'Guide to Secure Web Services' provides blueprint to safer Web 2.0

September 14 2007

Many Web-based services, from shopping to online word processing, allow computer programs to talk to each other and exchange user data across several Web sites without human intervention. Many of the attractive features of this "Web 2.0," including greater access to information and one-stop transactions that process information from several websites, are at odds with traditional ways of maintaining computer security.

A new NIST publication, called "Guide to Secure Web Services" (NIST Special Publication 800-95), provides details on how to make Web 2.0 more secure while maintaining its flexible and convenient features.

"The security challenges presented by the web services approach are formidable and unavoidable," according to the publication. "Difficult and unsolved problems exist," it continues, citing examples such as maintaining confidentiality and integrity in data that is transmitted via intermediary Web sites. Firewalls, which often protect single computers or networks from certain types of attack, are often inadequate to safeguard Web services data traveling between Web sites.

The publication recommends several steps to make Web services more secure. One recommended measure for content providers is to replicate their data and services at backup sites. This would improve the availability of their services in the event of "denial of service" (DoS) attacks intended to shut down a target Web site. Another recommendation is better and more uniform logging of visitors and

actions on Web sites. The publication also outlines several existing security techniques for making web services more secure, such as adding encryption to data transmitted through XML (eXtensible Markup Language), a protocol that allows the sharing and manipulation of data across different computer platforms.

Source: National Institute of Standards and Technology