nature news

Published online 15 August 2008 | Nature | doi:10.1038/news.2008.1044

News

Fare's fair for hackers?

Researchers warn of 'devastating effect' of computer-science gagging order.

Daniel Cressey (/news/author/Daniel+Cressey/index.html)

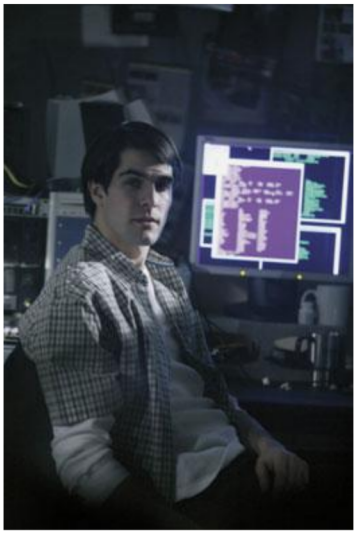
A legal ruling on a student project in the United States has thrown the computer science community into a battle over the line between legitimate research and illegal hacking. The disagreement turns on the principle of "responsible disclosure", which governs decisions by computer security researchers over when and how to make public weaknesses in commercial systems.

Eleven top-level computer scientists have publicly come out in support of a group of students from the Massachusetts Institute of Technology (MIT). The protest comes after the Massachusetts Bay Transportation Authority sought and received an order from the district court restraining the students from delivering a presentation to the annual DEFCON conference in Las Vegas. The undergraduates' talk was to be on alleged shortcomings in the security of 'smart-card' electronic tickets used by the MBTA.

According to documents the MBTA filed to the court, the students claimed to have circumvented security on e-tickets, offered "free subway rides for life" and "plan to allow others to duplicate their claimed 'breaking'".

In a letter sent in support of the students, the computer scientists say the court order is unfair and could have a devastating impact on future research.

"I find the court's decision troubling," said David Wagner, a computer scientist at the University of California Berkeley and one of the signatories to the letter, in an email to *Nature*. "If the decision is upheld, it could have a profound chilling effect on scientific research into the security of information technology."



Next step: responsible disclosure

Punchstock

Time to take stock

Experts in the area say the strategy of responsible disclosure is widely accepted for research on security topics. This involves quietly informing a product's manufacturer and users when a security issue is discovered and giving them a set period of time before you publish your findings.

"If all you do is report quietly it just gets buried and forgotten about," says Ross Anderson, a researcher at the University of Cambridge with much experience in the area. "There's been quite some debate and we've settled on responsible disclosure. This is widely accepted in the computer industry."

Exactly how much time you give the relevant companies and users is variable, says Bart Jacobs, a researcher at Radboud University Nijmegen, in the Netherlands. For a problem with a widely used software product where companies already have the intrastructure for updates, researchers might give a month. For something like a smartcard, a longer period might be necessary.

Jacobs was on the receiving end of a similar court case earlier this year when Dutch company NXP asked for an injunction to stop the publication of research on security of its Mifare Classic smartcards. These are used as Oyster cards for transport on London's trains and buses.

The injunction was refused: Jacobs plans to publish his findings later this year. "You give the manufacturer reasonable time to patch things and at the same time you put the company under pressure to really fix the problem," he says.

Indecent disclosure?

In the American case, there is disagreement between the MBTA and the MIT students over what information was provided and when.

In a statement, the students say they initially contacted the MBTA as they "wanted to let the MBTA know what they found and wanted to provide some ideas about how to fix the system". They also say their presentation would not have included crucial information needed to actually hack the fare system and that it contained less information than documents that the MBTA's court filing has now made available to the public.

"You put the company under pressure to really fix the problem"

Bart Jacobs
Radboud University
Nijmegen

An MBTA spokesman told *Nature*, "The MBTA received no pertinent information from the students before 4.30am on Saturday [the court order was granted at 1.30pm on Saturday]. We did ask for the information, and time, and got nothing." MIT declined to comment.

Yesterday, another judge at the district court ruled the restraining order — which bars the students from providing "program, information, software code, or command" that would help compromise the MBTA's fare media system – should stand. A decision is expected on Tuesday 19 August about whether it will be amended or withdrawn.

"One thing is clear — the Boston transit authority's [MBTA] actions backfired, big time," says Wagner. "The technical details are all over the Internet now. The lesson: trying to censor something just draws even more attention to it."

Comments

Reader comments are usually moderated after posting. If you find something offensive or inappropriate, you can speed this process by clicking 'Report this comment' (or, if that doesn't work for you, email redesign@nature.com). For more controversial topics, we reserve the right to moderate before comments are published.

Add your own comment

You can be as critical or controversial as you like, but please don't get personal or offensive, and do keep it brief. Remember this is for feedback and discussion - not for publishing papers, press releases or advertisements, for example. If you ramble on in an annoying way too often, we may remove your posting privileges.

You need to be registered with Nature to leave a comment. Please log in or register as a new user. You will be re-directed back to this page.

Log in / register (/news/login/index.html)