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

K. Malbrain
Petz Enterprises LLC

September 17, 2013

Problem Statement: Deployment of TLS Strong Authentication
draft-malbrain-tls-strong-authentication-00

Status of this Memo

Copyright Notice

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 the server they are connected to is the server they requested, and servers that act as client agents need to authenticate that the connection is directly to their client.

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]. Few servers demand authentication because of the lack of signed client certificates.

2. The Global directory of servers' public keys (DANE)

A network of DNS servers stores and makes available via query the public key certificates and IP address submitted and maintained by their Domain Owners.

Whenever a client application needs an authenticated and secure TLS connection into a Domain, DNS supplies the Domain's IP address and public certificate.

3. TLS authentication of clients by servers

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 and a hash of the certificate could be used by the server to authenticate the connection to an established client that the server recognizes from previous connections. Otherwise, it is up to the server and client to authenticate the certificate with a non-standard challenge exchange.

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

Unfortunately, there is no standard challenge/response by the server of the client's public and private key in the current TLS version 1.2. which is needed to use self-signed certificates.

4. MITM and Login Hacker attacks are precluded on strongly authenticated TLS connections

Making use of the public keys from the server certificates, TLS strong authentication includes a challenge that the certificate presenter holds the private key for the public certificate. A MITM attacker inserts a middle point between the client and the server under a forged bogus certificate provided to the client during TLS session negotiations. Since there is a 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 the server could utilize a hash of the client's public certificate to recognize connections to previously established accounts prior to demanding the account name and password.

5. Why this is not working as designed to obviate attacks and what can be done about the current state of affairs

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 vendors don't like 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 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. The average internet user doesn't have a signed public certificate and private key pair signed by a CA

Certificate generating software is freely available. Browser vendors could incorporate self-signed public/private key certificates on demand. The TLS server authentication of the client could be based on an additional challenge/response message exchange.

5.3. Server software doesn't ask for user certificates 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.

6. References

6.1. 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.

7. Acknowledgments

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

Author's Address

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

Email: Malbrain at Yahoo dot com