

## Re: Is SSL/TSL really secure?

---

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.misc/2006-03/msg00176.html>

---

- *From:* Volker Birk <[bumens@xxxxxxxxxxxx](mailto:bumens@xxxxxxxxxxxx)>
  - *Date:* 28 Mar 2006 10:11:25 +0200
- 

tomodachigai@xxxxxxxxxx wrote:  
[SSL and TLS]

When you ping a ip, it connects to several other ips before it reaches its destination. So, isn't it possible for those "middle-man" computers to record the private and public keys as they pass from my computer to the "secure" web site.

It is not possible, because private keys never are being sent, and public keys are public anyways ;-)

sorry if the question is dumb, just hoped someone could clear it up for me.

What you seem to miss is the understanding of the idea of asymmetric cryptography.

It works like this:

You have a key pair K1, K2. What you're encrypting with K1 cannot be decrypted with K1 any more. It only can be decrypted with K2. And vice versa, what is encrypted with K2, can only be decrypted with K1.

So both partners have such a keypair, say Alice has K1, K2 and Bob has L1, L2.

Now Alice keeps K1 strictly secret – it's her "private key". And Bob does so with L1 – it's his "private" key. The other keys they make public.

Now Alice sends K2 to Bob. And Bob sends L2 to Alice. It does not matter if somebody listens.

When Alice now is wanting to send a message C to Bob, she encrypts the message with her own secret K1. So when Bob is decrypting, he knows, that this message came from Alice for sure, because this message can be decrypted with K2, Alice's public key. And additionally, Alice encrypts the message

## Re: Is SSL/TSL really secure?

with the public key of Bob, L2. So this message can only be decrypted by Bob himself – because he is the only one, who has the matching private key L1.

So Alice encrypts the message C like this:

$$X = L2(K1(C)).$$

Only Bob can decrypt it, because only he has L1 to decrypt:

$$X' = L1(L2(K1(C))) = K1(C).$$

And Bob immediately can check, if this really is from Alice. Only, if Alice's public key matches, then this will be a sensible message:

$$X'' = K2(K1(C)) = C.$$

This is the concept of asymmetric cryptography. SSL further uses the concept of cryptographic hashes to secure, that C really is a correct message. And, when key exchange using such concepts is done, then the only data which is sent usually is a key for a simple symmetric block cypher, which is used afterwards instead of such asymmetric cryptography. The reason is speed – this computes much faster.

Yours,

VB.

—

At first there was the word. And the word was Content-type: text/plain

.