

Re: SRP for online chat authentication?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-06/msg01444.html>

- *From:* daw@xxxxxxxxxxxxxxxxxxxxxxxxxxxx (David Wagner)
 - *Date:* Fri, 30 Jun 2006 05:22:06 +0000 (UTC)
-

Paul Rubin wrote:

Alice and Bob, mutual strangers, meet in an online, plaintext chat room. They discover that they are both Lord of the Rings fans, so they want to talk privately about how to defeat Sauron. Sauron of course runs an automated system ("The Lidless Eye") that monitors all internet traffic and can carry out MITM attacks against known protocols that are susceptible to MITM, but being automated with current technology, it doesn't understand natural language to any extent.

[..]

Anyway, the idea is to use SRP to set up an encrypted channel authenticated by a password. SRP if I understand correctly is basically DH key exchange authenticated by a zero-knowledge protocol based on the password. So Alice says to Bob in plaintext, e.g.:

"Let's use the name of Gandalf's horse as a password".

Bob knows right away that the password is "Shadowfax". [...] Alice and Bob now arbitrarily decide that Alice will be the server and Bob will be the client. They start an SRP session authenticated by the password "Shadowfax" and begin chatting.

This is a very nifty idea. I think there's a man-in-the-middle attack here, but I think the idea can be patched up pretty easily.

Assume that Sauron compiles in advance a pre-determined dictionary of plaintext descriptions of a password ("the name of Gandalf's horse") along with the corresponding passwords ("Shadowfax"). This dictionary does not have to be exhaustive; Sauron just needs one plausible entry for every possible talk topic.

So Alice and Bob meet in an online chat room and discover they are both LOTR fans. Suppose Sauron's software determines that Alice and Bob are talking about LOTR. (It seems quite plausible to extract what topic they are discussing in a purely automated fashion, through standard natural

Re: SRP for online chat authentication?

language processing and data mining methods.) Next Sauron looks up that topic in his dictionary and picks any LOTR-related password from the dictionary. Now Sauron has everything he needs to mount a MITM attack.

The MITM attack goes like this. Sauron sends a spoofed message to Bob, that looks like it came from Alice (but actually came from Sauron), sending the English description of the password Sauron chose. (The English description came from the pre-determined dictionary, so can be computed automatically.) Because Sauron knows the corresponding password, Sauron can successfully set up a SRP session with Bob. Bob will end up with a SRP session where he thinks he is talking to Alice, but where he is actually talking to Sauron. Sauron can do the same to Alice, so that she thinks she is talking via SRP to Bob, but she is actually talking to Sauron. Sauron can shuttle Alice's messages to Bob, and vice versa, so that Alice and Bob hold a conversation that they think is private but actually is being observed by Sauron.

I think you can get around this if you require two passwords. Alice picks a password P_A and sends an English description of her password in the clear to Bob. Independently, Bob picks a password P_B and sends an English description of her password in the clear to Alice. Then, Alice and Bob use the concatenation $P_A \parallel P_B$ as the SRP-password and create a SRP channel between them. It looks to me like this will defend against automated attacks, even active attacks, and thereby meet your goals.

All of this assumes that Alice and Bob won't ever be fooled by an Eliza-style bot.

.