Internet Draft
Intended status: Informational
Expires: December 31, 2013

K. Malbrain
Petz Enterprises LLC

September 23, 2013

Problem Statement: Deployment of TLS Strong Authentication
draft-malbrain-tls-strong-authentication-01

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on December 31, 2013.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Abstract

The security provided by authenticated TLS connection between clients and servers should protect both parties from "Man-in-the-Middle" (MITM) attacks. Clients should be authenticating that their server connection is to the server they requested.

Servers that act as client agents need to authenticate that the connection is directly to their client secure against eavesdropping or account/password hacking.

An extension to the Domain Name System (DNS), The DNS-Based Authentication of Named Entities (DANE) (RFC 6698), allows TLS servers to publish their public certificates for use by TLS clients to authenticate the server connection.

Table of Contents

1. Introduction

TLS strong authentication by clients of their servers relies on comparison by the client of public certificates authenticated by TLS session negotiations [RFC 5246 Appendix

F] with a trusted copy of the certificate. DANE is a database of public key certificates published by the Domain Name owners in the DNS database, and made available by appropriate DNS queries.

On the server side there is currently only client certificate signing by Certificate Authorities (CA) under current TLS strong authentication of clients by servers [RFC 5246 Appendix D]. Of servers maintaining personal information on behalf of non-anonymous clients, few demand TLS strong authentication because of the lack in general of signed client certificates.

2. Server Authentication

The global network of DNS servers stores and makes available via query the public key certificates (or their hash values) and IP addresses submitted and maintained by Domain Owners [RFC 6698 Section 1.1].

Whenever a client application needs an authenticated TLS connection to a Domain Server, DNS supplies the Domain's IP address and either a copy of a certificate placed by the server or its hash value [RFC 6698 Section 2.1.3].

3. Client authentication

At the end of TLS session negotiation, the TLS implementation optionally makes available the client's public certificate if requested during TLS negotiations. This currently must be a certificate signed by one of the CA which is used by the server to authenticate an established client that the server recognizes.

If the server desires strong authentication and is open to connections from new clients, and in lieu of storing the entire client certificate, it should save a hash of the client certificate as part of the account data for authentication in future client logins.

4. Thwarting MITM and Login attacks

Making use of the server certificates, TLS strong authentication includes both a verification that the server holds the private key for the certificate, and a comparison of that public certificate against a trusted third party version.

A MITM attacker inserts a middle point between the client and server under a forged bogus certificate provided to the client during TLS session negotiations. Since there is a second, reliable source of server's public certificates available through DANE, it is now possible for the client to recognize the forged certificate used by the bogus connection by comparison with the server certificate registered for the Domain Name with DNS.

Likewise servers that hold personal data for non-anonymous clients should be utilizing the hash of the client's public certificate to recognize connections to previously established accounts even prior to requesting the account name and password.

5. Why TLS authentication is not working

The ability by TLS to perform for strong authentication by clients of server certificates during TLS negotiations is widely deployed. DANE provides the capability to post and retrieve IP addresses and public certificates for Domain Names in the DNS system. Servers could take the extra step to authenticate client certificates.

5.1. Browser acceptance of DANE

Browser vendors don't like using the DANE protocol because it requires an additional DNS request to obtain both the Domain IP address and public certificate for the DNS Server

DNS requests and their response are normally made using a single UDP packet. The size of the packet is limited by the DNS protocol to 512 bytes.

Either by utilizing larger packet sizes, up to 65536 bytes in IPv4, or by utilizing tcp or QUIC connections, along with an ability to request and return both the Domain Name IP address and public certificate in a single request could solve this problem.

5.2. Client Certificates

The average internet user doesn’t have a public certificate signed by a CA, despite its utility to both HTTPS and S/MIME applications.

Certificate generating software is freely available. Browser vendors could incorporate self-signed public/private key certificates on demand.

5.3. Client Authentication

Server software doesn't ask for a user certificate during TLS negotiations. Server operators need to exercise due diligence in securing client connections beyond the traditional login account and password to guarantee that private information is not being revealed to third parties. Storing and comparing on each connection the hash of the user's public certificate for each server account would provide another layer of security for the internet against MITM or Account Hacking.

6. Certificate Notaries

A criticism of DANE holds that it is merely a substitution of trust in Certificate Authorities for trust in DNS servers. The Carnegie-Mellon project "PERSPECTIVES" establishes a network of Notaries for Server Certificates. A wide scale deployment of this technology could address this.

7. References

7.1. Normative References

[RFC6698] Hoffman P. and Schlyter, J., "The DNS-Based Authentication of Named Entities (DANE)", RFC 6698, August 2012.

[RFC5246] Dierks T. and Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

8. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

Copyright (c) 2013 IETF Trust and the persons identified as authors of the code. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted pursuant to, and subject to the license terms contained in, the Simplified BSD License set forth in Section 4.c of the IETF Trust's Legal Provisions

Relating to IETF Documents (http://trustee.ietf.org/license-info).

Copyright (c) 2013 IETF Trust and the persons identified as authors of the code. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted pursuant to, and subject to the license terms contained in, the Simplified BSD License set forth in Section 4.c of the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info).

Author's Address

Karl Malbrain
Petz Enterprises, LLC
7575 W Linne Rd
Tracy, CA 95377

Email: Malbrain at Yahoo dot com