Secure JAVA Applets and Applications: Guidelines and Lessons Learnt from the JAVA Security Model

Isabelle Bichindaritz(1), Ph.D., Muriel F. Siadak(1), P.A., Jane Jocom(1), A.R.N.P., Carol Moinpour(1), Ph.D., Gary Donaldson(1), Ph.D., Nigel Bush(1), Ph.D., Michael Chapko(2), Ph.D., Keith M. Sullivan(3), M.D.

(1)Clinical Research Division, Fred Hutchinson Cancer Research Center
(2)Department of Health Services, University of Washington and Department of Veterans Affairs, Puget Sound Health Care System
Seattle, Washington
(3)Division of Medical Oncology and Transplantation, Duke University Medical Center
Durham, North-Carolina

The security system presented here has been developed for the Care-Partner system, which is a knowledge-based computerized decision-support system on the World-Wide Web (WWW). The health information protection system for Care-Partner encompasses both organizational and technical dimensions. We summarize here only the technical aspects of it. We found that, among the different techniques for implementing and deploying computer systems over the World-Wide Web (WWW), Java technology provides a global and efficient technical solution. The Java Cryptography Architecture (JCA) and the Java Cryptography Extension (JCE) permit to wire tailored security into Java applets and applications.

The security system in Care-Partner is an application-level security system, encompassing the three pillars of a security system, namely authentication, content integrity (encryption) and audit features, and an administrative utility:

♦ **Authentication**: authentication is ensured by the combined use of hardware tokens on the client side, with digital signatures. Two types of digital signatures are provided: by the server, permitting the client to authenticate the server, and by the client.

♦ **Content integrity**: content integrity is solved by encrypting all information transmitted between the client and the server. The Java client is a Java application, running independently from a browser. Here SSL encryption has to be performed at the application level. Similarly, if an applet it runs via a special plug-in (the Java plug-in), SSL encryption is also at the application level. This can be done either by using an additional class, called a SSLSocket (and associated SSLSocket), or the Cipher class from the JDK 1.2 with RSA encryption (which requires an additional class as well).

♦ **Audit**: the Java security manager signals security violations by throwing SecurityException’s. At the application level, these security exceptions are checked and subsequent measures taken. Moreover, auditing is performed at the application level by logging all accesses and modifications made to each field of each database in a Log database.

♦ **Administrative utility**: an administrative utility (Figure 1) has been developed for Care-Partner to map user names, user ID’s, user electronic signatures, roles, patients (identified by their patient ID), database fields and application components.

![Figure 1. Care-Partner’s administrative utility.](image)

Acknowledgments

This work was supported in part by grant R01HS09407 from the Agency on Health Care Policy and Research (AHCPR).