August 11, 2008

Hon. George A. O'Toole, Jr.
United States District Court
Federal District of Massachusetts
John Joseph Moakley U.S. Courthouse
Courtroom 9, 3rd Floor
1 Courthouse Way
Boston, MA 02210

Re: *Massachusetts Bay Transportation Authority v. Anderson, et. al,*
Case # 08-11364-GAO
Letter from Computer Science Professors and Computer Scientists

Dear Judge O'Toole:

We are computer scientists and researchers, many from the nation's top research and educational institutions. We write in letter form because we understand that time is short and that a temporary restraining order is currently in effect preventing the MIT student researchers from discussing their work. We hope this letter will assist you in your consideration of the Motion for Reconsideration.

Each of us engages in scientific research relating to computer systems and technologies. Each of us also engages in the routine publication and public discussion of that work. Our specific titles are listed with our signatures below.

We were quite troubled to learn that the Court has enjoined the students from discussing their research on the MBTA's fare payment system because that research might materially assist another person in defrauding the system. We write to express our firm belief that research on security vulnerabilities, and the sensible publication of the results of the research, are critical for scientific advancement, public safety and a robust market for secure technologies. Generally speaking, the norm in our field is that researchers take reasonable steps to protect the individuals using the systems studied. We understand that the student researchers took such steps with regard to their research, notably by planning not to present a critical element of a flaw they found. They did this so that their audience would be unable to exploit the security flaws they uncovered. We also believe that restraining orders such as that issued by the court over the weekend could have a devastating chilling effect on such research in the future.

Factual Background to this Letter

The focus of our letter is not on the specifics of this security research done by the MIT student researchers. Instead, we wanted to provide you with information about publishing computer security research and the dangerous impact that restraining orders such as the one issued here could have on that research.

This letter is based on our understanding of the following facts: the MIT students performed security research on the payment mechanisms for the MBTA fare collection system as part of a class project for which they received a superior grade. The students then submitted a presentation based on that research to the DEFCON security conference held in Las Vegas from August 6-10, 2008.

The students presented their research to technical representatives of the MBTA and to the FBI a few days before the conference. They also provided a confidential paper detailing the problems they found and proposed solutions. The confidential paper contained technical information not contained in their planned public presentation. The students informed the MBTA that they were not intending to release the entire results of their research, but instead were intending to withhold key pieces of information that could allow replication of their exploits. We also understand that the students engaged in puffery in advertising their presentation, stating that it would allow "free subway rides for life."

We are aware that both the slides for the intended presentation and the confidential paper have now been made widely publicly available, both through the conference materials submitted prior to the filing of the lawsuit and through filings in the public docket in this case by the MBTA.

The Nature Of Computer Systems Research

Much research in computer systems is based upon analysis - the careful examination of existing systems and approaches in order to understand what works well and what works poorly. Researchers discover flaws. They invent new and improved ways to detect and correct flaws, and they invent new and improved approaches to system design and implementation. This investigative approach has driven the computer systems field forward at an extraordinary pace for more than half a century.

Analysis is no less important when the system being studied is used to pay for public transit or any other public function. The best security systems are not one-off systems designed from scratch for single use, but designs that build upon prior

research. For this reason, it is critical that the researchers and engineers developing new systems be able to study existing ones for advantages and flaws. In turn, a system's ability to withstand repeated attacks best allows engineers and the public to trust its security. At a recent major computer security conference, for instance, about 15% of the papers presented were papers describing attacks on technical systems. Such research is broadly accepted in the profession.

The Importance Of Open Discussion And Publication To Computing Research

Open discussion of computing research and publication of its results is essential to the conduct of computing research. The computing research community is large - many thousands of individuals who follow the literature of security research. In computer science research, the "literature" includes code, algorithms, and their analysis.

Broad review and critique are fundamental to the advancement of research. There is a long history of open research in computer security and information hiding. It is no exaggeration to say that most of the security and information hiding technologies upon which we rely today are the products of this open research process.

The Importance Of Open Discussion And Publication On Public Safety And The Market

The restraining order at issue in this case also fosters a dangerous information imbalance. In this case, for example, it allows the vendors of the technology and the MBTA to claim greater efficacy and security than their products warrant, then use the law to silence those who would reveal the technologies' flaws. In this case, the law gives the public a false sense of security, achieved through law, not technical effectiveness. Preventing researchers from discussing a technology's vulnerabilities does not make them go away - in fact, it may exacerbate them as more people and institutions use and come to rely upon the illusory protection. Yet the commercial purveyors of such technologies often do not want truthful discussions of their products' flaws, and will likely withhold the prior approval or deny researchers access for testing if the law supports that effort.

