National Infrastructure Security Co-ordination Centre

TLS/SSL ASN.1 Vulnerability Testing

Version 1.0

This document and its content shall only be used for the purpose for which it was issued.
The copyright of this document is reserved and vested in the crown.

©2002 Crown Copyright

Executive Summary

NISCC and CESG have undertaken testing of a representative sample of commercial TLS web-servers to determine their susceptibility to ASN.1 vulnerabilities of the type researched by the University of Oulu's Secure Programming Group.

All of the web-servers tested have been found to have difficulties handling *exceptional* ASN.1 elements.

It is likely that other TLS products, e.g. web-browsers may also be vulnerable to Oulu-style vulnerabilities

NISCC is providing this information to system vendors in order to help them investigate and resolve these difficulties. It is hoped that vendors whose products are affected will be able to devise patches to address the underlying problems, or to produce recommendations for their customers of suitable mitigation measures.

Table of Contents

References

[CERT] CERT advisory CA-2002-23 Multiple vulnerabilities in OpenSSL, CERT/CC, 15 August 2002, available from http://www.cert.org/advisories/CA-2002-23.html

[Netcraft] Netcraft Secure Server Study, July 2002

[Oulu] PROTOS – Security Testing of Protocol Implementations, 19 July 2000, available from http://www.ee.oulu.fi/research/ouspg/protos/index.html

[PKCS#1] RSA Data Security, Inc Public-Key Cryptography Standards (PKCS), version 1.5, November 1993

[SSL] The SSL 3.0 Protocol, Netscape Communications Corp, . Frier et al November, 1996

[TLS] The TLS Protocol, Version 1.0, RFC 2246, Dierks et al, January 1999

[TLSWG] The Transport Layer Security Working Group Charter, available from http://www.ietf.org/html.charters/tls-charter.html

Acronyms

ASN.1	Abstract Syntax Notation 1
DSA	Digital Signature Algorithm
HTTP	Hypertext transfer protocol
HTTPS	HyperText Transmission Protocol, Secure
LDAPv3	Lightweight Directory Access Protocol version 3
PKCS#1	Public-Key Cryptography Standard #1
RSA	Rivest, Shamir, Adleman
SNMPv1	Simple Network Management Protocol version 1
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol over Internet Protocol
TLS	Transport Layer Security

1. INTRODUCTION

1.1.1 The University of Oulu's Secure Programming Group identified vulnerabilities in certain computer and communications protocols. Recent work performed by the Group has identified vulnerabilities in implementations of two ASN.1 based protocols: LDAPv3 and SNMPv1, [Oulu]. Oulu identified that a number of implementations were unable to safely handle *exceptional* (i.e. unusual or atypical) elements of ASN.1.

1.1.2 Analysis of the work performed by Oulu suggests that implementations of other ASN.1 based protocols may be vulnerable in a similar manner.

1.1.3 Preliminary work identified the requirement for further analysis of the TLS protocol and the need to determine the susceptibility of TLS implementations to mishandling exceptional ASN.1 elements received as part of the protocol.

1.1.4 This document describes the analysis made and the method used to examine particular TLS implementations and provides a summary of the results of testing.

1.1.5 The application testing examined web-servers using TLS to provide mutual authentication between web-server and web-client.

1.1.6 Each of the web-servers examined were found to have difficulties handling some exceptional ASN.1 elements. The exact details have been omitted from this document to allow vendors the opportunity to resolve these issues before wider dissemination.

1.1.7 The web-servers tested were chosen to be a representative sample of the common TLS web-servers in use.

1.1.8 Other applications using TLS may be as likely to be vulnerable to exceptional ASN.1 elements as web-servers have been demonstrated to be.

2. OVERVIEW OF TLS

2.1 What is TLS/SSL

2.1.1 TLS/SSL are intermediate protocols layered onto a TCP connection used to provide additional security to higher-level protocols. TLS/SSL are intended to provide security functionality between two TCP end points. Higher-level protocols, particularly application protocols such as web services or e-mail may be layered on top of a TLS/SSL connection.

2.1.2 TLS is based on SSL 3.0 and may be viewed as effectively being SSL 3.1. Although the two protocols are not interoperable, implementations of TLS 1.0 are likely to support SSL 3.0. For the purposes of the discussion below the differences are not significant.

2.1.3 An application may initiate, receive or both initiate and receive TLS connections. An application initiating a TLS connection is considered to be the TLS client. An

application receiving a TLS connection is considered to be the TLS server. Some applications are capable of acting as a TLS client and a TLS server.

2.1.4 TLS is defined in [TLS] and additional information on TLS and its development may be obtained from [TLSWG]. SSL is defined in [SSL].

2.1.5 TLS is not an ASN.1 based protocol and defines its own presentation language as part of the TLS specification. However, TLS makes use of ASN.1 fragments, particularly during the TLS Handshake protocol where cryptographic parameters are established.

2.2 TLS Handshake Protocol

2.2.1 The TLS Handshake Protocol is used to agree cryptographic parameters between the participants of a TLS session. The parameters are typically negotiated at the beginning of a session and may be renegotiated during a session.

2.2.2 TLS has a number of security options and depending on the security features desired the protocol elements used during the handshake may differ. For example, a TLS connection may negotiate no authentication between participants, authentication of one participant (typically the server) or mutual authentication between both participants. The protocol elements used may differ according to which algorithms are being used and the manner in which cryptographic variables are generated.

