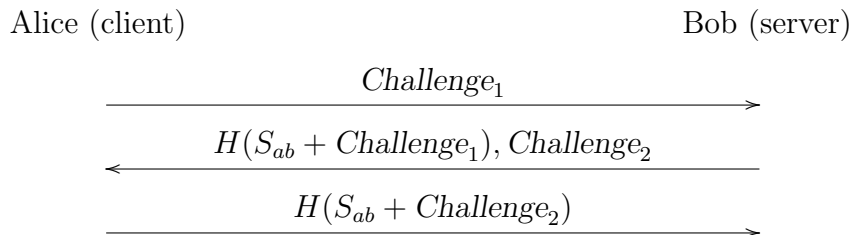


## Homework #2

Due: Tuesday, December 2nd, 2008, 3:30 PM.

**Problem 1** Consider the following simple variant of the mutual-authentication protocol Eric Rescorla presented in class, in which a client connects to a server and each verifies that the other knows the shared secret  $S_{ab}$ :



Here a client might be a user with a Web browser and a server might be a Web server accepting connections over the Internet. The client initiates connections; the server accepts connections.

Compared to the protocol presented in class, the protocol here has the client send the first challenge; it also doesn't tie the two challenges to each other. These appear to be innocuous changes, but in fact the modified protocol is *insecure*: Veronica, a malicious client, can convince the server Bob that she is Alice even though she doesn't know the secret  $S_{ab}$ .

Explain the security problem in the modified protocol. What exactly makes the original protocol immune to it?

*Hint*: Your attack will make use of more than one protocol interaction.

Suggest one way to fix the modified protocol without changing the number or direction of the message flows.

(The subtlety of such flaws is one reason that it is unwise to attempt to design new cryptographic protocols.)

**Problem 2** The Internet is, slowly, transitioning from the version of the TCP/IP protocol suite currently in use—IPv4—to a new version, IPv6.

Unlike IPv4 IP addresses, which are 32 bits long (e.g., 192.168.10.1), IPv6 IP addresses are 128 bits long (e.g., 2001:1890:1112:0001:0000:0000:0000:0020).

- (a) Consider random-scanning Internet worms. These worms spread by choosing a random IP address, connecting to any host answering to that address, and attempting to infect it.

Is the random-scanning strategy feasible if the Internet switches from IPv4 to IPv6? Why or why not?

*Hint:* Consider the density of Internet-connected machines in the IP address space.

- (b) On the IPv6 Internet, what are some specific ways that a worm, executing on a compromised computer, can discover IP addresses of other hosts to try to infect?

*Hint:* Consider sources of IP address on the infected computer itself and on the local-area network to which it is connected.

- (c) Suppose the worm targets Web servers running some application (say, bulletin board software written in PHP). Can Google searches help the worm find potential targets? How?

**Problem 3** As we discussed in class, e-mail is transmitted from sender to recipient by means of the SMTP protocol. Each domain advertises an SMTP server that receives incoming mail using MX records in the DNS. For example, GMail's incoming SMTP server is `gmail-smtp-in.1.google.com` (which is actually an array of machines load-balanced through DNS A-record resolution).

Users' desktop computers are not usually configured to connect directly to the recipient's incoming SMTP server. Instead, they relay all mail through an outgoing SMTP server for their domain, which itself handles the mail delivery. For example, outgoing mail from CSE department computers is handled by `cse-smtp.ucsd.edu`.

Now, consider a computer in the CSE department that has been compromised as part of a botnet and is being used by the botnet owners to send spam to users at various sites, such as GMail.

- (a) Suppose the bot software installed on the computer uses the outgoing SMTP server configured on the computer (`cse-smtp.ucsd.edu`) to send the spam. How can the CSE department network administrators best block the outgoing spam? (What is the anomalous behavior? What system detects it? What action does that system undertake to block the spam?)
- (b) Suppose instead that the bot software bypasses the outgoing SMTP server, and connects directly to the incoming SMTP servers for each domain to which spam is sent. (That is, the bot software installed on the compromised machine acts as its own outgoing SMTP server.) How can the CSE department network administrators best block the outgoing spam in this case? (What is the anomalous behavior? What system detects it? What action does that system undertake to block the spam?)