Panel: Security and the World-Wide Web

Win Treese
treese@OpenMarket.com
Open Market, Inc.
245 First St. Cambridge, MA 02142

The World-Wide Web has emerged as a primary means of sharing information on the Internet. It is also a powerful platform for building applications and tying together disparate data sources. As the Web has grown, the demand for security services has grown as well. New applications such as electronic commerce, business transactions, and internal information sharing have driven the development of many different approaches to security on the Web.

Three years ago, security on the World-Wide Web largely meant authentication with passwords sent in the clear. Early security proposals included Secure HTTP (S-HTTP) and Shen, which provided rich security models but did not achieve widespread use. These protocols added capabilities for encryption, strong authentication, and digital signatures for Web documents.

Today, security on the World-Wide Web usually means the use of the Secure Sockets Layer (SSL). SSL provides an encrypted communications channel. It uses public key certificates for authentication of servers and optional authentication of clients. Version 3 of the SSL protocol was released earlier in 1996, and it has quickly become common in both Web browsers and servers. SSL version 3 improved the client authentication capabilities, and certifying authorities that can issue the necessary certificates have emerged to support them. The Internet Engineering Task Force (IETF) has chartered its Transport Layer Security (TLS) Working Group to specify a standard security protocol of this type.

More recently, the development of downloadable code, using technologies such as Java and ActiveX, has raised new risks. One response has been a set of proposals for digital signatures on downloaded code to authenticate the origin of programs.

Many organizations protect their networks with firewalls, isolating the internal network from the public Internet. Allowing security protocols through firewalls has posed a technical challenge as well as questions about appropriate security policies for such systems. Should Web clients authenticate themselves to the firewall before being allowed to make external connections? Should the firewall be able to read the data on a connection, in order to ensure that corporate policies are being followed?

Other work has looked at how to bring well-established security protocols to the Web. One example is the integration of the Web with the Open Group's Distributed Computing Environment (DCE).

This panel will examine the current state of security on the Web and discuss some of the challenges facing the Web community today. We will also look at the security problems and potential solutions on the road ahead.