UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

Plaintiff

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, RONALD L. RIVEST, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Defendants

Civil Action No. 08- 11364-GAO

Declaration of Eric Johanson

I, Eric S. Johanson, hereby declare:

1. I am a security consultant specializing in penetration testing and application assessments. I have worked for the last seven years on application code assessments, wireless penetration tests, and architecture reviews. My involvement with the security industry builds on five years in software development.

2. I have worked for years as an independent consultant, and I have been a member of IOActive, Levianthan Security Group, and Security Innovation. My clients have included federal and state government agencies and Fortune 500 companies.

3. I am a frequent speaker at national and international computer security conferences, including ShmooCon, H.O.P.E., and DEFCON. I am a member of the Shmoo Group, a professional non-profit computer security organization that gives me an active research role in emerging security issues. My security research work has resulted in wide coverage in the press, including academic forums and national newspapers.

4. I hold the opinions expressed herein to a reasonable degree of professional certainty. If called as a witness I could and would testify competently to the following.

5. I have reviewed the slides submitted by Defendants Zack Anderson, RJ Ryan and Alessandro Chiesa to DEFCON 16, in connection with their presentation, "The Anatomy of a Subway Hack" (hereafter the "Slides"), which is currently scheduled for Sunday, August 10, 2008.

6. DEFCON is one of the premier computer security conventions and is held every year in Las Vegas, Nevada. Attendees at DEFCON include numerous computer security professionals, along with journalists, lawyers, and federal government employees.

7. As part of my professional career, I am familiar with the literature and continually survey the publicly available research on security issues in payment systems, including magnetic stripe and Radio Frequency Identifier (RFID) based technologies.

8. For example, I have reviewed a presentation that security researchers Karsten Nohl and Henryk Plötz gave in December 2007, entitled "Mifare—Little Security, Despite Obscurity," at the 24th Chaos Communication Congress (24C3) in Berlin. This presentation documented critical flaws in the security integrity of the Mifare RFID transit payment system and generated substantial comment in the security research community. I am informed and believe that the Charlie Card uses the Mifare technology.

9. I reviewed the Slides to determine the extent to which the information presented in the Slides was already publicly known, based on my knowledge of the literature and publicly available research. I also considered whether the Slides presented sufficient information to compromise the security of the Charlie Ticket and the Charlie Card.

10. As discussed in detail below, in my expert opinion, the information presented in the Slides regarding the Charlie Ticket and the Charlie Card is already publicly known.

11. Further, in my expert opinion, key information needed to compromise both the Charlie Ticket and the Charlie Card is not present in the Slides.

The Practice of Security Research

12. Security in any particular application often depends on the soundness of many different components, as well as how these components interact with one another. Vulnerabilities can, and frequently do, arise from weaknesses in cryptographic algorithms and protocols, incorrect assumptions about the nature of attack threats, poor overall design, and human factor and user interface problems, to name but a few.

13. A significant focus of ongoing research, therefore, must be concerned with evaluating real-world security systems in an effort to discover whether they are, in fact, secure. Case studies of proposed and existing systems and standards form the essential basis for this research.

14. It is only by a thorough understanding of how real systems fail in practice that we are able to develop design principles for more secure systems in the future. Because there are no systematic techniques for ensuring the correctness of most aspects of secure systems architecture, research toward discovering vulnerabilities in systems as they are actually designed and implemented is essential for the advancement of the field. Scientific progress in this discipline necessarily depends upon the exploration of computer system weaknesses and the publication of the knowledge learned.

15. Security researchers, like all scientific and engineering researchers, necessarily rely on open publication of the knowledge learned as the means for communicating with one another and for measuring progress in the field.

16. Although presentations on security vulnerabilities often discuss how weaknesses might be exploited, prohibition of open discussion and publication of security vulnerabilities greatly harms the ability of researchers to function, and has a chilling effect not only on publication, but on whether some important research is done in the first place, greatly stifling scientific advancement.

17. Publication restrictions also encourage vulnerability research to go underground. Discouraging aboveboard, open research in legitimate institutions leads to a situation where the people who enjoy the most complete knowledge of the subject are those working unlawfully in the underground. Criminal organizations already have obvious incentives to learn how to defeat security measures. The question is whether the open scientific community and the public will be permitted to study and fix the same vulnerabilities that are visible to criminals.

18. Security researchers are drawn from many different disciplines, come from a wide range of backgrounds, and enjoy a variety of employment situations. It is not uncommon for students and non-academics to make significant contributions to the field. The set of individuals with a legitimate need to test systems for vulnerabilities and publish their results is not at all limited to those holding academic credentials or advanced educational or professional status.

Analysis of the Slides

19. The Slides describe using commercial, off-the-shelf hardware to read the data encoded on the magnetic stripe portion of the Charlie Ticket. This technique is widely known.

20. The Slides describe having written software to interact with the commercial, off-the-shelf hardware. This technique is also widely known.

21. The Slides describe applying standard, commonly used research techniques to the magnetic stripe data to categorize the data.

22. The Slides describe using the commercial, off-the-shelf hardware to write updates to the data on the Charlie Ticket magnetic stripe. This technique is widely known.

23. The Slides depict a field called "checksum," and show that it changes when the ticket value changes, but do not describe how to compute the checksum.

24. The Slides describe implementing the public standard known as ISO14443A, using commercial, off-the-shelf hardware. ISO refers to the International Standards Organization.

25. The Slides summarize and describe implementing techniques disclosed in "Reverse-Engineering a Cryptographic RFID Tag," an academic paper published on pages 185-193 of the Proceedings of the 17th USENIX Security Symposium.

26. The Slides do not describe any new techniques for breaking the cryptography used by the Charlie Card.

27. Slides 60-62 appear to be merely aspirational, and do not document successful, new vulnerabilities.

I declare under penalty of perjury that the foregoing is true and correct and was executed at Las Vegas, Nevada on this 9th day of August 2008.

_____/s/_____
Eric S. Johanson