None
Internet-Draft
Intended status: Standards Track
Expires: December 5, 2009

P. Saint-Andre
Cisco
K. Zeilenga
Isode Limited
J. Hodges
NeuStar
R. Morgan
Internet2
June 3, 2009

Best Practices for Checking of Server Identities in the Context of Transport Layer Security (TLS)
draft-saintandre-tls-server-id-check-00

Status of this Memo

Copyright Notice

Abstract

This document specifies the how an entity establishing a TLS connection, or other PKI-based interaction, with a server should verify the server identity.

Table of Contents

1. Introduction

Establishing a TLS-based connection [TLS] with a server, or any other sort of client-server PKI-based interaction, entails, on the part of the client, verifying the "server's identity" based upon information presented by the server in its certificate correlated with the information about the server ensconced in the Domain Name System (DNS).

Presently, various Internet-Drafts utilizing TLS or prescribing PKI-based interactions, either prescribe their own server identity check, or reference [LDAP-AUTH] or its predecesor [LDAP-TLS]. [there may be other I-Ds referencing other specs that describe the equivalent of server identity checks]

Converging our present understanding of this critical aspect of PKI-based interactions is desirable in that it will hopefully encourage more coherence in specifications and actual implementations thereof, as well as ease the burden of crafting new specifications because this aspect has been factored out and separately standardized.

This document extracts the "server identity check" section from [LDAP-AUTH], with the goal of becoming a stand-alone BCP document appropriately referenceable by I-Ds and thus RFCs.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [TERMS].

3. Server Identity Check

In order to prevent man-in-the-middle attacks, the client MUST verify

the server's identity (as presented in the server's Certificate message). In this section, the client's understanding of the server's identity (typically the identity used to establish the transport connection) is called the "reference identity".

The client determines the type (e.g., DNS name or IP address) of the reference identity and performs a comparison between the reference identity and each subjectAltName value of the corresponding type until a match is produced. Once a match is produced, the server's identity has been verified, and the server identity check is complete. Different subjectAltName types are matched in different ways. Sections 3.1.3.1 - 3.1.3.3 explain how to compare values of

various subjectAltName types.

The client may map the reference identity to a different type prior to performing a comparison. Mappings may be performed for all available subjectAltName types to which the reference identity can be mapped; however, the reference identity should only be mapped to types for which the mapping is either inherently secure (e.g., extracting the DNS name from a URI to compare with a subjectAltName of type dNSName) or for which the mapping is performed in a secure manner (e.g., using DNSSEC, or using user- or admin-configured host-to-address/address-to-host lookup tables).

The server's identity may also be verified by comparing the reference identity to the Common Name (CN) [LDAP-SCHEMA] value in the leaf Relative Distinguished Name (RDN) of the subjectName field of the server's certificate. This comparison is performed using the rules for comparison of DNS names in Section 3.1.3.1, below, with the exception that no wildcard matching is allowed. Although the use of the Common Name value is existing practice, it is deprecated, and Certification Authorities are encouraged to provide subjectAltName values instead. Note that the TLS implementation may represent DNs in certificates according to X.500 or other conventions. For example, some X.500 implementations order the RDNs in a DN using a left-to-right (most significant to least significant) convention instead of LDAP's right-to-left convention.

If the server identity check fails, user-oriented clients SHOULD either notify the user (clients may give the user the opportunity to continue with the LDAP session in this case) or close the transport

connection and indicate that the server's identity is suspect. Automated clients SHOULD close the transport connection and then return or log an error indicating that the server's identity is suspect or both.

Beyond the server identity check described in this section, clients should be prepared to do further checking to ensure that the server is authorized to provide the service it is requested to provide. The client may need to make use of local policy information in making this determination.

3.1. Comparison of DNS Names

If the reference identity is an internationalized domain name, conforming implementations MUST convert it to the ASCII Compatible Encoding (ACE) format as specified in Section 4 of [IDNA] before comparison with subjectAltName values of type dNSName. Specifically, conforming implementations MUST perform the conversion operation specified in Section 4 of RFC 3490 as follows:

- in step 1, the domain name SHALL be considered a "stored string";
- in step 3, set the flag called "UseSTD3ASCIIRules";
- in step 4, process each label with the "ToASCII" operation; and
- in step 5, change all label separators to U+002E (full stop).

After performing the "to-ASCII" conversion, the DNS labels and names MUST be compared for equality according to the rules specified in Section 3 of RFC3490.

The '*' (ASCII 42) wildcard character is allowed in subjectAltName values of type dNSName, and then only as the left-most (least significant) DNS label in that value. This wildcard matches any left-most DNS label in the server name. That is, the subject *.example.com matches the server names a.example.com and b.example.com, but does not match example.com or a.b.example.com.

3.2. Comparison of IP Addresses

When the reference identity is an IP address, the identity MUST be converted to the "network byte order" octet string representation [IP] [IPv6]. For IP Version 4, as specified in RFC 791, the octet string will contain exactly four octets. For IP Version 6, as

specified in RFC 2460, the octet string will contain exactly sixteen octets. This octet string is then compared against subjectAltName values of type iPAddress. A match occurs if the reference identity octet string and value octet strings are identical.

3.3. Comparison of Other subjectName Types

Client implementations MAY support matching against subjectAltName values of other types as described in other documents.

4. Security Considerations

To follow.

5. References

5.1. Normative References

[IDNA] Faltstrom, P., Hoffman, P., and A. Costello, "Internationalizing Domain Names in Applications (IDNA)", RFC 3490, March 2003.

[IP] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[IPv6] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[LDAP-AUTH] Harrison, R., "Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms", RFC 4513, June 2006.

[LDAP-SCHEMA] Sciberras, A., "Lightweight Directory Access Protocol (LDAP): Schema for User Applications", RFC 4519, June 2006.

[TERMS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

5.2. Informative References

[LDAP-TLS] Hodges, J., Morgan, R., and M. Wahl, "Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security", RFC 2830, May 2000.

Authors' Addresses

Peter Saint-Andre
Cisco

Email: psaintan@cisco.com

Kurt D. Zeilenga
Isode Limited

Email: Kurt.Zeilenga@Isode.COM

Jeff Hodges
NeuStar

Email: Jeff.Hodges@KingsMountain.com

RL 'Bob' Morgan
UWashington/Internet2

Email: rlmorgan@washington.edu