



MU Secure Applications For EWeb (MU SafeWeb)

Since 2002, IATS has identified a variety of IT security issues that needed attention at MU. The issues have included password security, operating system updates, violations to the Digital Millennium Copyright Act (DMCA), and network vulnerabilities that required the deployment of firewalls and intrusion prevention tools. The number of existing vulnerabilities balanced against the resources available demanded that the needs be prioritized. Since 2002, IT security priorities have been set based on internal knowledge of the vulnerabilities and best practices information gleaned from outside sources including auditors, vendors and higher-education and industry organizations.

In FY04, E-commerce auditing became an important focus for security efforts at MU. Many MU entities were already transacting business over the Internet; others were interested in doing so. Credit card companies have established a set of pre-production audit requirements that must be met before merchant IDs would be issued. Based on those requirements, UM-IT and IATS agreed to jointly provide E-commerce auditing services for University entities. Individually, each of these two IT organizations had a limited number of staff qualified to provide such services; utilizing staff from both groups allowed for a more expeditious method of meeting auditing needs.

While not problem-free, this joint effort has generally worked well, providing a method for departments to accept credit card payments on-line while ensuring the security of those transactions. However, the occurrence of known cyber attacks from both within and outside of MU's network have placed the security of all Web-based applications, including E-commerce applications, at a high priority.

Most Web-based applications access or otherwise utilize information that typically is stored in databases. These databases may be core systems such as PeopleSoft and SIS (Student Information System), or duplicate copies of these core systems ("shadow systems"). Others may be created within the division or department for which the application is being deployed. Regardless of the source, many of these databases contain confidential information. Often, access to such applications requires the use of a university ID and password. Additionally, many of these applications are critical to the operations of a given college, division, or to the University as a whole.

MU SafeWeb

Objective

The objective of MU's SafeWeb initiative is to:

- 1) Heighten awareness of the need to incorporate sound security practices into Web application development.
- 2) Improve the overall security of applications utilized at MU and the systems upon which those applications reside or depend.
- 3) Avoid the unauthorized release of sensitive or confidential information.
- 4) Develop campus-wide standards for applications development.
- 5) Develop the resources and expert guidance for MU departments to utilize in their development work.
- 6) Develop policies that provide a method for enforcement.

Goal:

The goal of MU's SafeWeb Initiative is to improve the overall security of applications utilized at MU, with an emphasis on Web applications, and the systems upon which those applications reside or depend.

The success of this initiative will require campus-wide participation from colleges and divisions that have a need to develop and/or deploy Web applications and that have experience in the areas of applications development. Specific objectives include development, implementation, and/or establishment of:

- Applications development standards
- Security standards for applications development work
- Data classification policies
- Secure server environments that support the defined data classifications
- Set minimum training requirements for applications development, database administration and server administration.
- Auditing policies and processes to insure adherence to the standards

Web Application Defined

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.

What makes Web Applications so vulnerable?

Web applications have become common points of entry for attackers to gain access to a variety of resources or to take over systems within a network. Browser-based applications have become universally adopted by companies and other business entities to facilitate information processing and transactions. More importantly, attackers don't have to "break in" to a network to gain access to a Web server; they may simply get in

MU SafeWeb

the same way legitimate customers do. Web applications are also generally easier to develop and deploy. Many Web application developers are not sufficiently educated on the security aspects of their craft, being more focused on placing applications into production than on security.

Steps to securing our web development environment

Securing our Web applications environment will require that standards be set and adhered to: both for individuals entrusted to create and maintain Web environments and also the tools they use in their work. Specific areas that must be addressed include:

- Engagement and education of decision makers.
- Identification of developers and/or specific individuals responsible for Web application development throughout the campus.
- Establishment of minimum qualifications for Web developers and provision of an efficient and affordable method to obtain initial and ongoing training.
- Development and maintenance of a “secure development practice” manual and associated applications development standards.
- Procurement of auditing tools and development of auditing policies to ensure adherence to security best practices. These tools and policies will be used in development of efficient methods to audit web applications and remediate problems.
- Development of applications security specifications for use in procuring commercial software.

What is it going to cost?

The goals of this initiative will require campus-wide participation from colleges and divisions that have experience in the areas of applications development. Undoubtedly, it will cost more to develop using secure methods than insecure ones. The question remains, “what would be the cost to the institution should an application be compromised?” Additional costs can be expected in the following areas:

- 1) Staff salaries – It will become important for departments to employ fully qualified, fully trained staff to develop Web applications.
- 2) Training – Initial and ongoing training for Web application developers cannot be viewed as optional. The Internet is an increasingly risky place to do business. Keeping up with current security techniques will be an ongoing process and will have an ongoing cost.

MU SafeWeb

- 3) Auditing – There will be costs in staff time and tools to provide Web app auditing services. How those cost elements will be paid for is yet to be determined.

It will be difficult to determine exactly what all the associated costs are in relation to this effort. Undoubtedly, this initiative, if successful will carry a higher cost than the current method of doing business. It is IAT Services' goal to provide as much financial relief to departments as possible. IATS is working to provide auditing tools, staff to perform audits, development expertise, and access to training. However, funding for all aspects of this initiative has not yet been identified.

Securing the Data Sources – the next step

Web applications are the most publicly available entry point into data sets that we must keep secure. However, there are other methods for data to be compromised. In addition to securing our Web applications, IATS will also be working to heighten awareness of other IT security issues that are just as important, including server security and data classifications. Those two areas will require that additional campus-wide work be done to:

- Develop and implement data classification policies
- Develop and implement secure server environments that support the defined data classifications
- Establish training programs to enforce minimum training requirements for applications development, database administration and server administration.
- Set development standards for all applications (client server) including work performed in-house and commercial applications.

We expect that the initial stages of this initiative will take 2 years to complete. Security gains realized from these first steps will require an ongoing commitment to maintain. Even during the course of this work, we will undoubtedly see changes in the tactics used by attackers which will require the adoption of new tools and skills by our developers.