Flash, aaaaagh! Is your school website flashy but safe?

July 2 2010

Most educational websites in the U.S. are using Flash applications that fail to adequately secure these pages. This is a growing problem for the Internet as vulnerable sites can be hijacked for malicious and criminal activity, according to a paper published in the *International Journal of Electronic Security and Digital Forensics* this month.

Joanne Kuzma, Colin Price and Richard Henson of the Business School, University of Worcester, England, have used a simple tool provided by Hewlett Packard (HP), known as SwfScan, to analyze academic websites across the U.S. for security holes in their Flash applications.

Adobe Flash is a proprietary multimedia platform used to add animation, video, and interactivity to countless web pages. It is widely used by sites like Google Youtube and by gaming sites and in advertisements. It has also been positioned as a tool for "Rich Internet Applications". However, although provider Adobe releases regular security patches to address problems as they arise, many sites are not kept up to date and so remain vulnerable. Companies such as Apple, refuse to allow Flash to run on their consumer devices for this very reason.

Kuzma and colleagues point out that it is impossible to make any web application 100% secure, but that academic institutions must implement new policies better secure their sites and to protect their users. In 2008, HP used its SwfScan tool to audit 4,000 Flash applications across the web and found 250 Flash applications that had a login form in which usernames or passwords are hard-coded into the application. Older

versions of Flash are rife and more than a third of Flash applications violated Adobe's security recommendations.

The team has now used SwfScan to scan 250 educational websites, with worrying results. "Education sites are increasing the number of their Flash-based pages and applications, especially due to the growth of online learning," the team says, "Yet almost all pages showed at least low-level security vulnerabilities and over 20% of them had medium-level security issues where personal information could be disclosed to attackers." Six of the sites scanned (2.4%) showed critical vulnerabilities. Just two sites had no reported Flash vulnerabilities.

Well-publicized data breaches at Florida and Ohio universities led to the names and social security numbers of hundreds of thousands of students being exposed, which not only affected security for those individuals but led to such negative publicity that Ohio, at least, saw a significant decline in monetary donations. But, there are a variety of technical, legal and procedural methods that institutions could effectively implement to provide a better level of user protection, the team adds.

A serious problem in university security is that professors, colleges, departments and even student organizations regularly create and maintain separate shadow systems. So even if the university does have secure core applications and specific security policies, these shadow systems could open up security vulnerabilities. Moreover, academic departments often operate their own servers that bypass the institution's IT department. "A staff member could create a separate Flash application to collect miscellaneous user information and this application could be developed with minimal thought to security, or could bypass corporate [security](#) policies and development procedures," the team explains. "Those staff may be unaware of legal regulations that apply to the industry."

More information: "Flash vulnerabilities analysis of US educational websites" in Int. J. Electronic Security and Digital Forensics, 2010, 3, 95-107

Provided by Interscience Publishers