A Secure Web-based Framework for Electronic System Level Design

Tom Kazmierski and Xing Q Yang
Dept of Electronics and Computer Science
University of Southampton
Southampton, SO17 1BJ, United Kingdom
tjk@ecs.soton.ac.uk, xqy199@ecs.soton.ac.uk

Abstract

This contribution presents the concept of a secure implementation of a distributed, web-based electronic design framework. Our two-tier client-webserver-toolserver architecture has been extended to support permanent databases for collaborative, distributed design development. In the sample application of the framework, developed in Java, any of the servers can be based on Linux, MS Windows or Sun-SPARC Java-servlet enabled server. The feasibility of a secure, web-based design framework has been sufficiently proved. The technological approach used to do this involves the use of novel, yet tried and tested methods, taking where appropriate from the rapidly advancing field of e-commerce solutions.

1 Introduction

The aim of the work presented in this contribution is to present the implementation of a secure web framework for electronic system design. The convergence of the Internet and distributed-object technologies has facilitated the recent success of electronic markets and it is this convergence that our project aims to take advantage of. A keynote presentation at the DAC 2000 Conference [8] outlined a concept of how Internet-enabled designs will allow companies to create global design groups to complete complex system-on-chip systems. Having looked at the current position of the Internet as a design framework in the Electronic Design Automation world [1] it is clear that there is a demand for globally accessible tools. Our project considers the development of a secure, session-based framework to which the addition of some sort of subscriber system should be straightforward. The increasing desire for flexible frameworks has led to the web being explored in order to improve traditional areas of weakness in communication and display of the design process [5].

The feasibility of a web-based CAD tool framework has been established in a system based on the VHDL-AMS compiler [3] using the Common Gateway Interface and returning textual information. The Star-Hspice optimizing analog circuit simulator is Avant!'s industrial-grade circuit analysis product for the simulation of electrical circuits. It was clear from an earlier version of this project [3] that some means of processing data gathered from a user to launch appropriate code modules would be required. In previous electronic design tool frameworks, this had come in the form of proprietary central control software or a command shell. The Internet, as the environment of choice for this project requires that a web server handle this function. The nature of the framework requires that files (e.g. netlists) be uploaded from a user's computer to the web server for processing. This is not as simple as it first appears. The file must be streamed through a Java StreamReader classes in order to write out to the file system. Commercial sensitivity of the transmitted information may require SSL-based secure protocols of data transfers between both a client and the web server, and the web and tool servers. Code was written to do this and it was thoroughly tested to check that no characters were missing or changes as this could have serious effects on a netlist or listing when compiling. Servlets can be combined to give a system, which will uniquely record a user's identification when writing the uploaded files to the web server file system. A system was developed to store data about when files were written and last accessed in order to allow the web server to recover in the event of a crash and delete expired files. The block diagram in figure 1 shows how all the Java servlets relate to each other.

2 Security

Communication between applets and the web-server is controlled by using the 'javakey' system [2] to 'sign' the applet. Data is then only provided to an applet with the correct signature. A secure connection ensures privacy, transmission integrity, authentication and authorization. Gener-

