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