SECURE NETWORK-CENTRIC APPLICATION ACCESS

Nitesh Varma

Thesis submitted to the faculty of the Virginia Polytechnic Institute and State University

in partial fulfillment of the requirements for the degree of

Master of Science

in

Mechanical Engineering

Jan Helge Bøhn, Chair

Arvid Myklebust

Lawrence Sewell

September 17, 1998

Blacksburg, Virginia

Keywords: Client-Server, Internet, WWW, Security, Cryptography, Java

SECURE NETWORK-CENTRIC APPLICATION ACCESS

by

Nitesh Varma

Jan Helge Bøhn, Chairman

Department of Mechanical Engineering

(ABSTRACT)

In the coming millennium, the establishment of virtual enterprises will become increasingly common. In the engineering sector, global competition will require corporations to create agile partnerships to use each other's engineering resources in mutually profitable ways. The Internet offers a medium for accessing such resources in a globally networked environment. However, remote access of resources require a secure and mutually trustable environment, which is lacking in the basic infrastructure on which the Internet is based. Fortunately, efforts are under way to provide the required security services on the Internet. This thesis presents a model for making distributed engineering software tools accessible via the Internet. The model consists of an extensible client-server system interfaced with the engineering software tool on the server-side. The system features robust security support based on public-key and symmetric cryptography. The system has been demonstrated by providing Web-based access to a .STL file repair program through a Java-enabled Web browser.

ACKNOWLEDGEMENTS

I am thankful to a number of people who have helped me in completing this thesis.

- First, I would like to thank Dr. Bøhn for introducing me to the idea of Web-based application access, and helping me with his insight and suggestions.
- I would like to thank Dr. Myklebust for providing me with the opportunity to work as a teaching assistant in the Virginia Tech CAD lab. Further, I wish to thank him for introducing me to the CAD/CAM in general, and Computer Aided Geometric Design in particular.
- I would like to thank Mr. Sewell for agreeing to serve on my thesis committee on a very short notice, and for providing me with useful insights into several security related topics.
- I would like to thank Dr. Ioannou of Virginia Tech Industrial and Systems Engineering Department for serving on my thesis committee for the better part of my initial research work.
- I wish to thank to the Virginia Tech Department of Mechanical Engineering for providing me with financial support for the most part of my study here.
- I am really indebted to the numerous friends on the *comp.lang.java.programmer* and *comp.lang.java.security* newsgroups, and the Cryptix-Java mailing list, who came to my rescue whenever I needed help while developing my program. In particular, I wish to thank Aldo Eisma of IBM, Object Technology Group, Netherlands, who helped me with running Cryptix code in a Java applet.

- I thank the Cryptix team for developing the wonderful Cryptix library, and more importantly, making it a freeware; similar libraries from other companies cost a fortune.

Finally, I would like to thank my parents for their unending love and support during my study at Virginia Tech and throughout my life.

Several trademarks have been used in this thesis. These are as follows:

1. Java, Java Development Kit, Java Cryptography Extension, Java Cryptography Architecture and “Write Once, Run Anywhere” are trademarks of Sun Microsystem, Inc.
2. Netscape Navigator, Netscape Communicator, Object Signing, and Capabilities Classes are a trademarks of Netscape Communication Corporation.
3. Digital ID is a trademark of VeriSign, Inc.
4. Internet Explorer and Windows 95 are trademarks of Microsoft, Inc.
5. Cryptix is a trademark of Systemics, Limited.
6. Octane is a trademark of Silicon Graphics, Inc.
7. Pentium is a trademark of Intel Corporation.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES