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 ZACK ANDERSON IN REPLY TO OPPOSITION TO MOTION FOR RECONSIDERATION OF TEMPORARY RESTRAINING ORDER

1. I am a student in computer science and electrical engineering at the Massachusetts Institute of Technology. I am a defendant in this matter. I have personal knowledge of the matter stated in this declaration. If called upon to do so, I am competent to testify to all matters set forth herein.
2. I am 21 years old. My fellow students RJ Ryan and Alessandro Chiesa are also defendants in this case. RJ is 22 years old and Alessandro is 20.
3. The computer science and electrical engineering program at MIT is academically demanding. I worked hard in high school to be accepted at MIT and I work hard now to maintain high academic standards now that I am a student. I have a 4.5/5 GPA.

4. I have received the following awards and honors: DARPA Grand Challenge Robotics Competition Finalist (2004), US FIRST Rookie All-Star Award (2005), George C. Newton Prize (2008), California Scholarship Foundation Award (2005), 1st Place at LA County Science Fair for autonomous robot (2003), National AP Scholar (2005), SFV Engineer's Council Robotics Engineering Excellence Award (2002).
5. I have also applied for two patents.
6. I have many extracurricular projects related to my academic areas of interest, including robotics projects.
7. RJ and Alessandro are also serious students with important extracurricular activities. My understanding is that both are also at the top of their class at MIT. Both RJ and Alessandro are on MIT's Division I rowing team, and RJ has been very involved with volunteer work. RJ has been nationally recognized for his work in computer graphics. For all three of us, our education at MIT is extremely important.
8. For the final project in one of our classes with Professor Ron Rivest, RJ, Alessandro, another student and I applied existing research on stored value cards commonly used for fare payment in transit systems to the Boston subway's CharlieCard and CharlieTicket. This experiment confirmed that an attacker could modify the CharlieTicket and presented an aspirational attack on the CharlieCard that showed that additional security measures employed by plaintiff Massachusetts Bay Transportation Authority ("MBTA") were inadequate to prevent card modifications. Our paper received an "A."
9. As part of the security research, RJ and I tested the CharlieTicket vulnerability. Allessandro did not participate in the security testing. To conduct this security

vulnerability testing, it was not necessary to (and we did not) ride the subway or otherwise use the MBTA's transportation services for free. In the course of our research we spent between $100 and $200 on MBTA stored value cards, plus hundreds more on research equipment. To put that in perspective, MIT students can obtain monthly T passes for $29.50 through MIT. *See* "Take the T to Work and Leave the Driving to Someone Else," http://web.mit.edu/facilities/transportation/tpass.html

10. The teaching assistants for Professor Rivest's class, Computer and Network Security, asked whether we would like our paper posted publicly on the class website. We said we did not want to post the paper because we wanted to have an opportunity to discuss our findings with the MBTA first.
11. On May 15, 2008, RJ, Alessandro and I submitted a talk proposal to present our research at the DEFCON computer security conference, held August 8 to August 10, 2008 in Las Vegas, Nevada. Our talk was accepted.
12. DEFCON is advertised as one of the oldest and largest hacker conferences in the world. It is the sister conference to Black Hat, which happens earlier in the week. Academics, corporate security officers, government officials and IT experts from companies like Microsoft and Google pay to attend Black Hat and get free admission to DEFCON. In addition, a lot of independent security researchers attend and speak at the conference. It is supposed to be fun.
13. In both the proposal and the abstract for our talk, we blatantly emphasized that our findings showed a security flaw that could be exploited by attackers because we wanted to sensationalize our talk and make it seem fun so that people would attend.
14. For the substance of the talk, we always planned to include existing and original

research, but to leave out information we had discovered about a checksum safeguard that the MBTA had implemented on the CharlieTicket because we believed that that information could give an attacker too much assistance in modifying the ticket or creating a false ticket. We also did not disclose details about the encryption algorithm (Crypto-1) behind the CharlieCard, some of which we do not know.

15. On Friday, July 25, 2008 we emailed Professor Rivest to ask for assistance setting up a meeting with the MBTA about our findings. We did not immediately receive a response from Professor Rivest, who was away at a conference, so we emailed again on July 30, 2008.

16. Professor Rivest called the MBTA on July 31, 2008 and then let us know that the agency was concerned about our upcoming talk and that they had contacted the FBI.

17. We set up a meeting with the MBTA for August 4, 2008. The MBTA sent Sergeant Detective Richard Sullivan of the Transit Police, and he brought a special agent from the Federal Bureau of Investigation, Jacob Shaver, with him. MBTA had not told us that an FBI agent was going to be at the meeting.

18. At the end of the meeting, Detective Sullivan did not request that that we give him a copy of our slides. Rather, we agreed to deliver a short confidential report to the MBTA summarizing our vulnerability findings and recommendations. Later that day, we received a friendly note from S.A. Shaver. We did not believe that there was any problem going forward with our talk as planned.

19. Attached as Exhibit 1 are true and correct copies of two emails I sent to Nikita Caine, an organizer for DEFCON. These emails have been provided to the MBTA in discovery.

