Technical Note

HushMail Test Environment

Brendon J. Wilson

May 4, 2001
Version 1.1

Copyright Notice

Table of Contents

Overview

This document outlines methods for reviewing the activity of the HushMail applet in an integrated development environment for the purposes of reviewing the activities of the applet as part of a formal or informal security audit. The configuration information presented here enables a developer to use the publicly available source code for the HushMail applet and a live HushMail server to exercise all aspects of the application's functionality; this is required to encourage peer review, while keeping the code for the server side component of the HushMail application private.

Origin of this Document

Originally the contents of this document were created to train new developers; however, given the importance of public review of the security aspects of the application, I've retooled the document for public consumption.

Intended Audience

Any developers who wish to analyze the operation of the HushMail application, but do not have the benefit of access to the server side components.

Relation to Other Systems

As the HushMail applet relies on the support of the HushMail server, and a HushMail key server, this topic is intimately related to the communication protocol, and ciphers us ed by the HushMail system. This document will not describe any aspects of the HushMail protocol, or the server side architecture.

Detailed Description

Requirements

In order to use the source code provided by Hush, you will require a Java 1.2 development environment; you should preferably use an integrated development environment, such as VisualAge for Java (available for free at www.ibm.com/vadd). In addition, you should have some knowledge about Java, Java applets, and the configuration details of your Java environment.

Obtaining Source Code

Hush Communications (www.hush.com) has made the source code the HushMail client applet public available for peer review; all versions of the source code can be obtained from the Hush.ai server (www.hush.ai). Choose the latest release of the client source code, and unzip the source code in a location appropriate for your Java development environment.

In addition to the source code provided by Hush, you will require the set of images and properties used to populate text and buttons in the applet; for your convenience, a package of the required files has been made available at www.brendonwilson/projects/hushmail/testenvironment.zip. Unzip this file in the same location as you unzipped the source code files.

Configuring the Client Applets

The HushMail applets rely on `<PARAM>` tags in the calling `<APPLET>` tag to provide it with a variety of configuration details, including:

- An initial session key for encrypting communications
- A HushMail user name
- A domain
- The HushMail server address and port for the user's account
- The server's public key

In order to test against a live HushMail server, you will first need to go to www.hushmail.com and create a new account to use for testing. Once you've created the account, login to the account and use your web browser's 'View Source' capabilities to view the source of the HTML page. Look for a section that looks something like:

```
<param name=”username” value="…">
<param name=”sessionKey” value="…">
<param name=”small” value=”no”>
<param name=”domain” value="hushmail.com">
<param name=”port” value="80">
<param name=”exitpage” value="…">
<param name=”serverAddress” value="userX.hushmail.com">
<param name=”serverPublicKey” value="…">
```

Your account should have specific details required to access the correct server for your account, specifically the `username`, `domain`, `serverAddress`, `port`, and `serverPublicKey` values.

Using the set of HTML pages provided in the test environment zipfile, cut and paste the value of these parameters into the sections marked `REPLACEME` in each file. For the new account applet HTML file, NewAccountApplet.html, you should enter a different account username than the one you just created; the new account applet will not be able to create an account that already exists, and you will not be able to test all of the applet's functionality.

Running the Applets

Compile the applet source code, ignoring any complaints about missing Microsoft or Netscape security classes (see next section). Once the application has been compiled, run the application using the applet viewer and the HTML files provided in the test environment zipfile.

Security Restrictions

The Hush applet makes use of Internet Explorer and Netscape-specific APIs to obtain permission from the user to perform restricted actions; however, these APIs have been wrapped in a browser-independent framework that chooses the appropriate classes to use based on the 'java.vendor' system property of the Java Virtual Machine. You may need to alter code in the `StrategyFactory` class in the `com.hush.client.security` package to use the stub class `IBMStrategy` instead of the `NetscapeStrategy` or `MicrosoftStrategy` classes.

In addition to using the stub security provider framework, you may have to configure your IDE to allow applets to perform restricted activities to avoid the burden of producing a signed applet. See your IDE's documentation, and documentation on configuring security policies from Sun available at http://www.javasoft.com/products/jdk/1.2/docs/guide/security/PolicyFiles.html.

GNU Free Documentation License

In order to limit the size of this document, a copy of the GNU Free Documentation Version 1.1 has not been included within the document itself. A copy of the license is freely available for download from the Free Software Foundation:

http://www.gnu.org/copyleft/fdl.html

Alternatively, a copy of the license terms can be obtained by writing the Free Software Foundation at:

Free Software Foundation, Inc.
59 Temple Place, Suite 330,
Boston, MA
02111-1307
USA

References

Sun Microsystems. Default Policy Implementation and Policy File Syntax [online]. Palo Alto: Sun Microsystems Inc., 2001 [cited May 4 2001]. Available from the World Wide Web: (http://www.javasoft.com/products/jdk/1.2/docs/guide/security/PolicyFiles.html)

Revision History

Version	Author	Date	Description
1.0	Brendon J. Wilson	May 4, 2001	Document Created
1.1	Brendon J. Wilson	June 9, 2001	Added GNU license info.