/view.bg?articleid=1113095

0.04444 : cached : hawk.heraldinteractive.com
ma20041112940_2008-08-13 22:31:03_text_1_0_0

Court tells students to disclose hacker secrets in T case

The Boston Globe

Refuses to lift order prohibiting public discussion

By Maddie Hanna, Globe Correspondent | August 15, 2008

A federal judge yesterday refused to lift an order prohibiting three MIT students from publicly talking about how they allegedly hacked into the MBTA's automated ticketing system. However, he did order the trio to privately provide more information to the court about the security flaws they say they have uncovered.

US District Judge George A. O'Toole Jr., granting a request by the MBTA, ordered Zack Anderson, Alessandro Chiesa, and R.J. Ryan to provide him with a paper they wrote for a class at MIT and correspondence they had with the organizers of Defcon, a Las Vegas hacker convention where the students were slated to speak last Sunday on alleged security flaws in the MBTA's system.

The judge said he needed to know more to "enable me to make a sounder decision about the facts of the case." He ordered the students, who were not present, to provide the information by 4 p.m. today. He said he'll weigh all the facts, then hold another hearing Tuesday on whether to dismiss or extend the 10-day restraining order that was issued Saturday and prevented the students from giving their presentation at the convention.

The MBTA filed suit last week, alleging trespass and computer fraud by the students and negligence by the Massachusetts Institute of Technology after a vendor spotted promises of "free subway rides for life" on a website advertising the students' presentation.

After yesterday's hearing, Jennifer Granick, a San Francisco attorney who represents the students, dismissed those promises as "puffery" and said the students had used "florid language" to drum up interest in their presentation.

In court, Granick, who is civil liberties director of the Electronic Frontier Foundation in San Francisco, said the students have already provided "the entire universe of information," including material they never intended to release about security flaws, in a 30-page sealed document provided to the court earlier this week.

Granick argued that the restraining order is an unconstitutional gag order that has done "irreparable harm" to the students and the First Amendment. Granick said the students have acted responsibly and "never intended to release important information that would allow or teach a bad guy" to hack into the system.

MBTA spokesman Joe Pesaturo said the students have not provided the MBTA with enough information for officials to know whether the system's security is endangered. "We simply want them to provide the information that's been requested by the court or the MBTA," he said.

Ieuan G. Mahony, a Boston lawyer who is representing the MBTA, said after the hearing that some form of a restraining order is necessary until the agency has fixed any flaws that may exist.

The MBTA contends that the students had a responsibility to share their findings with agency officials before making them public so the agency would have time to fix the problems before they could be exploited, Mahony said.

After the hearing, Granick said the restraining order is "preventing them from talking about what they found, even though there's a public debate. If these students figured it out, other people could figure it out, too."

She said today's deadline would be difficult to meet because Anderson is not in the country and Ryan and

Chiesa are not in Boston. ■

GLOBE EDITORIAL

The Boston Globe

Hacking and free speech

August 14, 2008

THREE MIT students claim to have identified ways of hacking the MBTA's automated fare-collection system, and they could have spared themselves some trouble had they notified the transit agency of any security flaws right away. The T found out about their work only after they made plans to describe their discoveries last Sunday at DEFCON, a conference for hackers. On Saturday, the agency persuaded US District Judge Douglas Wood-lock to issue a temporary restraining order against the undergrads.

But what the students should have done out of moral obligation and what they have the right to do under the First Amendment are two different questions. For good reason, US courts have long been highly skeptical of prior restraints on what may be said in a public forum. Woodlock strayed into dangerous territory by restricting what the students could disclose at the conference. At a hearing today, Judge George O'Toole will hear motions to modify or lift the order. He ought to lift it.

The order had its intended effect, for the students did not give their talk. But it would be a mistake to regard them merely as mischief-makers bent on helping scofflaws ride for free. Finding security breaches in electronic systems is a legitimate, even vital, line of inquiry. The students began looking into the T's CharlieCards and CharlieTickets in conjunction with an MIT class.

The T says it wants to enforce the principle of "responsible disclosure" - the notion that a security researcher who finds a flaw in an electronic system should notify the owner and give sufficient time to fix the breach before going public.

The students and T officials met for the first time about a week before DEFCON. The transit agency argues that the students did not offer enough information to judge whether they would behave responsibly at the conference. But should the T be the arbiter of what constitutes responsible disclosure? The students' lawyer says they met the standard, because they planned to withhold from their talk key information necessary to cheat the fare collection system.

