EXHIBIT 4

The Anatomy of a Subway Hack:
Breaking Crypto RFID's and Magstripes of Ticketing Systems

Zack Anderson *Student, MIT*
RJ Ryan *Student, MIT*
Alessandro Chiesa *Student, MIT*

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.

Zack Anderson is studying electrical engineering and computer science at MIT. He is an avid hardware and software hacker, and has built several systems such as an autonomous vehicle for the DARPA Grand Challenge. Zack is especially interested in the security of embedded systems and wireless communications. He has experience building and breaking CDMA cellular systems and RFID. Zack has worked for a security/intelligence firm, and has multiple patents pending. He enjoys building systems as much as he enjoys breaking them.

RJ Ryan is researcher at MIT. His longtime passion for security has resulted in a number of hacks and projects, including a steganographic cryptography protocol. RJ works on a number of technical projects ranging from computer security to operating systems, distributed computation, compilers, and computer graphics. He enjoys learning how things work, and how to make things work for him.

Alessandro Chiesa is a Junior at MIT double majoring in Theoretical Mathematics and in Electrical Engineering and Computer Science. Born and raised in Varese,Italy, he came to MIT with interests in computational algebraic geometry, machine learning, cryptography, and systems security. He has authored papers such as "Generalizing Regev's Cryptosystem", which proposes a new cryptosystem based on shortest vector problems in cyclotomic fields. He is currently working with Oracle's Database Security group.

José Parada is an IT Pro Evangelist in Microsoft. He is a very famous speaker in Spanish conferences about IT Infrastructures, Microsoft Technologies and Security. He has been working in the Microsoft Technet Program from 2005 delivering conferences, webcasts and technical information.

Top of page

The Anatomy of a Subway Hack:

Breaking Crypto RFID's and Magstripes of Ticketing Systems

Zack Anderson*Student, MIT*
RJ Ryan*Student, MIT*
Alessandro Chiesa*Student, MIT*

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.

Zack Anderson is studying electrical engineering and computer science at MIT. He is an avid hardware and software hacker, and has built several systems such as an autonomous vehicle for the DARPA Grand Challenge. Zack is especially interested in the security of embedded systems and wireless communications. He has experience building and breaking CDMA cellular systems and RFID. Zack has worked for a security/intelligence firm, and has multiple patents pending. He enjoys building systems as much as he enjoys breaking them.

RJ Ryan is researcher at MIT. His longtime passion for security has resulted in a number of hacks and projects, including a steganographic cryptography protocol. RJ works on a number of technical projects ranging from computer security to operating systems, distributed computation, compilers, and computer graphics. He enjoys learning how things work, and how to make things work for him.

Alessandro Chiesa is a Junior at MIT double majoring in Theoretical Mathematics and in Electrical Engineering and Computer Science. Born and raised in Varese,Italy, he came to MIT with interests in computational algebraic geometry, machine learning, cryptography, and systems security. He has authored papers such as "Generalizing Regev's Cryptosystem", which proposes a new cryptosystem based on shortest vector problems in cyclotomic fields. He is currently working with Oracle's Database Security group.

Top of page

Digital Security: a Risky Business

Ian O. Angell*Professor of Information Systems. London School of Economics*

In this talk Professor Angell will take the devil’s advocate position, warning that computer technology is part of the problem as well as of the solution. The belief system at the core of computerization is positivist and/or statistical, and that itself leads to risk. The mixture of