Justification

Category: Web Security

This paper proposes WSF (web server firewall) to help system administers provide perimeter security to their web systems via a flexible security policy framework. WSF differs from existing web protection systems in several aspects.

First, WSF provides a language for specifying security policy regarding permitted accesses and enforcing it at the perimeter of a web server. For example, instead of asking an web administrator to enumerate all possible malicious request patterns as attack signatures, WSF allows an administrator to specify what input patterns are valid, which is much easier for administrators. We show that, with proper policy specification, WSF can help mitigate many attacks such as buffer overflows via sending long parameters to CGI programs and SQL injection attacks.

Second, WSF support access control for web systems. It can be used to limit authenticated or unauthenticated users to only specified CGI programs/web services and with specified restrictions on parameters.

Finally, WSF can audit web clients' behaviors and compiled them into per-user security contexts. The behavior statistic records can be used to detect abnormal behaviors. In addition, behavior history can be used to heuristically change the access policy to proactively block malicious users.