April 20, 2006
U.S. Department of Justice
Central District of California
Debra Wong Yang
United States Attorney
Thom Mrozek, Public Affairs Officer
Contact: (213) 894-6947

San Diego Computer Expert Charged with Hacking into U.S.C. Computer System Containing Student Applications

A San Diego man has been charged with hacking into a computer system at the University of Southern California and accessing confidential information submitted by students applying to the school.

Eric McCarty, 25, was named in a criminal complaint that was unsealed yesterday charging him with knowingly having transmitted a code or command to intentionally cause damage to USC's on-line application system. McCarty, who is employed as a computer network administrator, also earns money by performing "penetration testing" designed to simulate malicious attacks on computer networks.

According to the affidavit in support of the criminal complaint, on June 17, 2005, McCarty used a computer at his home to visit USC's on-line applicant website. The applicant website, which exists for persons applying for admission to the university, requires the use of a login username and password, and allows a user to apply or modify an existing application to the school. Information for more than 275,000 applicants from 1997 through the present is stored within a sequel database, and includes data such as social security numbers and birth dates.

McCarty exploited a vulnerability in the sequel database to by-pass the password authentication used to protect the sequel database. After determining the vulnerability, McCarty staged an "SQL injection" attack to gain access to the database, which allowed him to access and copy several applicant records. Following the SQL injection attack, McCarty created an email account Ð ihackedusc@gmail.com Ð which he used to report his attack to securityfocus.com. A reporter at securityfocus.com later contacted USC and informed them that its applicant website database was vulnerable.

On June 21, 2005, the USC applicant website and SQL database were shut down as a direct result of the SQL vulnerability. The website remained off-line for nearly two weeks, causing considerable expense along with disruption to applicants.

A subsequent investigation by the Federal Bureau of Investigation led to McCarty through the Internet protocol number on his home computer.

McCarty is scheduled to make his initial appearance in United States District Court in Los Angeles on April 28. If he is convicted of the computer intrusion charge alleged in the complaint, McCarty would face a maximum possible sentence of 10 years in federal prison.

A criminal complaint contains allegations that a defendant has committed a crime. Every defendant is presumed innocent until and unless proven guilty.

The case against McCarty is the result of an investigation by the Federal Bureau of Investigation.

CONTACT:
Assistant United States Attorney Michael C. Zweiback
Cyber and Intellectual Property Crimes Section
(213) 894-2690

###