In any case, responsible disclosure, while a valuable ethical standard, is not enshrined in federal statutes, and should not trump First Amendment rights. Such rights aren't absolute; if the students were to incite others to commit crimes, they could face civil and criminal penalties. But if expression can lead to penalties after the fact, that is one more reason not to block it in advance.

The MIT undergrads and others in this field surely need to learn that, even if they have a First Amendment right to disclose their work at their discretion, it doesn't mean they always should. But the MBTA should recognize that security flaws are a design problem, not a legal one. ■

ABC NEWS

Leading Computer Scientists Defend Student Hackers

11 of the Country's Top Researchers Call Judge's Order 'Dangerous'

By KI MAE HEUSSNER

Aug. 14, 2008—

Eleven of the country's top computer scientists have come out in support of the three MIT students who were silenced by a gag order before they were able to tell a hackers conference in Las Vegas how they were able to break into Boston's subway fare collection system.

In an eight-page letter, the researchers argued that the injunction and others like it could have a "dangerous impact" on computer security research.

The temporary restraining order was meant to block discussion of how the students at the Massachusetts Institute of Technology figured out how to evade the computer system's security to change a $1.25 fare card to a $100 fare card.

In the letter filed Tuesday, the researchers, from leading institutions such as the University of California at Berkeley and Columbia University, urged the court to remove the restraining order issued against the students Sunday.

"We are concerned that the pall cast by the temporary restraining order will stifle research efforts and weaken academic computing research programs," the letter said. The students received an A on the project from their MIT professor.

"In this case, the law gives the public a false sense of security, achieved through law, not technical effectiveness," the letter also noted.

Despite the researchers' support, U.S. District Judge George O'Toole Jr. today left the injunction intact.

According to a spokeswoman for the Electronic Frontier Foundation, the civil liberties group defending the students, the judge did not uphold or remove the temporary restraining order. Instead, he postponed the decision to another hearing that will take place Tuesday.

The judge also asked the students to turn over more documentation on their research. By Friday afternoon, the students must hand over the class report that they submitted to their professor, part of the code that was intended to be part of their presentation and e-mail correspondence with organizers of the hacking conference.

The students and their lawyers said they are moving toward the judge's deadline but also plan to appeal the ruling to the U.S. 1st Circuit Court of Appeals.

"These restraints on the students' speech is flatly unconstitutional," said Rebecca Jeschke, a foundation spokeswoman.

Computer security experts say the attempt to gag the alleged hackers has boomeranged -- again.

"Every single time, harassing the researcher ends up spreading the research," said Dan Kaminsky, a computer security consultant for Seattle-based IOActive, Inc.

MIT students Zack Anderson, R.J. Ryan and Alessandro Chiesa were scheduled to present their "Anatomy of a Subway Hack" Sunday at Defcon, the popular Las Vegas hackers convention. Their trip to the podium, however, was blocked when they were served with an injunction obtained by the Massachusetts Bay Transportation Authority ordering them not to talk about the flaws in the MBTA security system.

But not only had the presentation already been distributed at the Defcon convention, it had been entered into public record when the MBTA filed its complaint. In the blink of a mouse click, the slides were posted on the Internet and hackers were shaking their heads at the MBTA's attempt to block discussion of the information.

"The bottom line is independent security research is how we get more secure networks," Kaminsky said. "But because anyone can just say anything, the way we differentiate what's true from what's not is to actually show the details that can be independently verified."

The students emphasize that their objectives were not to defraud the transit authority.

"Our intention & was to find out what vulnerabilities might be present and then determine how those might be fixed," Anderson told ABCNews.com.

Most importantly, he said, the students never planned to reveal the information that would actually permit others to hack the system. The slideshow and presentation did not include the key enabling information.

Anderson said they contacted transit authority officials in late July. The purpose of the meeting was to educate them about the system's flaws and present them with possible solutions.

Early last week, Anderson said, the students met with the transportation officials. After walking representatives through their presentation, the students thought they had allayed the transit authority's fears.

But Aug. 8, they were notified that a federal lawsuit had been filed against them.

"It was a huge shocker," said Anderson.

In a complaint filed Aug. 8 with a U.S. district court in Massachusetts, the transportation authority said the students did not provide it with ample time to address the system's weaknesses. As a result, public disclosure of the flaws could cause significant damage to the transit system.

