Paper Title: Computer Security vs. Educational Effectiveness: Is Security Hurting Federal ADL?

Steven A. Kerschenbaum, Esq.
VERTEX Solutions, an Adayana Company
Falls Church, VA
skersch@vertexsolutions.com

Sean Brady
VERTEX Solutions, an Adayana Company
Falls Church, VA
sbrady@vertexsolutions.com

ABSTRACT

All Federal Government agencies are planning to use technology (Advanced Distributed Learning – ADL) to deliver training more effectively. For this reason, and consistent with industry trends, most agencies are using Web-based approaches to deliver as much electronic content as possible. However, in many and sometimes subtle ways, Web security and end-user computing platform restrictions have now become leading considerations and limitations in the development and delivery or instructional content. Sound instructional system design methodology (ISD) emphasizes the importance of proper analysis, media selection, interactivity, and collaboration to ensure the development and delivery of effective learning content. Unfortunately, many modern approaches to delivering this functionality (e.g., Macromedia Flash and Web-based collaborative tools such as WebEx) have been severely restricted or even prohibited by several Federal organizations. For secure networks with high network overhead, even straightforward rich media content can become prohibitive. Perhaps more disturbing are the subtle ways that confusion and uncertainty about the proper application of security and technical constraints work to impede ADL effectiveness.

Traditionally, security concerns always trump instructional concerns. However, what good is ineffective, security-compliant educational content? The truth is that content security levels dramatically influence ADL effectiveness for a number of reasons, and organizations should be considering these tradeoffs on a course-by-course and enterprise-wide basis. This presentation will introduce and discuss these impacts on Federal Government Agencies, summarize lessons learned, current workarounds, and considerations for moving forward, including:

- An overview of the security restrictions and technical constraints that often impact effective ADL development and delivery;
- A summary of the current security issues specifically encountered by Web instructional content;
- Considerations and recommendations for balancing effective ADL content and security

ABOUT THE AUTHORS

Steven A. Kerschenbaum, Esq. is Chief Technology Officer for Adayana, Inc., and General Counsel for VERTEX Solutions, Inc., an Adayana Company. Steve holds a B.S. in Computer Science and J.D. from Hofstra University, and is currently a member of the New York and Connecticut State Bars, the American Bar Association, the American Society for Training & Development (ASTD), and a member of the American Intercontinental University's IT Business Advisory Council.

Sean Brady is Chief Information Officer for Adayana, Inc., and Chief Systems Architect for VERTEX Solutions, Inc., an Adayana Company. Sean holds a B.S. in Electrical Engineering, Computer Engineering, and Mathematics from Carnegie-Mellon University.

Paper Title: Computer Security vs. Educational Effectiveness: Is Security Hurting Federal ADL?

Steven A. Kerschenbaum, Esq.
VERTEX Solutions, an Adayana Company
Falls Church, VA
skersch@vertexsolutions.com

Sean Brady
VERTEX Solutions, an Adayana Company
Falls Church, VA
sbrady@vertexsolutions.com

I. INTRODUCTION

New and more comprehensive computer security measures are making computing more difficult and complex for almost everyone. The impacts of tighter computer security are broader than most people realize, and are starting to become evident in new ways. This is especially true for Federal Government Advanced Distributed Learning (ADL). The reason is that the immediate threats are not obvious (as compared to identity and information theft) and the impacts are more subtle and long-term. Even so, the threats and challenges are very real, and organizations may not understand or appreciate the learning and performance impacts of how their IT security decisions are being applied.

The fear of introducing new security threats tends to cause organizations to rely on safer, more well-established Web technologies (e.g., HTML) without adequate regard for the potential interactivity and fidelity provided by more advanced technologies (e.g., Adobe Flash). From an instructional perspective, it has long been accepted that effective learning content must contain engaging, interactive elements. If security risks always trump the introduction of new interactive technologies, how can modern learning continue to advance?

To prevent computer security from stagnating ADL growth, it is important to understand how current security measures are affecting ADL development and delivery today. With this baseline, learning professionals can then help educate their organization about the trade off decisions they are making, and help influence future IT decisions in a more balanced manner regarding ADL.

II. STARTING AT THE WEB BROWSER

Most ADL content is normally delivered to the user via standard Web browsers such as Microsoft Internet Explorer (IE), Apple Safari, or Mozilla Firefox. Browsers themselves are computer programs that provide various configuration and extension options, and work with the content to deliver the end-user experience. For this reason, ADL content developers often rely on the proper configuration of the Web browser to deliver their content.

