Mt Wilson

Authorization

# Background

An extensible application needs a facility for extensions to declare permissions required to use them, and for an administrator to selectively grant permissions to other users. The authorization facility must apply to every programming and user interface available - HTTP service requests, console commands, automated tests, etc.

# Architecture

Mt Wilson uses Apache Shiro with aspect-oriented processing of permissions.

The Apache Shiro architecture is not described here; see <http://shiro.apache.org/>

## Adding Shiro to an Application

Add “shiro.ini” and “shiro-ip.ini” to the configuration folder.

Add a dependency on “mtwilson-shiro-file” for a simple file-based storage of users and permissions, or add a dependency on “mtwilson-shiro-jdbi” for database storage. These projects include setup tasks and command-line tools to create the admin user and manage user permissions.

Add an optional dependency on “org.apache.shiro:shiro-core” in any project that declares permissions via annotations. Add annotations to methods to indicate what permissions are required, like this:

@RequiresPermissions("documents:edit")

Add the following elements to web.xml:

<context-param>

<param-name>shiroEnvironmentClass</param-name>

<param-value>com.intel.mtwilson.shiro.env.LocalIniWebEnvironment</param-value>

</context-param>

<listener>

<listener-class>org.apache.shiro.web.env.EnvironmentLoaderListener</listener-class>

</listener>

<filter>

<filter-name>ShiroFilter</filter-name>

<filter-class>com.intel.mtwilson.shiro.LoggingShiroFilter</filter-class>

</filter>

<filter-mapping>

<filter-name>ShiroFilter</filter-name>

<url-pattern>/\*</url-pattern>

<dispatcher>REQUEST</dispatcher>

<dispatcher>FORWARD</dispatcher>

<dispatcher>INCLUDE</dispatcher>

<dispatcher>ERROR</dispatcher>

</filter-mapping>

## Using IP Address Whitelist

In general this is insecure because IP addresses can be faked. To enable this, copy “shiro-ip.ini” over “shiro.ini” and restart the server.

# Development Roadmap

Apache Shiro supports a selector field that could be used for row-based selections, but a suitable format for expressing selection criteria needs to be adopted and implemented. The format must be flexible enough to be able to reference any field of an object or its children, and it must support dynamic expressions so that objects can be selected based on their relationship to the current user (for example, allowing a user to edit only documents they own and not all documents).

Need to implement data integrity controls for the user and permission storage so that an attacker with some inside access cannot just edit the permissions. File-based storage can be encrypted and also protected with data integrity directly using the document container format. Database storage needs to be managed using queries, where the query and its result are saved with the signature.