Network Working Group
Request for Comments: 1511

J. Linn
Geer Zolot Associates

September 1993

Common Authentication Technology Overview

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard. Distribution of this memo is unlimited.

Overview

The IETF's Common Authentication Technology (CAT) working group has pursued, and continues to pursue, several interrelated activities, involving definition of service interfaces as well as protocols. As a goal, it has sought to separate security implementation tasks from integration of security data elements into caller protocols, enabling those tasks to be partitioned and performed separately by implementors with different areas of expertise. This strategy is intended to provide leverage for the IETF community's security-oriented resources (by allowing a single security implementation to be integrated with, and used by, multiple caller protocols), and to allow protocol implementors to focus on the functions that their protocols are designed to provide rather than on characteristics of particular security mechanisms (by defining an abstract service which multiple mechanisms can realize).

The CAT WG has worked towards agreement on a common service interface, (the Generic Security Service Application Program Interface, or GSS-API), allowing callers to invoke security functions, and also towards agreement on a common security token format incorporating means to identify the mechanism type in conjunction with which security data elements should be interpreted. The GSS-API, comprising a mechanism-independent model for security integration, provides authentication services (peer entity authentication) to a variety of protocol callers in a manner which insulates those callers from the specifics of underlying security mechanisms. With certain underlying mechanisms, per-message protection facilities (data origin authentication, data integrity, and data confidentiality) can also be provided. This work is represented in a pair of RFCs: RFC-1508 (GSS-API) and RFC-1509 (concrete bindings realizing the GSS-API for the C language).

Concurrently, the CAT WG has worked on agreements on underlying security technologies, and their associated protocols, implementing the GSS-API model. Definitions of two candidate mechanisms are currently available as Internet specifications; development of additional mechanisms is anticipated. RFC-1510, a standards-track specification, documents the Kerberos Version 5 technology, based on secret-key cryptography and contributed by the Massachusetts Institute of Technology. RFC-1507, an experimental specification, documents the Distributed Authentication Services technology, based on X.509 public-key technology and contributed by Digital Equipment Corporation.

References

[1] Kaufman, C., "Distributed Authentication Security Service", RFC 1507, Digital Equipment Corporation, September 1993.

[2] Linn, J., "Generic Security Service Application Program Interface", RFC 1508, Geer Zolot Associates, September 1993.

[3] Wray, J., "Generic Security Service API : C-bindings", RFC 1509, Digital Equipment Corporation, September 1993.

[4] Kohl, J., and C. Neuman, "The Kerberos Network Authentication Service (V5)", Digital Equipment Corporation, USC/Information Sciences Institute, September 1993.

Security Considerations

Security issues are discussed throughout the references.

Author's Address

John Linn
Geer Zolot Associates
One Main St.
Cambridge, MA 02142 USA

Phone: +1 617.374.3700
Email: Linn@gza.com