In an e-mail, a spokesman for the MBTA told ABCNews.com that, at the meeting, the students agreed to provide the transit authority with a copy of the presentation. After several days passed without receiving the information, the MBTA said it had "no choice but to seek assistance from a federal court judge."

The MBTA said it is now "reviewing the information to determine if there is any degree of substance to the claims being made by the students."

Corynne McSherry, a staff attorney with the Electronic Frontier Foundation, said injunctions such as the one requested by the MBTA chill the conversations that protect consumers from computer security threats.

The Electronic Frontier Foundation, a nonprofit group that advocates for civil liberties in the digital world, is defending the three students. The group's lawyers contend that the court violated the students' First Amendment rights to discuss their research.

"The court stopped researchers from speaking about their research traditional academic research," she said. "[It] essentially decided that talking about security vulnerabilities was somehow forbidden."

Some legal experts have a different view.

"It's one thing, for academic purposes, to do research. It's something entirely different to actually carry it out," said Peter S. Vogel, an attorney with the Dallas office of Gardere Wynne Sewell who specializes in Internet security and e-commerce. He is also an adjunct professor at the Southern Methodist University Dedman Law School.

If transit authority lawyers presented compelling evidence that the students violated state or federal laws while conducting their research, the judge would have been obligated to grant the injunction, Vogel added.

"The First Amendment doesn't protect people from breaking the law. It's a fine line to draw between violating a law and freedom of speech," Vogel said.

MIT students must turn in CharlieCard data today

By Marie Szaniszlo | Friday, August 15, 2008 | http://www.bostonherald.com | Local Coverage

The lawyer for three MIT students, who say the CharlieCard - the MBTA's automated fare collection system - is vulnerable to hackers, has until this afternoon to hand over documents detailing their claim.

U.S. District Court Judge George O'Toole Jr. gave lawyer Jennifer Stisa Granick until 4 p.m. to turn over a paper the students wrote on the topic for a class, as well as any materials they had been planning to distribute last Sunday at a hackers conference and any communication they had with conference organizers.

Stisa Granick said she had already submitted a sealed document - open only to the students, the MBTA, MIT, their lawyers and O'Toole - containing everything the students know about the CharlieCard.

Last Saturday, MBTA lawyers obtained a 10-day restraining order barring undergraduates Zack Anderson, R.J. Ryan and Allessandro Chiesa from speaking at the Las Vegas conference.

The MBTA argued their presentation could jeopardize the CharlieCard's security.

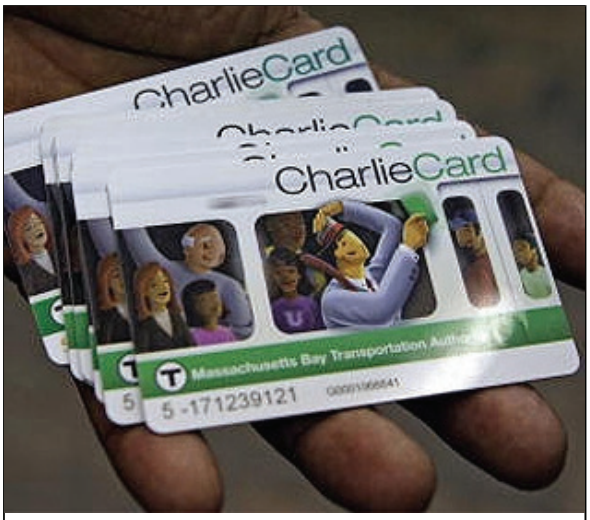


Photo by Herald (file)

But Stisa Granick said, "The question of whether the system works is a critical part of the public debate."

Article URL: http://www.bostonherald.com/news/regional/general/view.bg?articleid=1113095

Related Articles:

MBTA worker nabbed in 'drop-box' scheme
/news/regional/general/view.bg?articleid=1113522

Critics rail over MBTA raises
/news/regional/politics/view.bg?articleid=1113247

Building program's schools for scandal
/news/opinion/editorials/view.bg?articleid=1113064

boston.com

THIS STORY HAS BEEN FORMATTED FOR EASY PRINTING

Missed opportunity on MBTA security

The Boston Globe

August 16, 2008

IT'S SURPRISING to see the MBTA's actions concerning the MIT student project concerning Charlie Card security ("T sues 3 students before hacker show," City & Region, Aug. 10). This is very unlike Dan Grabauskas; I can only guess he was browbeaten by his legal staff into wielding a sledgehammer here.