However, because of security concerns, many users and system administrators have configured their browsers for optimal security. In many cases, system administrators have "locked down" browsers by preventing any further configuration by end users. These steps are effective in preventing security breaches, but also interfere with ADL delivery and effectiveness in a number of different ways:

Disabled JavaScript

JavaScript – the principle scripting language for the Web – is used as a primary means for courseware to communicate with a Learning Management System or "LMS" (the program delivering and tracking the courseware). When completely disabled in the browser, ADL content cannot communicate correctly with LMS, and often presents strange behaviors that are difficult to troubleshoot. The JavaScript settings can be enabled to fix the problem, but the user must have the proper privileges and expertise to make the change.

Pop-up blockers

In an attempt to stop annoying and occasionally malicious pop-up windows, many of the current browsers come with a pop-up blocker feature (usually enabled by default). Unfortunately, pop-up blockers also affect courseware because LMS maintain their own windows when launching courses, and create a separate window to hold the course materials. If the browser blocks the new window, the courseware fails to launch and causes problems. This issue can be addressed by configuring the browser to "trust" content from certain locations and allowing their pop-up windows to launch. Again, this only works for folks with the proper privileges and expertise.

Blocked Cookies

Cookies – small bits of information written to a user's computer to retain information about the site or the user – have often been the target of security scares. Unfortunately, these bits of "persistent" data were often the targets of unwanted spyware that snooped out user's browsing habits and personal information. While there are several work arounds used by today's ADL content developers (e.g., by storing information in variable within invisible frames), some existing content still use "session cookies" (a less irksome variety) to pass information from screen to screen. These courses simply do not work when the browser blocks the cookie.

Plug-in Restrictions

Plug-ins – small applications that interact with a Web browser to provide a richer, more complex Web experience – extend the browser's ability to display content and objects otherwise not permitted by standard HTML and JavaScript. Java is one such Web plug-in that is necessary for some modern courseware to function, and is often required by the LMS to communicate correctly. These additional components need to be "plugged" into the browser to provide the necessary functions (e.g., Adobe Acrobat readers and Apple QuickTime video players). In the past, some malicious plug-ins caused trouble, and resulted in many folks simply preventing their installation. In many cases, critical plug-ins are installed initially and then locked down for protection. Unfortunately, new courseware often requires updated versions of the initial plug-ins, and the locked configurations prevent the installations.[1]

IE 7 Display of External Content

Figure 1. Side-by-Side Content Display (IE 7 / IE 6)

When Microsoft Internet Explorer was updated to version 7.0, new capabilities and functionalities were introduced to the popular browser. With these new capabilities also came new "features," including some new security-related changes. More specifically, all Web content accessed from an outside domain (http://machine.domain.com vs. http://machine/) must display the address bar AND footer activated by default. This feature cannot be disabled, and is intended to prevent outside content from hiding its source (a nasty habit of malicious websites). These additions, however, add roughly 52 pixels to the height of the browser window and sometimes introduce scroll bars into the content.[2] This relatively small reduction in screen real estate caused trouble for many ADL users and even greater challenges for folks trying to troubleshoot the cause (See Figure 1).

III. MOVING TO THE SERVER SIDE

As mentioned earlier, ADL content is normally delivered through an LMS. Most modern LMS products are Web-based (relying on the support of a Web Application server), and use standard communication protocols to deliver and track the delivered content. The most prevalent protocol is SCORM, short for the Sharable Content Object Reference Model. It provides a reference standard for both communication (known as the run-time environment – RTE) and content structure (known as the aggregation model).[3] While the industry appreciates the standardization and ease-of-use provided by Web-based delivery, it is also susceptible to many common Web-based threats. When today's Web security measures are applied to server-side ADL delivery however, a variety of different issues can arise:

SCORM Cross-Domain Issue

In the past, malicious Web code was discovered that probed open browser windows for information (a particularly nasty threat). To counter this threat, security measures were put in place to ensure that the LMS was only running code from a trusted domain (attempting to prevent malicious code from running by restricting the content to your current domain). However, as architectures grew and folks wanted to share content more broadly (normally a good thing), the industry discovered that launching content from a

[1] Web content can be written to check first and ensure that the plug-in is available, and provide links to the latest and version as needed, but the user must have the privileges to install them on their system.

[2] See Cascading Style Sheet Compatibility in Internet Explorer 7, Markus Mielke and Dave Massy, Microsoft Corporation (January 31, 2006), for more details regarding the impact of IE7.

