Chapter V

Managing Security in the World Wide Web: Architecture, Services and Techniques

Fredj Dridi and Gustaf Neumann
University of Essen, Germany

Advances in the World Wide Web technology have resulted in the proliferation of significant collaborative applications in commercial environments. However, the World Wide Web as a distributed system, which introduces new technologies (like Java applets and ActiveX) and uses a vulnerable communication infrastructure (the Internet), is subject to various security attacks. These security attacks violate the confidentiality, integrity, and availability of Web resources. To achieve a certain degree of Web security and security management, different protocols and techniques have been proposed and implemented. This is still a hot topic in the current research area and still requires more ambitious efforts.

We give an overview of the Internet security issues with special emphasis on the Web security. We describe an architecture built up by the means of security services to shield against these threats and to achieve information security for networked systems like the WWW. We focus on the authentication and access control services (like role-based access control) and their administration aspects. We discuss several elementary techniques and Internet standards which provide state-of-the-art of Web security.

The World Wide Web (WWW or Web) is a distributed, collaborative hypertext- and hypermedia-based information system and uses the Internet, a global public TCP/IP based communication architec-
ture, as a transport mechanism. The Web is today the most significant use of the Internet. It introduces new protocols and standards (like HTTP, HTML, CGI, XML, RDF, etc.) which have the potential to be used in complex distributed applications. Since the Web technology can be used to provide uniform access to a wide variety of information managed by different organizations, enterprises are increasingly using the it to access Internet corporate information as well.

Advances in the Web technologies have resulted in the proliferation of significant collaborative applications in commercial environments. Collaborative applications is the term used to denote a class of applications which facilitate information sharing in an inter- or intra-enterprise environment. Examples of collaborative applications are: groupware, document (project) management, electronic commerce, and workflow automation, etc.

The term intranet usually refers to an internal enterprise network, that uses Web technology. In large organizations collaborative applications are relevant to a large number of users who want to share and grant access to documents in a controlled way. Typically, the documents are placed on various decentralized Web servers. Some of those documents may contain sensitive information and consequently must not be disclosed to every user. In addition, because the Web uses the Internet as its transport mechanism, it inherits all of the security vulnerabilities of the Internet. As a result, the demand for security services (like authentication, access control, non-repudiation service, etc.) has grown rapidly. The documents and the administration of access rights for a huge number of users is becoming increasingly complex.

The area of Inter-/Intranet and Web security is a very active research area where new approaches and techniques are constantly proposed. Literature references addressing this topic in more detail are, for example, Garfinkel and Spafford (1997); Lipp and Hassler (1996); and Oppliger (1998). In this chapter, we give an overview of the Internet security issues, with special emphasis on Web security. First, we give an introduction to the various types of security attacks the Web-based applications are exposed to. Next we describe a communication-based architecture, e.g. the Internet, for building collaborative applications. This architecture contains several services: communication, coordination, cooperation, and security services. We focus on the security services and their administration and management.
Related Content

Handling the Dataflow in Business Process Models
www.igi-global.com/chapter/handling-the-dataflow-in-business-process-models/198255?camid=4v1a

Risk Analysis Using Earned Value: An Engineering Project Management Study
www.igi-global.com/article/risk-analysis-using-earned-value/133545?camid=4v1a

The Compliance of IT Control and Governance: A Case of Macao Gaming Industry
www.igi-global.com/article/the-compliance-of-it-control-and-governance/155103?camid=4v1a
Malware Detection and Prevention System Based on Multi-Stage Rules
International Journal of Information Security and Privacy (pp. 29-43).
www.igi-global.com/article/malware-detection-and-prevention-system-based-on-multi-stage-rules/87413?camid=4v1a