Grabauskas has long been a competent, out-of-the-box state official. He has a shining track record for fixing what's broken in state agencies, often with the most innovative of solutions.

What I would have expected is Grabauskas to form some kind of team or partnership with the students, praising MIT for its students' contributions to the betterment of the Commonwealth, and reaping their undoubted expertise. Instead, it seems like both an operational and promotional opportunity missed.

ROBERT CARON
Northborough ■

HARVEY SILVERGLATE

The Boston Globe

National security and free speech

By Harvey Silverglate | August 16, 2008

WHY DID the federal district court gag three MIT undergraduates who apparently discovered a flaw in the MBTA's electronic fare-collection system? The reason one judge imposed the unconstitutional gag order prohibiting the students from presenting their paper Aug. 10 at the DEFCON computer "hackers" conference, and another judge refused on Aug. 14 to vacate that order even after the conference ended, is the current excuse du jour for an epidemic of censorship: national security.

The students, as a project for their class in computer security, discussed how the CharlieCard could be decoded and used to obtain free T rides. When the MBTA learned that they were going to present their paper at DEFCON, it sought a temporary restraining order. Judge Douglas Woodlock, sitting as emergency "duty judge," granted the T's request and prohibited the presentation -- a clearly unconstitutional decision -- citing a violation of the federal Computer Fraud and Abuse Act. Even after a follow-up Aug. 14 hearing before Judge George O'Toole, the order stands.

The Computer Fraud and Abuse Act almost certainly does not apply to mere speech; rather, it covers someone who "knowingly causes the transmission of a program, information, code, or command to a computer or computer system." In other words, the statute outlaws hacking, not a scholarly (or even unscholarly) presentation. And even if the statute could be twisted to cover the DEFCON presentation, the First Amendment's free speech guarantee would render this use unconstitutional. Yet Woodlock issued a patently unconstitutional order. Why?

This bizarre court intervention is rooted, as are many other recent civil liberties violations, in the aftermath of the Sept. 11, 2001, terrorist attacks. The MBTA's court complaint highlights "the role of the MBTA in Homeland Security efforts" and claims that the hacking threat "affects a computer system used by a government entity for national security purposes." A supporting affidavit of MBTA personnel adds that "in 2007 the MBTA received $4 million from the Department of Homeland Security . . . for use in emergency communications initiatives." Thus the T, in reality just another local transit system struggling under crushing debt and long-term mismanagement, transmogrified a temporary threat to its fare collection system into something so urgent as to override the First Amendment.

The MBTA's motion for a gag order was heard by Woodlock. Four years ago, the judge penned an opinion when civil libertarians and political activists challenged Draconian security measures aimed at severely limiting demonstrations at the 2004 Democratic National Convention in Boston. While characterizing the chicken-coop-like "free speech zone" into which protesters were to be herded outside the Fleet Center as akin to "an internment camp," Woodlock said that it was "irretrievably sad" that post-Sept. 11 security threats made such tight restrictions on otherwise protected activity necessary. "One cannot conceive of other elements [that could be] put in place to create a space that's more of an affront to the idea of free expression than the designated demonstration zone," Woodlock moaned as he facilitated the affront.

The convention security issues were, admittedly real, even if the solution was unnecessarily harsh on free speech. But the possibility of real or merely feared -- but in any event temporary -- revenue losses for the T should not qualify as the kind of extraordinary and irreparable threat that can justify a restraining order. The Supreme Court has not had occasion -- yet -- to change that high legal barrier, but some lower federal courts have nonetheless since 9/11 been setting a lower bar for the censors.

Ironically, this constitutional violation is for naught, since the order will not stop other bright minds from making the same discovery. Knowledge and its spread, for both constitutional and practical reasons, are not subject to court injunctions. The MBTA would have been better off hiring, rather than suing, the MIT trio to solve the electronic flaw. The students (and their professor) could doubtless do a better job of patching the security hole than the T's security officials, consultants, and vendors who designed the vulnerable system. But with the

ghosts of 9/11 and "national security" hovering, the students and the First Amendment didn't stand a chance.

Harvey Silverglate is a criminal defense and civil liberties litigator and writer. ■

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.