

Re: SSL certificate modification

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2002-10/3308.html>

From: Anne & Lynn Wheeler (lynn@garlic.com)

Date: 10/10/02

From: Anne & Lynn Wheeler <lynn@garlic.com>

Date: Thu, 10 Oct 2002 21:04:41 GMT

Henrick Hellström <henrick.hellstrm@telia.com> writes:

- > *That's only one reason for the existence of SSL server*
- > *certificates. The other reason, which IMHO is even more important, is*
- > *that certificates contains certified public keys which are used during*
- > *the SSL handshake and e.g. prevents man-in-the-middle attacks.*

see later in the (same) post regarding near real time serving of trusted public keys ... as opposed to stale,
<http://www.garlic.com/~lynn/2002m.html#64> SSL certificate modification

aka that the CA requirement for improving domain name infrastructure by having the domain name infrastructure register public keys at the same time they register the domain name:

1) improves the integrity of the domain name infrastructure so that the CAs can trust the information ... but if the CAs can trust the information ... then other people can trust the information ... by implication then the domain name infrastructure is a trusted server ... a catch-22 that eliminates the main reason for having SSL domain name certificates ... aka i've actually heard of real situations involving domain name take over and impersonation, i have yet to hear of a situation of real actual a significant mitm attacks.

2) if public keys are registered as part of #1 ... and also by #1 the domain name infrastructure is a trusted server ... then the existing domain name infrastructure can to trusted, near real time serving of public keys ... which is significantly better than the stale information paradigm implemented with certificates. as noted previously ... the domain name infrastructure is implemented to serve up general information ... not just ip-addresses.

not mentioned in the previous posting, that with the ability to obtain both the real trusted ip-address and the trusted public key in a single operation ... there can be a reduction in the SSL protocol handshaking chatter as part of setting up a session. The client as part of the original contact to the server ... include a SSL setup request piggybacked with the random session key (encrypted with the

comp.security.misc: Re: SSL certificate modification

the server's public key) and the acceptable symmetric algorithms. The
serve