Tom King

Mobilemind

LETSI 2008 Call for Paper on SCORM 2.0

August 14, 2008

SCORM Is Insecure: Secure It Before Adding Features

ABSTRACT

Security Before Features– The current SCORM Run-Time Environment (RTE) presents many security risks, and must be secured before the model is extended. At least one security exploit currently exists. Many LETSI white papers propose extending SCORM features and offering additional integration. This should only be done after, or possibly or in conjunction with, securing SCORM.

PROBLEM AND USE CASES

With minimal programming skills and an amateur's understanding of software security, I developed a working exploit in just a few hours. This exploit sends arbitrary scores, status values and times to many SCORM systems. Systems successfully exploited include the ADL SCORM 2004 3rd Edition Conformance Test Suite, sample SCORM content from ADL, sample SCORM content from commercial elearning tools, and at least one commercial LMS. Quick and rudimentary research on software security leads me to believe that there are additional attack vectors ripe for exploit in more serious ways.

STAKEHOLDERS AND ISSUES

The value and quantity of vulnerable data increases dramatically as SCORM systems become integrated with social networks, simulations and HR systems. Likewise, the attack surface expands. There may even be significant liabilities associated with an exploit that “only” allows cheating on score, time or mastery. For example, consider the impact on legal liability regarding corporate compliance training if it became widely known that completion of mandatory governance or safety training was easily bypassed.

INTEGRATION AND TECHNICAL ISSUES

In addition to attacks that undermine the value and validity of student performance data, there may be additional exploits such as SQL injection or buffer and stack overflow areas. As SCORM systems integrate with talent management functions and sophisticated technical simulations the exposure starts to extend towards a variety of personal identity, corporate, and high-value technical, industrial and military data. This underscores the need to secure SCORM on all fronts, starting with the integrity of student data and extending to every integration avenue.

RECOMMENDATIONS

Initial efforts on securing SCORM may likely focus on best practices to reduce exposure with the current model. In parallel, work should begin on authentication of the parties in each type of transaction, and securing the communication methods that are currently publicly exposed in the browser DOM and can be spoofed, modified or overwritten.

Finally, proposed extensions and new features should be vetted *during the design phase* with independent security analysts to increase overall security. Example and reference implementations need to undergo an independent security audit. Training software often has a longer shelf life than other applications and software attacks against systems always improve with time.

EXISTING IMPLEMENTATIONS AND SUMMARY

As indicated, a current exploit allows one to bypass genuine completion or scores. I am withholding further details of both a known generic and a targeted exploit approach that I have developed. However, I am willing to arrange private demonstrations of these techniques to qualified interested parties. Given the opportunity I am also willing to demonstrate the exploit at the LETSI SCORM Workshop in October.

The issue of SCORM security should be neither trivialized nor sensationalized. It must not be neglected. LETSI members, the international community, vendors and individual professionals must act. Everyone needs to address known and anticipated security issues in order to maintain the trust and respect of their colleagues, students, customers, and partners. If the security, validity, safety and trustworthiness of learning systems suffers, everyone suffers.