STANDARDSCONNECTION

E-learning Meets Security Policies

How will organizational security problems impact your system?

BY ROBBY ROBSON

As e-learning has evolved, content has become separated from the systems that deliver it. This is a good thing. It allows a single learning management system (LMS) or learning content management system (LCMS) to use content from multiple sources, and supports enterprise environments where content is distributed among multiple servers. Interoperability standards like SCORM and those produced by the Aviation Industry CBT Committee (AICC) allow properly designed learning content to communicate with and be tracked by any compliant LMS or LCMS. But there's a rub.

Web-based training and online learning run in Web browsers, usually Internet Explorer or Netscape. As a security measure, these browsers do not allow content coming from one place to communicate with content coming from a different place. This prevents potentially malicious practices such as a Web page from one company accessing data entered into a Web page from another company—your credit card data from a recent online purchase, for example. Unfortunately, it also prevents an LMS or LCMS running on one server from communicating with content that is delivered from a different server. And that's a problem.

In the e-learning space, some have dubbed this the "three-node scenario problem" because it involves two servers and one client as shown in the illustration on the right. The more technical name for it is the "cross-domain security problem." Regardless of what it is called, it typifies the conflicts that arise between the need for security and the desire to meet user requirements. In this case, security can thwart the requirement that content be served from a separate server and still communicate with an LMS or LCMS.

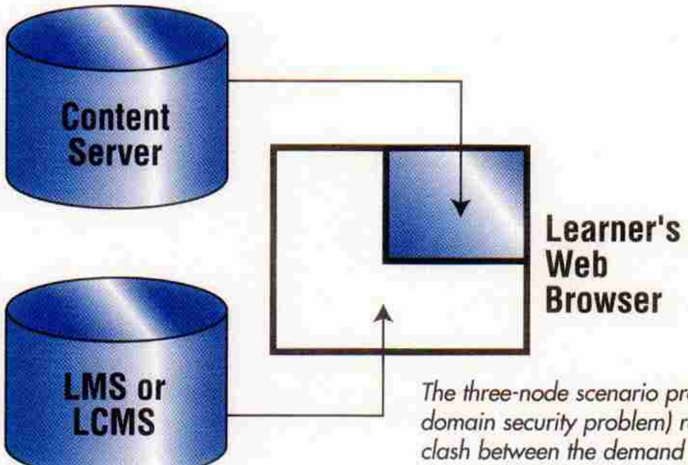
Solutions

Almost every vendor of enterprise LMS or LCMS products has encountered the cross-domain security problem. Not surprisingly, numerous real world solutions have been found. Some solutions make content from different sources appear to a Web browser as if it came from a single source. Other solutions establish direct communication between an LMS or LCMS and a content server, and still others make use of the ability of a learner to explicitly grant a Web browser permission to communicate with a trusted source. The number and diversity of solutions are a tribute to the ingenuity of e-learning customers and vendors.

Still, none of the solutions are perfect. Asking learners to grant explicit permissions often presents them with confusing and distracting dialogue boxes and is enough to drive some users away. Almost all other types of solutions rely on software, hardware, and network configurations that require cooperation and permission from the IT department. But IT departments have security policies and procedures in place, some of which may turn apparently reasonable solutions into non-starters. For example, an IT department may restrict the use of applets, thereby ruling out solutions that depend on them.

The mobile code directive

A publicly available example of a security policy is the "mobile code directive" (www.c3i.osd.mil/org/cio/doc/mobile-code11-7-00.html) which applies to the U.S. Department of Defense. This direc-



The three-node scenario problem (or cross-domain security problem) represents the clash between the demand for security and the need for addressing user requirements.

tive, issued in November 2000, addresses the security threats posed by software that is downloaded from an external source and can execute on a local computer, possibly without the user's knowledge or permission. Such software is called *mobile code*.

Many common file types can contain or be used as mobile code. These include Java applets, Active X controls, Visual Basic scripts, UNIX shell scripts, JavaScript, Flash and even PostScript, the native format used by many printing and display devices. The mobile code directive categorizes the security risks associated with various file types and sets out policies of prevention, vigilance, and risk mitigation. It implies, among other things, that servers must use encryption, and that Java applets can only be used if they are downloaded from trusted sources. It also places an onus on an IT department to keep current with security patches, making it very natural to require all servers to be identically configured and to bar any user installation of software. Similar policies are common in corporations as well, also motivated by security and maintenance needs. These policies profoundly affect the kinds of solutions available for problems like the cross-domain security problem in a given installation.

Lessons learned

E-learning applications interact with other IT infrastructure, use common technologies, and are subject to the same policies and procedures as any other enterprise software. As e-learning becomes more deeply embedded, organizational security policies are even more likely to impact the type of e-learning content that can be used and how e-learning systems can be configured.

The cross-domain security problem results from the desire to have content and learning systems reside on different servers and still communicate with each other in a standardized way. Although there is no "one size fits all" solution because of the wide variation in local policies and requirements, existing solutions illustrate that most obstacles can be overcome. According to the chief architect of the Advanced Distributed Learning initiative (www.adlnet.org), a document detailing some of the known solutions is in the offing. Solutions to the cross-domain security problem also illustrate that the success of an e-learning implementation depends in part on its ability to integrate well with existing infrastructure and to work within the constraints of IT policies and procedures. It is to our advantage to develop standards, technology, content, and best practices that make this as easy as possible. *e*