Contribution ID: **12** Type: **Oral**

Grid website vulnerabilities and the GridSite Security Framework

Wednesday 13 February 2008 11:20 (20 minutes)

CSRF and XSS attacks have been used against major public websites, such as Google's GMail, for several years, and generally involve "confused deputy" scenarios in which an authenticated user's web browser is deceived into carrying out an action desire by the attacker. Due to the support for Javascript functions such as XMLHttpRequest in browsers, it can be possible for an attacker's script to communicate with a website using the user's credentials without their knowledge. The credentials involved have typically been HTTP cookies issued by websites to legitimate users, and the attacks have relied on users being logged-in at the time of the attack.
However, in Grid environments many websites authenticate users with their X.509 user certificates, and so users are always logged-in from the point of view of an attacker's script.

3. Impact

This class of vulnerabilities has the potential to allow some severe escalation attacks against web-based management components of Grids, as the sessions of users with lower credentials are used to inject attacker's scripts into wikis, bug tracker sites, monitoring messages etc. When users with higher administrative privileges view pages containing these scripts, their credentials could then be used to modify access policies, group memberships, site configurations etc.

This talk explains how the GridSite Security Framework prevents these attack modes using a combination of X.509 user certificates, the established double-submit cookie method and cross-domain limitations on cookie sharing and creating XMLHttpRequest connections. This method involves inserting an additional login page step, which also allows the integration of non-X.509 authentication systems such as Kerberos and Shibboleth on an equal footing with X.509.

URL for further information:

http://www.gridsite.org/

4. Conclusions / Future plans

Support for this system is included in the mod_gridsite extension to Apache, and can be used as the basis of third-party portals, management sites etc in any language supported by the Apache HTTP server. Furthermore, this mechanism for limiting CSRF/XSS attacks can also be implemented by other web application hosting environments, or by applications themselves.

Provide a set of generic keywords that define your contribution (e.g. Data Management, Workflows, High Energy Physics)

gridsite security x.509 csrf xss websites portals

1. Short overview

This talk describes Cross Site Request Forgery (CSRF) and Cross Site Scripting (XSS) attacks which can be attempted against administrative websites and portals used in grid projects. It explains how the X.509 certificates used in grid projects actually make these attacks easier, and then describes a solution implemented by the GridSite project.

Primary author: Dr MCNAB, Andrew (UNIVERSITY OF MANCHESTER)

Presenter: Dr MCNAB, Andrew (UNIVERSITY OF MANCHESTER)

Session Classification: Grid Access

Track Classification: Existing or Prospective Grid Services