1530-1591/03 $17.00

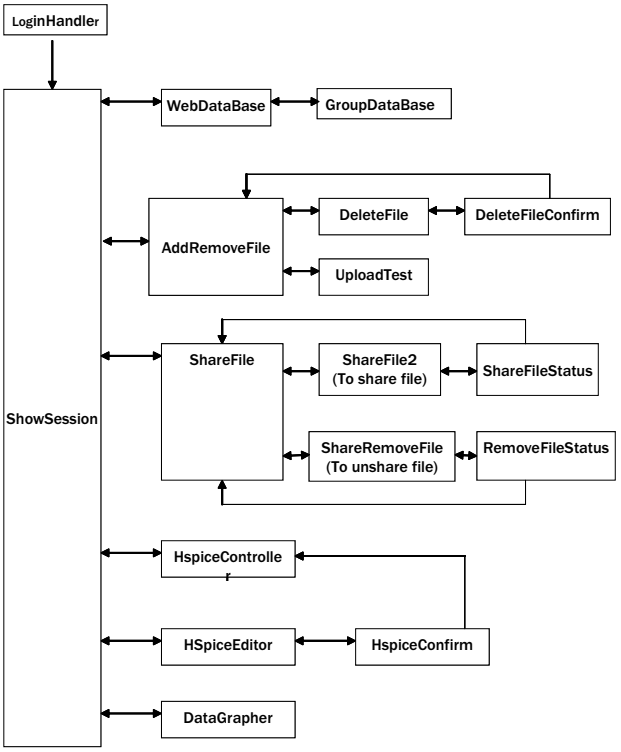

Figure 1. Java servlet configuration.

ally, all these points can be achieved by using a combination of key encryption of data, certificate exchanging and digital signatures. These functions can be implemented at a higher level but this would be tedious. Instead we have used OpenSSL. This allows the above program to run normally whiles the socket handles the algorithms, which are configured for the security.

OpenSSL and a special module (ModSSL) for Apache were installed. OpenSSL is an open source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general-purpose cryptography library. The ModSSL module provides strong cryptography for the Apache Server with the help of the OpenSSL toolkit. Once installed and configured a test certificate was created and self signed to test the connection. ModSSL integrates into the Apache server. This allows functionality for the server to use the OpenSSL toolkit to create secured connections.

Assuming that the whole system is behind a firewall then the tool servers can be protected from attacks. As only the Web Server would be viewable from the outside world. However, if the tool server was not behind a firewall then some sort of security needs to be applied. In the case of some one else trying to use the tool server with out going through the web server, it can be programmed so that the tool server only accepts connections from certain IP addresses i.e. the web server IP address. However, the link still may not be secure and private. Therefore, our system also implements secure connections by using JSSE (Java Secure Socket Extension) package with RMI. This allows us to create RMI sockets to uses the SSL protocol.

3 Conclusions

The constant development of electronic design tools from standalone simulators through integrated single user suites to network based systems such as the popular Cadence system shows the continuing importance of these tools to the electronic design world. The importance of the Internet as an environment for a global Electronic Design tool framework is clear. The feasibility of a web-based design framework has been sufficiently proved. The aim of this project was to further this proof by providing a platform independent framework supporting distributed tool servers that is sufficiently abstracted to make the integration of other tools a simple task. The technological approach used to do this will in the most part use tried and tested methods, taking where appropriate from the rapidly advancing field of e-commerce solutions. Research has shown that the electronic design world is centered on command-line tools that are the result of many years' iterative growth and as such it is a requirement of a web-based framework to be able to integrate these tools and provide interfaces that enable internet based communication of parameters and data.

References

[1] C. Ajluni. Internet-enabled tools open doors to new design strategies. *Electronic Design, Penton Media.*, 8(5), 6th March 2000.

[2] J. Jaworski. *Java 1.1 Developers Guide*. Sams.net Publishing, 2nd edition edition, 1997.

[3] T. Kazmierski and N. Clayton. A two-tier distributed electronic design framework. In *Proceedings DATE 2002*, pages 227–231, Paris, March 2002.

[4] G. McGraw and E. Felten. Secure computing with java: Now and the future. Whitepaper, Sun Microsystems Inc., 1997.

[5] A. Newton. Impact of web technologies on EDA system architectures. In *Proceedings ISPD'1998, Monterey, CA*. ISPD, April 6 1998.

[6] L. L. Peterson and B. S. Davie. *Computer Networks, a Systems Approach*. Morgan Kaufman, 2nd edition edition, 2000.

[7] J. L. Rogers and A. O. Salas. Towards a more flexible web-based framework for multidisciplinary design. *Advances in Engineering Software*, 30:439–444, January 1 1998.

[8] A. Sangiovanni-Vincentelli. The internet: the next IC design wnvironment. In *DAC'2000 Conference, Keynote presentation*, June 2000.

[9] A. Weissinger. *ASP in a Nutshell*. O'Reilly & Associates Inc, 2000.