

Re: SSL & Man In the Middle Attack

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-01/0269.html>

From: JoshB (metrix007@yahoo.com)

Date: 01/15/03

From: metrix007@yahoo.com (JoshB)

Date: 14 Jan 2003 21:24:28 -0800

Anne & Lynn Wheeler <lynn@garlic.com> wrote in message news:<8yxpfewt.fsf@earthlink.net>...

> "NEWS.DFN.CIS" <anyone@nowhere.com> writes:

> > Hi, I'm a newbie

> >

> > I was wondering if SSL was still vulnerable to man in the middle attack?

> >

> > E.g., if some one is sitting between me and an trusted server, and

> > intercepts our handshake during initiation of our secure conversation, isn't

> > it possible for the middle man to intercept all messages from server to me

> > (but not from me to server)?

> >

> > server sends client a signed message along with a digital certificate.

> > the client validates the digital certificate (i.e. it is for the

> > server that i think i'm talking to) and then validates the signed

> > message using the public key in the digital certificate (i.e. the

> > server has to be the one described in the digital certificate or

> > otherwise the signed message wouldn't verify).

mitm couldnt fake a digital certificate? mitm could get a copy and

then send it back to client? or just sniff it and client gets it

anyway

>

> client generates a random secret key, encrypts it with the server's

> public key (from the certificate) and sends it to the server. from

> then on the server and client encrypt everything using the generated

> random secret key. only the server specified in the validated digital

> certificate will be able to decrypt the random secret key (since they

> should be the only one with the private key capable of decrypting

> something that had been encrypted with the corresponding public key).

> the client knows the random secret key because it generated it ... the

> server knows the random secret key because it was able to decrypt it

> with the server's private key.

mitm could not pretend to be client? client to mitm, mitm to server

> recent refs:

> <http://www.garlic.com/~lynn/2003.html#19> Message (authentication/integrity); was: Re: CRC-32 collision

comp.security.misc: Re: SSL & Man In the Middle Attack

- > <http://www.garlic.com/~lynn/2003.html#41> InfiniBand Group Sharply, Evenly Divided
- > <http://www.garlic.com/~lynn/2003.html#42> basic pki question
- >
- > there used to be an issue that a man-in-the-middle could play during
- > SSL setup negotiation ... where it would fake messages as to the
- > agreed upon secret key encryption protocol ... and force both the
- > client & server to select the weakest encryption protocol (with the
- > shortest key length). then once the secret key was exchanged ... the
- > man-in-the-middle was out of the loop ... other than attacking the
- > encrypted messages to determine the secret key (which it had forced to
- > the shortest possible).
- >
- > other attacks on SSL infrastructure ... as opposed to SSL protocol ...
- > is to get the client redirected to a different site by substituting a
- > different URL. The actual SSL check is does the URL in the certificate
- > match the URL that the client entered. If the attack can get the
- > client to enter the URL of the man-in-the-middle (i.e. a bogus URL)
- > ... who has a valid certificate for their site ... then the SSL
- > protocol works to the man-in-the-middle ... who then can fake a
- > client to the real web site.
- >
- > basically the SSL certificate protocol was to handle an ip-address
- > take-over in the domain name infrastructure ... aka man-in-the-middle
- > corrupted a DNS cache entry for a URL->IP-address mapping with the
- > wrong ip-address. The client typed in the correct URL ... but was sent
- > off to the wrong ip-address. The server at the fraudulent website
- > would be unable to establish a correct certificate for the original
- > URL.
- >
- > However, if the attack involved getting the client's browser somehow
- > to go to the wrong URL ... then the fraudulent website could have a
- > valid certificate for the fraudulent URL and everything proceeds.
- > Since frequently a client is just clicking on something ... rather
- > than actually typing in the actual URL ... there could be lots of
- > opportunities for incorrect URLs (even to trying to obtain domain
- > names for the common mistypings of URLs).
- >
- > the other is trying to spoof getting an issued certificate for the
- > desired URL (a recent case was an IE problem that accepted as valid,
- > certificates generated by individuals).
- >
- > misc refs:
- > <http://www.garlic.com/~lynn/subpubkey.html#sslcerts>