Null Prefix Attacks Against SSL/TLS Certificates

Moxie Marlinspike

07/29/09

Abstract

This paper presents some new tricks for performing undetected man-in-the-middle attacks against many common SSL/TLS implementations.

A Brief Reminder

The SSL and TLS protocols aim to provide secrecy, authenticity, and integrity – safeguarding communication from both passive and active adversaries. SSL and TLS rely heavily on the x509 certificate structure in order to deliver authenticity, and both parties in an SSL/TLS connection have the opportunity to identify themselves with an x509v3 certificate.

The original vision of the x509 standards committee was to create a certificate structure that would uniquely identify individuals within a global Directory Information Tree. While that ultimate never fully materialized, SSL/TLS does not need to pay much attention to the heirarchical context of an entity that is identifying itself anyway. For the SSL/TLS protocols, it is the "common name" field in the subject of an x509 certificate that is used to identify entities presenting certificates over SSL/TLS – particularly servers. Most of the other information in the Distinguished Name is simply ignored. PayPal will list www.paypal.com in the "common name" field, Ebay will list www.ebay.com, and Bank Of America will list www.bankofamerica.com.

The signing process for contemporary Certificate Authorities relies heavily on this convention. Entities submitting Certificate Signing Requests to Certificate Authorities are validated based on proof of ownership of the domain listed in the "common name" field. This can be as simple as looking up the technical or administrative contract in the WHOIS database for the root domain listed and sending them a confirmation email. What's important is that since identity information is only associated with the root domain, most Certificate Authorities completely ignore the content of any subdomains that might be present in the signature. Verisign, for instance, does not care whether you're submitting a request for www.ebay.com, verisign.eats.children.ebay.com,

or this.sub.domain.does.not.exist.ebay.com – so long as you can prove that you own ebay.com.

Useful Tricks

x509 certificates are formatted using ASN.1 notation. ASN.1 supports many different string types, but all of them are represented as some variation of PASCAL strings. In memory, PASCAL strings are represented by a series of bytes which specify the length of the string, followed by the string data itself – one character per byte. This is in contrast to C strings, which are represented in memory as a series of bytes – one character per byte – which are terminated by a single NULL character.

PASCAL String:

0x04 (Length)	0x44 ('D')	0x41 ('A')	0x54 ('T')	0x41 ('A')

C String:

0x44 ('D')	0x41 ('A')	0x54 ('T')	0x41 ('A')	0x00 (NULL)

One important effect of representing strings in PASCAL format is that NULL characters are treated just like any other character in your character string and are not embued with any special meaning. This means that we can freely include NULL characters in any of the fields within our x509 certificates, including the "common name" field.

One might issue a Certificate Signing Request like this:

www.paypal.com\0.thoughtcrime.org

As mentioned, the Certificate Authority will ignore the prefix, and only examine the root domain, thoughtcrime.org. If the person issuing the request is the legitimate owner of thoughtcrime.org (and presumably he would be), he would be able to prove his ownership of the domain to the Certificate Authority without any difficulty.

As it stands, most contemporary SSL/TLS implementations treat the fields obtained from x509 certificates as ordinary C strings, using ordinary C string functions for comparison and manipulation. As a consequence of this, a string comparison between www.paypal.com\0.thoughtcrime.org and www.paypal.com will identify the two strings as identical. The owner of the certificate for www.paypal.com\0thoughtcrime.org can thus successfully present this certificate for connections intended to www.paypal.com, effectively defeating the authenticity property of SSL/TLS and allowing for, among other things, undetectable man-in-the-middle attacks.

Universal Wildcard Certificates

While many SSL/TLS implementations fall victim to this, Mozilla's NSS is the worst. For NSS it is only necessary to shell out a little more money for a wildcard

certificate and get *\0.thoughtcrime.org. Because of an idiosyncrasy in the way that NSS matches wildcards, this will successfully match *any* domain. While other SSL/TLS implementations require a different certificate for every site an attacker would like to intercept communication for, NSS only requires that an attacker obtain this single certificate in order to intercept all traffic initiated by NSS applications (Firefox, Thunderbird, Evolution, Pidgin, AIM) to any server.

Deploying This Attack

The SSL/TLS man-in-the-middle attack tool, sslsniff[1], has been updated to support these modes of attack, along with related modes such as hijacking requests for automatic updates.

[1] http://www.thoughtcrime.org/software/sslsniff/