OWASP Logging Project Roadmap

Goals

- Provide tools for software developers in order to help them define and provide meaningful logs

- Provide code audit tools to ensure that log messages are consistent and complete (content, format, timestamps)

- Facilitate the integration of logs from different sources

- Facilitate attack reconstruction

- Facilitate information sharing around security events

Subprojects

1) IDE integration (auto-completion, templates, logging policy definition support) for guiding software developers to define and provide meaningful logs

2) Implement the Standardized Common Event Expression (CEE) for Event Interoperability.

CEE includes: Event Taxonomy, Standard terminology, Log Syntax, Consistent data elements and format, Log Transport Standard communications mechanisms, Log Recommendations

See http://cee.mitre.org/ and http://n2.nabble.com/attachment/1143183/0/useCases_A2.doc

3) Integrating application logs into a Security Information Management configuration

OSSIM (http://www.ossim.net/) has numerous plugins for parsing webserver, appserver, WAF, IPS, IDS logs and generating/storing events in its standard format.

Adding a plugin for parsing custom application logs is as easy as finding the correct regular expression provided that developers included all relevant information in the log message and that they have done so in a consistent way.

You can refer to the OSSIM database model to see what data is stored for events.

4) Reconstructing attacks

It is difficult to analyze, filter and generally reconstruct an attack because messages are spread around various log levels.

Arshan Dabirsiaghi's proposal of adding a security log level is very interesting

See http://www.owasp.org/index.php/How_to_add_a_security_log_level_in_log4j

5) Implement automated code audit tools (s.a. OWASP yasca) to ensure that log messages are consistent and complete (content, format, timestamps)

Related OWASP projects: http://www.owasp.org/index.php/Category:OWASP_Orizon_Project

6) Implement scripts for filtering/scrubbing logs in order to enable log data sharing between organizations

Goal: information sharing around security events