3. ANALYSIS OF TLS ASN.1 USAGE

3.1 X.509 Certificates

3.1.1 X.509 certificates are the largest single blocks of ASN.1 used within TLS. An X.509 certificate will contain a public key, the electronic identity of the public key, the electronic identity of the issuer of the certificate and supplementary information relating to these three principle data items. The supplementary information may typically include information about the validity

3.1.2 An X509 certificate has the potential to contain a relatively large amount of information with maybe 300 primitive ASN.1 elements. Simple X.509 certificates may have as little as approximately 20 primitive ASN.1 elements. Typical sizes of certificates may range from 400 bytes to 2000 bytes.

3.1.3 Not all of the information contained within a certificate may be processed by an application. Some certificates may contain additional information that is not strictly necessary for the establishment of the TLS session. Some applications may not make use of all the data within the certificate for the purposes of validity checking. For example, some applications may not perform validity or path verification – these functions may be configuration options within an application.

3.1.4 TLS makes use of public key certificates in two places: the server certificate message and the client certificate message. The server certificate is passed from the server to the client if authentication is taking place. The client certificate

is passed from client to server when mutual authentication has been configured. The TLS specification simply provides space for the exchange of certificates as part of the protocol.

3.1.5 The TLS standard requires that a client certificate only be sent if a client certificate request message has been sent earlier in the exchange. A client application may send a client certificate regardless of whether a request message was sent (i.e. the client may not comply with the TLS specification). The behaviour of a server on receiving an unexpected client certificate is not specified by the standard. It is not clear whether a server will process an unexpected certificate. (At least one vendor product has the options to refuse, allow or require client certificates – the standard presents the option to require.)

3.1.6 TLS supports and allows anonymous (or unauthenticated) connections. Where TLS is used the server is usually authenticated with the server certificate being passed from server to client.

3.1.7 The application testing undertaken has focussed on the use of client certificates and the possibility of a client sending a certificate containing an exceptional element to a server. The rationale for this is that the perceived impact of the denial-of-service or exploitation of a server is seen to be far greater than that of the impact on clients.

3.1.8 The use of exceptional elements of ASN.1 with server certificates has not been explicitly tested and is an area that may be the subject of further study.

3.2 Miscellaneous ASN.1 Fragments

3.2.1 While certificates may be the largest single block of ASN.1 used with TLS exchanges, a number of small ASN.1 fragments are used to hold cryptographic material, including:

a. RSA PKCS#1 Signature: contains a small-encrypted ASN.1 object. Although normally encountered as part of a certificate the ASN.1 object is not revealed until the signature is verified.

b. DSA Signatures: where a DSA signature is used then a small fragment of ASN.1 is used to specify the format of the two components of the DSA signature.

3.2.2 The use of exceptional elements of ASN.1 within these fragments has not been explicitly tested. This is an area that may be the subject of further study.

4. TLS TEST HARNESS

4.1 Scenario

4.1.1 The scenario under test is that a web-server has been configured to accept (or require) mutual authentication using certificates. The web-server may be intended for open access across public networks and there is a risk that a client may intentionally (or otherwise) submit a certificate containing an exceptional ASN.1 element during the TLS session.

4.1.2 The principle purpose of the testing of the web-servers was to demonstrate ASN.1 related vulnerabilities across a representative sample of web-servers.

4.2 Test Harness

4.2.1 Modifications were made to an existing TLS client capable of initiating mutually authenticated connections. The modifications allowed the client to function without breaking on the certificates under test. (The particular client used would normally parse the certificate as part of its own functionality.)

4.2.2 A reference certificate chain was created using the OpenSSL library and toolset. The reference chain consisted of a self-signed root certificate used to sign certificates for each web-server under test and the client certificates under test.

4.2.3 Failed tests were repeated using a second, disjoint, certificate chain to represent the submission of untrusted certificate paths.

4.2.4 The client, server and root certificates were all version 1 certificates. I.e. there were no certificate extensions present in the certificates under test. Examination of certificate extensions may be an area for further study.

4.2.5 All of the certificates contained RSA public keys based on a 1024 bit public key. RSAwithMD5 was used as the signature and hashing algorithm.

4.2.6 A large number of certificates, approximately 300,000, containing a variety of exceptional ASN.1 elements were created. Two different sets of certificates were created: one set contained exceptional elements and had a valid signature block, the other set contained exceptional elements where the validity of the signature block could not be guaranteed. (The certificate signature block is specified in ASN.1).

4.2.7 The suite of certificates does not include test cases containing exceptional ASN.1 elements within the encrypted component of the PKCS#1 RSA signature.

4.2.8 The modified client made requests to the web-server under test for a single web page submitting a different certificate for each separate request.

4.2.9 The web-servers tested included product ranges that account for 88% of SSL use, [Netcraft].

4.2.10 Each web-server was configured to require mutual authentication.

4.2.11 The web-servers were monitored for loss of service. The impact on a web-server's performance or response times were not monitored.

4.2.12 All of the web-servers under test were found to have difficulties handling particular ASN.1 elements containing exceptional elements.

5. CONCLUSIONS

5.1.1 Each TLS/SSL web-server tested has been found to have difficulties handling particular exceptional ASN.1 elements.

5.1.2 NISCC is currently working with system vendors to resolve these difficulties, with the intention of enabling the vendor provide patches for their systems.

5.1.3 It is likely that other TLS implementations may be susceptible to ASN.1 related vulnerabilities.