September 12, 2007
United States Attorney's Office
Southern District of Texas

Texas A&M Grad Convicted of Hacking into Alma Mater's Computer System

(HOUSTON, Texas) - A December 2006 graduate of Texas A&M University has been convicted of recklessly accessing and causing damage to the protected computer system of his former alma mater, United States Attorney Don DeGabrielle and FBI Special Agent in Charge Andrew R. Bland III, announced today.

At a hearing this afternoon before U. S. District Judge Kenneth Hoyt, Luis Castillo, 23, who graduated with a bachelor's degree in computer science from Texas A&M University in December 2006, admitted to recklessly gaining unauthorized access to the university's domain controller, code named "Ajax," a protected computer system, and capturing 133,000 network IDs and passwords of unsuspecting students and employees of the university. "Computer systems have simplified our lives and we rely upon them, particularly those within our academic institutions, to be safe, informative and secure," United States Attorney Don DeGabrielle said following the hearing. "When, as here, that security is breached, federal felony convictions will result. The Department of Justice will continue to work together with our state and local law enforcement partners to prosecute cyber criminals." "This successful investigation exemplifies the FBI's steadfast commitment to allocate the appropriate resources and expertise needed to address the FBI's number three priority, which is cyber crimes," said FBI Houston's Special Agent in Charge Andrew R. Bland III. "The FBI continues to work closely in cooperation and collaboration with state and local law enforcement, area universities, and the private sector to ensure that insidious crimes of this nature, as well as cyber crimes that jeopardize the safety of our children, are investigated successfully by professionals who specialize in cyber crime matters."

"We appreciate the FBI's commitment to investigating this type of crime. Such action and results should certainly serve as a deterrent to anyone else who might be contemplating such activities," said Dr. Pierce Cantrell, vice president and associate provost for information technology at Texas A&M University. "We heartily thank everyone who participated in the investigation."

On February 28, 2007, Texas A&M University officials discovered the domain controller of its virtual private network (VPN), "Ajax," had suffered multiple unauthorized computer intrusion incidents. Steps were taken by the university to prevent the illegal or fraudulent use of the captured information and a criminal investigation was initiated by the FBI with the assistance of the university's administration and law enforcement authorities.

Through their joint investigation, agents learned that in mid-February 2007, Castillo logged on to the university's VPN utilizing his own ID and password from a wireless account located at an apartment in Oregon where Luis Castillo was living while working in the area. Thereafter, Castillo began logging on to the protected system from the same computer using unauthorized network IDs and passwords and ultimately accessed the university's VPN server to gain unauthorized access to the "Ajax." Once access to the domain controller "Ajax" was established

Feb. 24, 2007, Castillo injected malicious (Malware) computer programs into the university's protected computer system which operated to capture 133,000 network IDs and passwords of unsuspecting students and employees of the university. Thereafter, the program dumped the captured netwoek IDs and passwords into a temporary file on the system where Castillo could have access. An analysis of the injected Malware ultimately tied Castillo to the intrusions.

As a result of the intrusions and injection of the malicious software by Castillo, the university incurred a loss of over $67,000 in its efforts to protect students and faculty from the illegal or fraudulent use of private account information obtained through Castillo's unauthorized access to the university's protected computer system, including the retrieval of the captured files. To date, no known use or misuse of the captured information has been reported .

Castillo faces a maximum of five years imprisonment and a $250,000 fine for this conviction and is scheduled to be sentenced on Dec. 10, 2007 at 10 a.m. The court has entered an order permitting Castillo to be released on a $25,000 unsecured bond pending his sentencing.

The charges against Castillo are the result of the investigative efforts of the Houston division of the FBI, the Houston Area Cyber Crimes Task Force, the Bryan resident agency of the FBI, the Texas A&M University Police Department, and the Portland, Ore. division of the FBI, with the cooperation of Texas A&M University administration. The case is being prosecuted by Special Assistant U.S. Attorney Bret Davis.

###