

SRP for online chat authentication?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-06/msg01442.html>

- *From:* Paul Rubin <<http://pbr.cx@xxxxxxxxxxxxxxxx>>
 - *Date:* Fri, 30 Jun 2006 05:06:36 GMT
-

This is a pretty obvious SRP application, but I thought I'd ask if I'm missing something boneheaded. The goal is to allow secure online chat between strangers without needing PKI.

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". The Lidless Eye doesn't understand this itself, but it naturally records the conversation for later review by Sauron's live minions ("orcs").

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.

A minute later, one of Sauron's orcs reads the transcript of the plaintext portion of Alice and Bob's conversation. The orc also immediately guesses the password, but by then it's too late; Alice and Bob already have a secure session with forward secrecy. The orc cannot use the password to break into or decrypt the session. The password would only have been useful before the session started.

Alice and Bob can, of course, now use their secure session record a permanent shared secret, or exchange public keys, to authenticate future sessions without the SRP trick. SRP has amplified "obscurity" (mutual knowledge of LOTR trivia) into something closer to security.

SRP for online chat authentication?

The password is used only once and by the time it's compromised, it's no longer useful to the attacker.

This even (somewhat) works if an orc is monitoring the plaintext conversation in real time and can tamper with it. If the orc is not a Tolkien buff, it will take him/her a minute or so to discover the answer, and by then Alice and Bob's session is already under way. Alternatively, the orc can interrupt the connection while looking up the answer, but that introduces a suspicious delay (or connection failure), and Alice and Bob know they should try again if that happens.

The most obvious failure is if Alice is herself an orc trying to trap Bob, or vice versa. There's also the amusing case where Alice and Bob are both orcs, each unwittingly trying to trap the other. Cryptography can't help with either of these cases so we don't try to address them here.

Any thoughts?

.