Inside The Open Group

A Report on Emerging Technology and Standards

Security in Electronic Commerce

Through the use of standards and new technology, The Open Group is working toward bringing effective security to electronic commerce.

By Dean Adams

Are corporate distributed computing environments ready to embrace the World Wide Web and electronic commerce? Most people would answer No. Security solutions for one platform in the multivendor, distributed environment may not be portable between platforms or interoperate with the solutions on other platforms. The lack of a cohesive security standard for distributed systems is limiting the use of public networks, such as the Internet, for electronic commerce.

The Open Group is approaching this problem on two fronts. One is the process of threading together industry-accepted specifications into a coherent infrastructure for enterprise security, and delivering testing and branding programs to ensure vendor compliance with these specifications across platforms. The other is new technology development that fills gaps in the current picture for enterprise security and electronic commerce. Customer input, together with that of systems and software suppliers, is being actively included in the development of these new solutions.

Security product specifications are in various stages of development; some have already been delivered. These standard specifications are intended to be implemented on all systems participating in the distributed environment. They will be accompanied by test suites, and conformance to the product specifications will be enforced by the X/Open branding program. Consistent security will be guaranteed between systems passing the tests and branded to X/Open Security. Security product standards development can be categorized into three broad areas: security of the platform, security of the enterprise-wide network and security for open trading environments such as the Internet.

For the platform, a product standard specification has been delivered that defines a set of baseline security features for the commercial marketplace. For the enterprise-wide network, specifications are under development. A specification for secure communications is being implemented in products. This is being followed by product standard specifications for cryptographic services, distributed auditing, secure backup and restore, and single sign-on. In order to support operations in an open trading environment like the Internet, product standards for an Internet firewall and key management are under development.

A Range of Specifics

The Open Group has defined a standard specification for baseline security services. This defines a standard set of security facilities that should be made available on all computing platforms. In addition, it defines reasonable and safe default security parameters that are mandated on delivery of the system.

Distributed auditing provides the ability to audit the new types of distributed business applications that are being deployed. These distributed business applications may be made up of several communicating and integrated software components spread over several systems in the corporate network. The ability to audit these complex applications as a single logical entity is essential if sophisticated attacks involving more than one system are to be detected. A useful by-product of this standard will be a portable audit record format, which allows for the transport and merging of dissimilar audit streams.

A specification for secure communications services has been delivered and is being built implemented in products. It provides for the mutual authentication of distributed software entities and can protect ongoing communications between them. The Open Group also is developing a standard specification for single sign-on, whereby a user logs on only once to the enterprise-wide network of various systems.

The development of standard specifications for cryptography is high on The Open Group's agenda. A generic cryptographic services specification has just been completed. It insulates applications from whatever type of cryptography is being used, whether it is implemented in hardware or software. It supports both symmetric or private-key (secret) and asymmetric or public-key cryptography. Products based on this standard specification are being built, and the National Institute of Standards and Technology (NIST) has announced plans to base a federal procurement standard on it.

Cryptography—in particular, public-key cryptography—can provide the underpinning for various vital services required to support electronic commerce that are scalable on a worldwide basis. Follow-up work is under way to define key-management standards that support the use of cryptographic-based services in a global electronic commerce environment.

DCE Capabilities

Complementing The Open Group's security specification effort is a software development project to bring the secure enterprise computing capabilities of the Open Software Foundation's Distributed Computing Environment (OSF DCE) to the World Wide Web and electronic commerce. This effort incorporates technologies that support and are consistent with The Open Group security standards. These include Kerberos authentication, authorization based on the Posix standard access control list mechanism, and data privacy and integrity protection based on DES private-key and other standard encryption technologies.

The Open Group's standards for security are being combined with enabling technology for secure electronic commerce. This combination can move the business world closer to realizing the efficiencies it strives for and the opportunities offered by electronic commerce in public arenas such as the Internet. IT

***Dean Adams** is manager of security and electronic commerce for X/Open Co. He can be reached at d.adams@xopen.co.uk.*