Journal of Computer Security 5 (1997) 189–190
IOS Press

Guest Editors' Preface

Special issue on Security in the World Wide Web (WWW)

Despite its initial goal as a tool to support scientists in their research, the World Wide Web (WWW) has today become essential whenever information needs to be widely and rapidly disseminated. WWW is now used in a large variety of organizations, including social, business, and government organizations, and applications, such as education, entertainment and commerce. As an increasing number of organizations and applications start depending on WWW for some of their functions, security becomes crucial. Moreover, the novel applications, enabled by WWW, introduce new security requirements and raise issues that have not been addressed before.

The focus of this special issue is on research and development efforts leading to identify requirements and viable solutions for WWW security. This special issue contains two regular papers and four short papers describing on-going projects.

The paper "Strong authentication and privacy with standard browsers", by F. Bergadano, B. Crispo and M. Lomas, deals with the problem of securing client/server communications by means of strong encryption and authentication. The proposed approach is based on public key cryptography and is performed outside the browser, by using applets and other installed software. In the paper, a new certification scheme is also proposed supporting the principles of separation of duty and maintenance of sufficient evidence. The certification scheme makes use of a Certification Authority and a Revocation Authority in any domain of users. The authors also show how their approach proves correct even if one party misbehaves.

In the paper "Authentication of sequences with the SL_2 hash function: application to video sequences", J.-J. Quisquater and M. Joye propose an approach to authenticate a sequence of images. The approach is intended to be applied in cases where a sequence of images undergoes an editing process that removes some images. Goal of the approach is to guarantee that the edited sequence is a subsequence of the original sequence. At the time of the original recording, cryptographic information is computed. The camera is committed in the signature process from a secret attached to it and no valid signature can be generated outside the camera. The proposed approach permits the detection of any manipulation after the original recording.

In the first project synopsis "CWASAR: a European infrastructure for secure electronic commerce", C. Bryce, W. Kühnhauser, R. Amouroux, M. López and H. Rudnik describe CWASAR (Cooperative Wide-Area Service Architecture), a project to design and implement a low-cost European infrastructure for a secure electronic

market place. The project is intended to produce an electronic commerce infrastructure for small and medium-size enterprises in Europe. The paper describes the main functional and architectural components proposed in the project. In particular, the authors illustrate the various user requirements that need to be addresses in such a framework and the problems posed by the different legal positions held by many individual EU states on the use of security techniques.

The paper "Private Web browsing" by P.F. Syverson, M.G. Reed and D.M. Goldshlag deals with the problem of protecting the privacy of network communications. Most protection systems available today protect only the data being transmitted but do not protect the identities of the communicating parties. The authors extend the notion of privacy to include confidentiality of both the data stream being transmitted and the identities of the communicating parties. In the proposed approach, data streams and identities are kept secret from both network elements and external eavesdroppers. This protects against traffic analysis. An implementation of the proposed approach is also described.

In the paper "A network-centric design for relationship-based security and access control" M. Röscheisen and T. Winograd propose a relationship based approach for defining rights and controlling access in heterogeneous networked environments. In the approach proposed by the authors, information exchanges are regulated by specifying relationships between the different entities. The paper describes the architecture that provides the basis for the user-conceptual model of access control and the prototype that provides an interface for direct manipulation of the objects available through the architecture.

In the paper "Using digital credentials on the World Wide Web" M. Winslett, N. Ching, V. Jones, and I. Slepchin describe their project exploring the use of digital credentials in enforcing access control to objects available through the Web. The approach proposed by the authors departs from the traditional identity-based access control to address situations in which access to particular objects can be granted by virtue of some properties or association of the requesting subject rather than of its identity. In the proposed approach, servers maintain policies describing credentials needed to access each of the objects they make available. Clients requesting access will be asked to provide the necessary credentials and only then access will be granted. The paper describes the main problems to be tackled in such a framework and discusses the problems to be addressed in the design and development of automated procedures to enforce these credential-based policies at both the client and the server.

Elisa Bertino *Pierangela Samarati* *Gian Paolo Rossi*