INTERNET-DRAFT
Expires in six months

G. Bossert
S. Cooper
Silicon Graphics Inc.
W. Drummond
IEEE, Inc.

February, 1996

Requirements for Web Transaction Security

<draft-ietf-wts-requirements-01.txt>

Status of this Memo

Abstract

This document specifies the requirements for the provision of security services to the HyperText Transport Protocol. These services include confidentiality, integrity, user authentication, and authentication of servers/services, including proxied or gatewayed services. Such services may be provided as extensions to HTTP, or as an encapsulating security protocol. Secondary requirements include ease of integration and support of multiple mechanisms for providing these services.

1. Introduction

The use of the HyperText Transport Protocol [1] to provide specialized or commercial services and personal or private data necessitates the development of secure versions that include privacy and authentication services. Such services may be provided as extensions to HTTP, or as encapsulating security protocols; for the purposes of this document, all such enhancements will be referred to as WTS.

In this document, we specify the requirements for WTS, with the intent of codifying perceived Internet-wide needs, along with

existing practice, in a way that aids in the evaluation and development of such protocols.

WTS is an enhancement to an object transport protocol. As such, it does not provide independent certification of documents or other data objects outside of the scope of the transfer of said objects. In addition, security at the WTS layer is independent of and orthogonal to security services provided at underlying network layers. It is envisioned that WTS may coexist in a single transaction with such mechanisms, each providing security services at the appropriate level, with at worst some redundancy of service.

1.1 Terminology

This following terms have specific meaning in the context of this document. The HTTP specification [1] defines additional useful terms.

Transaction:
A complete HTTP action, consisting of a request from the client and a response from the server.

Gatewayed Service:
A service accessed, via HTTP or an alternate protocol, by the HTTP server on behalf of the client.

Mechanism:
An specific implementation of a protocol or related subset of features of a protocol.

2. General Requirements

WTS must define the following services. These services must be provided independently of each other and support the needs of proxies and intermediaries

- Confidentiality of the HTTP request and/or response.
- Data origin authentication and data integrity of the HTTP request and/or response.
- Non-repudiability of origin for the request and/or response.
- Transmission freshness of request and/or response.
- Ease of integration with other features of HTTP.
- Support of multiple mechanisms for the above services.

3. Confidentiality

WTS must be able to provide confidentiality for both requests and responses. Note: because the identity of the object being requested is potentially sensitive, the URI of the request should be confidential; this is particularly critical in the common case of form data or other user input being passed in the URI.

4. Service Authentication

WTS should support the authentication of gatewayed services to the client.

WTS should support the authentication of the origin HTTP server or gatewayed services regardless of intermediary proxy or caching servers.

To allow user privacy, WTS must support service authentication with user anonymity.

Because the identity of the object being requested is potentially sensitive, service authentication should occur before any part of the request, including the URI of the requested object, is passed. In cases where the authentication process depends on the URI (or other header data) of the request, such as gatewayed services, the minimum necessary information to identify the entity to be authenticated should be passed.

5. User Authentication

WTS must support the authentication of the client to the server.

WTS should support the authentication of the client to gatewayed services.

WTS should support the authentication of the client to the origin HTTP server regardless of intermediary proxy servers.

6. Integrity

WTS must provide assurance of the integrity of the HTTP transaction, including the HTTP headers and data objects of both client requests and server responses.

7. Integration

In order to support integration with current and future versions of HTTP, and to provide extendibility and independence of development, the secure services provided by WTS must be orthogonal to and independent of other services provided by HTTP.

In accordance with the layered model of network protocols, WTS must be:

- independent of the content or nature of data objects being transported although special attention to reference integrity of hyperlinked objects may be appropriate

- implementable over a variety of connection schemes and underlying transport protocols

8. Multiple Mechanisms

WTS must be compatible with multiple mechanisms for authentication and encryption. Support for multiple mechanisms is required for a number of reasons:

- Accommodation of variations in site policies, including those due to external restrictions on the availability of cryptographic technologies.
- Support for a variety of applications and gatewayed services.
- Support for parallel implementations within and across administrative domains.
- Accomodation of application-specific performance/security tradeoffs.

To allow interoperability across domains, and to support the transition to new/upgraded mechanisms, WTS should provide negotiation of authentication and encryption mechanisms.

References

[1] T. Berners-Lee, R. T. Fielding, and H. Frystyk Nielsen. "Hypertext Transfer Protocol -- HTTP/1.0" Internet-Draft <URL:gopher://ds1.internic.net/00/internet-drafts/draft-ietf-http-v10-spec-05.txt>, February, 1996

[2] G. Bossert, S. Cooper, W. Drummond. "Requirements of Secure Object Transfer Protocols" <URL:http://www-ns.rutgers.edu/www-security/draft/draft-rutgers-sotp-requirements-00.txt>, March 1995.

The revision history of this document can be located at <URL:http://reality.sgi.com/csp/wts-wg/wts-documents.html>

Acknowledgments

This document is a product of the IETF WTS working group. The working group uses the wts-wg@postofc.corp.sgi.com mailing list for discussion. The subscription address is wts-wg-request@postofc.corp.sgi.com.

Eric Rescorla of Terisa <ekr@terisa.com> provided valuable comments on an early draft of a document called "Requirements of Secure Object Transfer" [2], a principal influence on this document.

Security Considerations

As noted above.

Author's Addresses

Greg Bossert -- bossert@corp.sgi.com
Simon Cooper -- sc@corp.sgi.com
Silicon Graphics, Inc. MS 15-7
2011 North Shoreline Blvd.
Mountain View, CA 94043-1389
USA

Walt Drummond -- drummond@ieee.org
Institute of Electrical and Electronics Engineers, Inc.
445 Hoes Lane
Piscataway, NJ 08855-1331
USA
PH: 908-562-6545
FAX:908-562-1727