As an example, computer anti-virus experts rely heavily on public dissemination of timely information about threats on the horizon. For instance, the "Code Red" worm released a few years ago was designed to spread rapidly for about a week, and it was very successful at infecting more than 200,000 computers. Security

researchers across the country rallied together in a concerted effort to blunt the attack, and discovered through last-minute reverse engineering (disassembly) that the worm was designed to make all infected machines attack the White House web server on a specified date. With only a few days to counter this threat, experts were able to study the reverse engineered worm to identify a weakness of the attack and counter it, protecting the White House web server and others. This containment of the Code Red worm would not have been possible without immediate, unrestricted public dissemination of full information about its spread, which included open discussion of the flaws it exposed in other computer software.

Similarly, in 1989 complexity theorists Adi Shamir and Eli Biham invented the technique called differential cryptanalysis, which called into question the strength of various ciphers. The research prevented weaker systems from being adopted to replace the famous DES block cipher, which was then being used by all commercial banking systems and by the U.S. government. Nonetheless, the two scientists were treated as heroes rather than criminals. The publication of a new means of attacking encryption – called differential cryptanalysis - made it possible for the research community to design the AES block cipher, which is vastly more secure as a result of this understanding and is now the federal encryption standard.

This free flow of information also helps the market. With free flow of information about the cost and quality of different payment and security schemes, market forces should lead to the production of better and cheaper schemes. By chilling the flow of information about the quality of competing fare collection schemes, orders such as that issued by the court cripple the market's ability to reward higher quality schemes.

The analogy to the research done by the MIT students is obvious. A break in the security system for payments on the MBTA system teaches how to design better systems. If a break exists it will be discovered. It is much better from everyone's perspective if researchers discover the break and publish it than if unscrupulous discoverers of the break exploit it without public notice. While the publication need not always contain every detail necessary to allow criminal exploitation of the flaw, as the students here rightly decided, the fact of the security flaw should not have been hidden from the public.

Responsible Security Disclosures

It is the case that security researchers need to make careful decisions about how much detail of a particular security break they should make public. Generally

speaking, when large public security systems are at issue, the norm in our field is that researchers take reasonable steps avoid inadvertently teaching others how to exploit the flaw. From what we understand of the facts, the MIT student researchers took such steps in planning their presentation, withholding key information about the flaws they discovered. They also intended to do the same in the future, although this might not be necessary any more since we understand that the MBTA has now voluntarily placed that same information in the public record in this case.

Yet at the same time that researchers need to act responsibly, vendors should not be granted complete control of the publication of such information, as it appears MBTA sought here. As noted above, vendors and users of such technologies often have an incentive to hide the flaws in the system rather than come clean with the public and take the steps necessary to remedy them. Thus, while researchers often refrain from publishing the technical details necessary to exploit the flaw, a legal ban on discussion of security flaws, such as that contained in the temporary restraining order, is especially troubling.

Chilling Effect of the Court's Order

The court's order, if not lifted, will chill research and publication when the technologies or systems in question are used to collect payments on public transportation. Fears of violating vaguely-defined prohibitions are expected to lead researchers to choose "safer" topics of study and to censor their publications rather than risk lawsuits.

In particular, the court's ruling that "transmission" of a computer program to a computer system could include a public presentation about flaws in the security of the system is especially troubling. It is even more so here because we understand that key portions of the research needed to duplicate the attack were not going to be presented at the conference and will not be presented in the future.

Conclusion

In sum, we are concerned that the pall cast by the temporary restraining order will stifle research efforts and weaken academic computing research programs. In turn, we fear the shadow of the law's ambiguities will reduce our ability to contribute to industrial research in security technologies at the heart of our information infrastructure. We urge that you reconsider and remove the temporary restraining order issued on August 10, 2008.

Sincerely,

Professor David Farber[1]
Distinguished Career Professor of Computer Science and
Public Policy in the School of Computer Science
Carnegie Mellon University

Professor Steven M. Bellovin
Professor of Computer Science
Columbia University

Professor David Wagner
Associate Professor of Computer Science
University of California at Berkeley

Professor Dan Wallach
Associate Professor of Computer Science
Rice University

Professor Tadayoshi Kohno
Assistant Professor of Computer Science and Engineering
University of Washington

Professor David Touretzky
Research Professor
Computer Science Department &
Center for the Neural Basis of Cognition
Carnegie Mellon University

[1] All titles are for affiliation purposes only.

Patrick McDaniel
Co-Director Systems and Internet
Infrastructure Security Laboratory (SIIS)
Pennsylvania State University

Professor Lorrie Faith Cranor
Associate Professor of Computer Science
and Engineering and Public Policy
Carnegie Mellon University

Professor Matthew Blaze
Associate Professor of Computer and Information Science
University of Pennsylvania

Stefan Savage
Associate Professor
Department of Computer Science and Engineering
University of California, San Diego

Bruce Schneier
Chief Security Technology Officer, BT