[3] See http://www.adlnet.gov/scorm/index.aspx for more information regarding SCORM.

different domain was interpreted as a potential security violation and therefore prevented.

The simplest way to correct this is to co-locate the ADL content server with the LMS application server in the same Web domain. For situations where this is not possible, the ADL Co-Lab provides further workarounds such as "cross-domain scripting" and the use of a reverse proxy.[4] Even with established guidance, these technical issues and workarounds are considerably complex, and continue to challenge experienced and inexperienced ADL users alike.

Mistaken Denial-of-Service (DoS) Attacks

A Denial-of-Service attack is an attempt to make the assets of a computer unavailable by overwhelming the server with requests. The media has reported several high-profile DoS attacks over the past few years (e.g., attacks against Yahoo and Buy.com). Many websites today have provisions and controls to permit the administrator to block certain clients from making requests if they are seen to be attempting a Denial-of-service attack. As mentioned earlier, SCORM provides the means for Web courseware to store and retrieve information within the LMS for use content delivery. Unfortunately, under certain circumstances, the ongoing act of storing and retrieving data from the LMS can be misconstrued as a DoS attack on the LMS host.

To avoid such complications, content developers now design their content to spread out their requests, only getting data needed for the presentation of the current set of pages. In cases where the content requires multiple interactions, course sponsors must coordinate with network administrators to loosen the DoS restrictions for the content to function. Again, these technical nuances can be complex, and often experienced professionals to diagnose and correct.

Port-sharing limitations

In some ADL deployments, the LMS is installed in an environment where another application or Web server is using the standard logical port – port 80. In these cases, system administrators may change the default LMS port number to another commonly used one, such as 8000, 8080, or others. The application server is able to adjust the ports, and the LMS can function quite well using the non-standard port number.

Problems arise however when people outside of the firewall try to reach the LMS on the non-standard port. Most office infrastructures are protected with firewall devices that block connection attempts on non-standard ports to prevent unauthorized intrusions. Unless the firewalls, network switches, and Web servers are configured properly (requiring considerable technical expertise), users will be unable to reach the LMS. The same issues regarding standard ports can also arise with other ADL Web services such as podcasts, synchronous collaboration (e.g., Adobe Breeze), Learning Content Management System (LCMS) integration, and even simple chat.

V. THE FUTURE OF FEDERAL ADL AND SECURITY

Almost all Federal workstations are locked down to varying degrees, and the guidelines have tended towards greater restrictions over time. This single fact has been perhaps the most damaging impact of effect Federal ADL content. To combat this effect, it is critically important to be aware of your organizations security measures and your audience's needs very early in the content development process. Answering the following four questions in cooperation with your technical staff for each ADL effort can often highlight or mitigate potential issues before they become truly insurmountable:

1. What will your ADL content require from the learner's browser (plug-ins, JavaScript?)
2. How many different Web browsers will the ADL content support?
3. Where are the learners located (behind the corporate firewall, at remote offices, in the field, at home?)
4. Where will the ADL content be located (behind the corporate firewall, a third-party host provider?)

Armed with these answers, you should have enough information to discuss the security needs of your ADL with your corporate IT staff. They should be able to determine whether their standard browser configurations will accommodate your needs, or whether additional browser or hosting configurations will need to be changed. Based on other IT initiatives, they may ask you whether you can reduce some of the ADL requirements to avoid problems (perhaps with users outside your corporate environment). In any event, it is always best to have this discussion as early as possible for each WBT initiative.

[4] See the ADL Co-Lab Cross Domain Scripting Document for more details (http://www.adlnet.gov/downloads/downloadpage.aspx?ID=58)

While it seems absurd to allow a training initiative to jeopardize organizational and personal security, today's federal ADL restrictions are having a chilling effect in the industry. Like any development activity, ADL content has performance requirements that make it effective. If these requirements are always secondary to security considerations, we are limiting how effective our ADL can ever be.

The key is finding the proper balance between Web security and effective learning. While effective learning is not usually considered in terms of organizational IT security and risk assessments, perhaps it should. It may be time for ADL professionals to emphasize the close relationship between computer security and educational effectiveness (particularly ADL), and for decision makers to appreciate the potential impacts of always trumping ADL considerations with security.

ACKNOWLEDGEMENTS

Thank you to our Federal Government clients and partners for sharing their experiences, and to all the ADL professionals that contributed to our findings.