20. To address the MBTA's concerns, we asked DEFCON to modify the abstract to make it clear that we had no intention of teaching people how to make counterfeit cards or tickets. Exhibit 1, Email from Zack Anderson to Nikita Caine, August 5, 2008, MBTA00011
21. On July 31, 2008, I informed Ms. Caine that RJ, Alessandro and I intentionally left out key details from the slides. Exhibit 1, Email from Zack Anderson to Nikita Caine, July 31, 2008, MBTA00012
22. Before DEFCON we provided a Confidential Vulnerability Report ("CVR") to the MBTA. That document contained the information about the checksum on the CharlieTicket, which we had always intended to withhold. MBTA has publicly filed the CVR in this case and it is now a public document. The three of us were surprised and concerned that the MBTA chose to do that.
23. The MBTA did not ask for copies of our slides until Friday, August 8, 2008, after we had already been told by MIT's counsel Jay Wilcoxson that he understood the MBTA was in the process of filing suit against us and seeking a temporary restraining order to keep us from giving our presentation. We decided not to send the slides to the MBTA until we had an opportunity to review the lawsuit.
24. In order to further assist the MBTA we created a longer, more detailed report about our research. We provided that report under seal in this case. This report also represents everything that we want to be able to talk about in the future regarding our research on MBTA security. Furthermore, it covers all of our significant and relevant findings about the vulnerabilities.

25. Speakers at the DEFCON conference have the option to receive a $200 honorarium or free passes to the conference. We elected to take the honorarium. This nominal compensation would not have even covered our expenses in traveling to the conference. Since we did not give the talk, we are not entitled to receive any compensation at all.
26. We did not and do not intend to publish the Class Paper.
27. We did not publish the software tools developed in the course of this research.
28. We never decided which research materials, including software code, if any, we would include or demonstrate in our final presentation at DEFCON. Our efforts to re-evaluate the materials after the MBTA expressed its concerns delayed the decision-making process. In light of the MBTA's concerns and the subsequent filing of this lawsuit, we ultimately did not finalize any software or demonstration plans for the DEFCON presentation.
29. Our research materials were never presented to the public.
30. We do not currently intend to demonstrate any research materials.

Signed under penalty of perjury this 18th day of August 2008.

\s\ Zack Anderson
Zack Anderson

Subject: Re: Revised abstract
Date: Tue, 05 Aug 2008 22:29:35 -0400
From: Zack Anderson <zacka@mit.edu>
To: Nikita Caine <barkingkitten@gmail.com>
References: <48988CC7.5060901@mit.edu>
<5dba3ce20808051926m7555b2c5o4cb74c1ddda11117@mail.gmail.com>

Thanks so much!

Zack

Nikita Caine wrote:
This should be updated on the website soon if not already, however do note the webmaster is in las vegas at the moment, and your previous abstract will be what is printed on the program.

On Tue, Aug 5, 2008 at 10:24 AM, Zack Anderson <zacka@mit.edu> wrote:

Hi Nikita,

We met with a Sargent Detective of the Intelligence unit at the MBTA and a Special Agent of the cybercrimes division of the FBI yesterday. The meeting went well, and our legal counsel has advised us that we can definitely proceed with the talk. If you don't mind, can you change our abstract on the website to this:

"In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We survey 'human factors' that lead to weaknesses in the system, and we present a novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote in the process of researching these attacks. With live demos, we will demonstrate how we broke these systems."

Thanks,
Zack

-------- Original Message --------
Subject: Revised abstract
Date: Tue, 05 Aug 2008 13:24:23 -0400

From: Zack Anderson <zacka@mit.edu>
To: Nikita Caine <barkingkitten@gmail.com>

Hi Nikita,

We met with a Sargent Detective of the Intelligence unit at the MBTA and a Special Agent of the cybercrimes division of the FBI yesterday. The meeting went well, and our legal counsel has advised us that we can definitely proceed with the talk. If you don't mind, can you change our abstract on the website to this:

"In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We survey 'human factors' that lead to weaknesses in the system, and we present a novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote in the process of researching these attacks. With live demos, we will demonstrate how we broke these systems."

Thanks,
Zack

-------- Original Message --------
Subject: Re: Defcon CD
Date: Thu, 31 Jul 2008 22:33:37 -0400
From: Zack Anderson <zacka@mit.edu>
To: Nikita Caine <barkingkitten@gmail.com>
References: <5dba3ce20807010045o46a72b5bi6700c97871711870@mail.gmail.com>
<489231BD.6030209@mit.edu>
<5dba3ce20807311734n416e4aa6pd03a9c6b6728a838@mail.gmail.com>

We still plan on giving the talk. We left out a couple of key details from the slides, so for now I think we will be alright. We are meeting with the MBTA and legal counsel on Monday. I will keep you posted if anything changes, but expect us to give the talk.

Zack

Nikita Caine wrote:
Zack,

The CD's have been printed and are on their way to Vegas, There is no way to change it at this point. Please let me know if you will be