

MU SAFEWeb

MU Secure Applications For EWeb Initiative

January 12, 2005



THE CHRONICLE OF HIGHER EDUCATION

Special Report

<http://chronicle.com/weekly/v51/i18/18a01002.htm>

From the issue dated January 7, 2005

OUTLOOK 2005

Technology: Keeping Networks Safe Is Administrators' Dominant Worry

By ANDREA L. FOSTER

Colleges are likely to increase spending on computer security by millions of dollars in coming years to protect confidential data and combat hackers who create the malicious codes that are infiltrating campus information systems.

Safeguarding networks and data is expected to be the most important information-technology issue in the next two to three years, said 21.2 percent of technology administrators who participated last year in the Campus Computing Project, an annual survey of how colleges use information technology.

IT Security Efforts at MU

2002 - present

- Account management
- Password safety
- Incident prevention and response
- Server and system administration
- Secure file transfer and certificates
- Security awareness education
- DMCA compliance monitoring and response

IT Security Efforts at MU

2002 - present

- Network security
 - Traffic monitoring
 - Virtual private networking
 - Firewalls
 - Device registration
 - Intrusion detection and prevention
- Desktop management
 - Antivirus software
 - Automated patch distribution
 - MU-Ready CD

IT Security Efforts at MU

2002 - present

- E-mail security
 - Spam management
 - Elimination of redundant SMTP servers
 - Forensics
- Law Enforcement incident handling
- Physical Security
- Systems Disposal and Asset Recovery

Yale University

- July 26, 2002 – A Princeton official broke into Yale University's Web site, used to notify students about admission decisions, and obtained personal information on 11 Yale applicants.

The Chronicle of Higher Education, August 9, 2002

University of Kansas

- January 22, 2003 – Officials discovered unauthorized access to their SEVIS system, allowing personal information on 1,450 international students to be downloaded.

The Chronicle of Higher Education, February 24, 2003

University of Texas-Austin

- February 26, 2003 – Hackers broke into a database and obtained Social Security numbers and email addresses on 59,000 employees, students and former students. Authorities filed federal charges against a 20-year-old student.

<http://www.dallasnews.com>

Georgia Institute of Technology

- March 31, 2003 – Online intruders broke into a server containing the credit card numbers of more than 57,000 patrons of a Georgia Tech arts and theater program.

http://news.com.com/2100-1002_3-994821.html

UCLA

- November, 2003 – Thieves broke into a locked van and grabbed a laptop with a database that included names, birth dates and Social Security numbers for 145,000 blood donors registered in UCLA's Blood and Platelet Center.

http://news.com.com/2100-1029_3-5230662.html

University of Georgia-Athens

- January 28, 2004 – Officials discover that a server in the Bursar's office has been compromised, with the potential inappropriate access to information on 31,000 student applicants, including:
 - Name
 - Birth Date
 - Social Security Number
 - Personal Contact and Parental Information
 - Credit Card Account Number and Expiration Date

<http://www.uga.edu/inside/fraudconcerns.html>

University of California-Berkeley

- August, 2004 - A computer hacker gained unauthorized access to information about *In Home Supportive Services* recipients and providers. The data set contained names, addresses, telephone numbers, and Social Security numbers of about 1,400,000 Californians.

<http://www.cdss.ca.gov/ihss/>

George Mason University

- January 10, 2005 – Officials discover that hackers compromised the university ID server, gaining access to names, photos, Social Security numbers and institutional ID numbers of 32,000 faculty, staff, and students.

http://news.com.com/2100-7349_3-5519592.html

Security Incidents at MU

- Security incidents
 - CY2003: 2042
 - CY2004: 1499
- A recent random 6-day sample
 - 12,750 “brute-force” attacks (unsuccessful) on MU domain controllers (password cracking) sourced from:

US	Taiwan	Philippines	China
France	Italy	Peru	Japan
Estonia	Sweden	Canada	Cameroon
Denmark			

Recent MU Security Incidents

- Web page defacements
- Imposter “computing staff” installed key-logging software on administrative systems
- E-commerce services improperly collecting or storing credit card information
- Compromised or poorly-designed servers & applications:
 - Brute-force password cracking
 - Distribution of computer hacking tools
 - Distribution of pirated copies of motion pictures and other copyrighted materials
 - Distribution of pornography and spam
 - Publishing of confidential or private information

What is a Web Application?

- Any Web page or set of pages that are dynamic in nature and are used to display, transmit, process or otherwise share information using a Web browser.
- **NOT** the same as a Content Managed Website

MU SAFEWeb Goals

- Heighten awareness of the need to incorporate sound security practices into Web development
- Improve the overall security of applications utilized at MU and the systems upon which those applications reside or depend
- Avoid the unauthorized release of sensitive or confidential information

MU SAFEWeb Objectives

- Establish application development standards
- Establish security standards
- Develop data classification policies
- Implement secure server environments to support data classifications
- Establish minimum qualifications and training requirements for developers, database administrators and server administrators
- Implement auditing policies and processes to insure adherence to standards

Security PS

- Based in Lenexa, Kansas
- Specialize in IT Security consulting company offering training, security assessments and vulnerability tools
- Engaged by IATS to improve MU's Web application security environment

What about MU Web Apps?

Administrative systems exist that very easily provide:

- Employee expense reimbursement details
- Social Security Numbers
- Employee IDs, which in turn allow
- Payroll Histories of individual employees

What about MU Web Apps?

Systems exist that:

- Until recently, processed credit card information without authorization from the Treasurer's Office.
- Use insecure "form-mail" applications leaving the Web server vulnerable to becoming a spam relay agent.

What about MU Web Apps?

Individual Colleges and sub-departments have Web services that:

- Display directories with student numbers
- Display directories with personal directory information for students who have asserted FERPA
- Accept credit cards on an insecure Web servers
- Allow access to Web server logs to anonymous users allowing accounts to be harvested and many other potential exploits

Recently Completed Tasks

- Identified Web application development standards and security as a priority – initiated MU SAFEWeb
- Provided information three times on campus to select Web developers, IT professionals and/or campus leaders
- Obtained Web application auditing tools
- Attended Web application security training

Tasks to be Completed

- Engage and educate decision makers throughout the campus
- Obtain names of responsible individuals from all Colleges and Divisions
- Establish minimum qualifications for developers (including incorporation of qualifications into job specifications)
- Provide an easy, affordable method to obtain initial and ongoing training

Tasks to be Completed

- Provide an effective method to audit web sites and remedy problem
- Develop and maintain a “Secure Development Practice” standards manual
- Develop applications security specifications to be used in procuring commercial software
- Identify funding

Applications Standards

- In part, driven by security needs
- Pockets/silos of developers at diverse skill levels
- No formal mechanism for sharing code
- Duplication of effort; no university-wide perspective
- Long-term supportability
- Need for a “loosely-coupled” application architecture



Eugène Delacroix *Tiger*, c. 1830, National Gallery of Art

