Homework 3 Solutions

Sam Mergendahl

Feb 2, 2020

1. Textbook, Chapter 6 Exercises, Problem 15

   - You could set aside some bits reserved to provide an authentication header. The authentication header part of the address could refer to both authentication (ie assuring that the IP packet did indeed come from that IP address) and data integrity (ie assuring that the contents have not been modified along the path from the source node to the destination node). Similarly, extra bits can be used to specify the encryption algorithms and key lengths that this IP address supports. If your answer disagrees with the use of the IP bits for security, I will give full credits as well as long as the answer makes sense.

2. Textbook, Chapter 6 Exercises, Problem 16

   - They could try and replace the address translation in the table to a malicious IP address that the attacker controls, so that when a user attempts to visit yourdomain.com, they are taken to a different address than they are expecting.

3. Textbook, Chapter 6 Exercises, Problem 25

   - One way to determine if the denial of service is an attack or lack of capacity is to see if the behavior of the traffic is benign or random. If the traffic is doing something abnormal such as sending TCP SYN over and over again, it can be considered attack rather than a "flash-crowd" of benign users that caused a lack of capacity.

4. Textbook, Chapter 6 Exercises, Problem 27

   - One could look at the diversity of addresses outside the local network a particular host is sending traffic to. Many worms are self-propagating (i.e., they try to infect other hosts as well), so they need to preform large scans over the entire IP address range. You could also look to see if the host in the local network has begun to change its behavior (i.e., a change to higher traffic spikes out of the local network or constant traffic out of the network). The best defense is to know what type of behavior belongs in your network and flag any other suspicious behavior.

5. Textbook, Chapter 6 Exercises, Problem 37

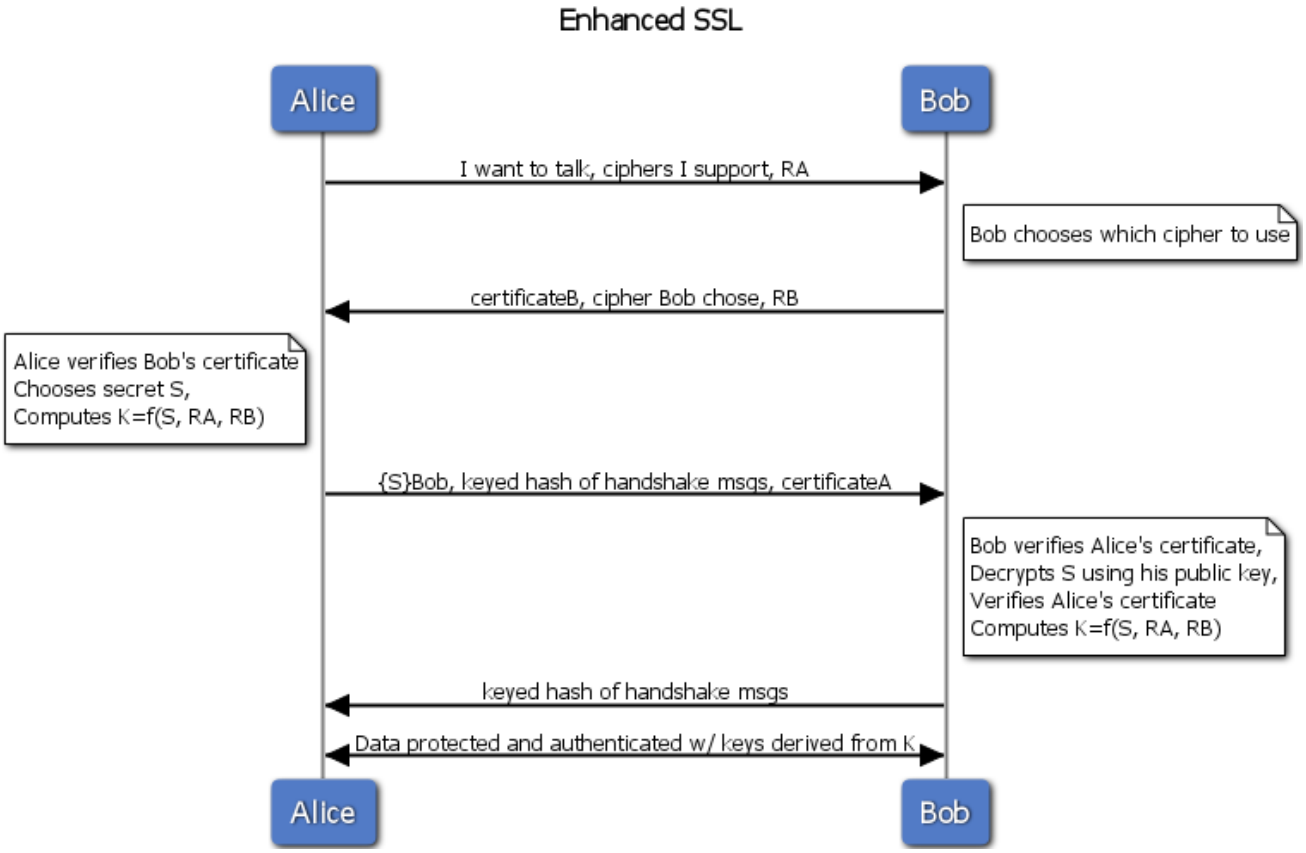
   - The sequence number can help prevent against replay attacks (i.e., prevent old messages from being resent to the receiver at a time that the receiver is expecting a similar packet, thus making the receiver think the protocol has been successfully completed). Similarly, it can identify any unexpected additions or deletions in a string of messages.

6. Textbook, Chapter 6 Exercises, Problem 41

   - It could look for known worm signatures to see if its network is infected with any known worms. It could also preform ingress filtering (ie if it's an edge network and there are source IP addresses in packet headers that are not actually from the IP range the network offers, one can assume that they are spoofed packets and the firewall could not forward them).

7. In the SSL protocol we discussed in class, Bob presents his certificate to Alice, but Alice does not present her certificate to Bob. Enhance the SSL protocol so that Alice presents her certificate to Bob as well. Draw the new diagram to illustrate how the enhanced SSL works, and explain what this enhancement achieves.

   - Bob sends Alice his certificate so that when she sends Bob confidential information she only wants Bob to know, she knows for a fact that she is sending it to Bob. If Bob ever needed to send confidential information to Alice without starting a new SSL session (e.g., Alice preforms a look up on her own information) Alice would also need to send Bob a certificate.



8. Worm detection can be either signature-based or behavior-based. List three reasons/scenarios when behavior-based worm detection is preferred.

    - Zero-day worms: worms continuously exploit new vulnerabilities, so the signature may not be up to date.
    - Polymorphic Worms: a worm can have almost arbitrary payloads, and it is infeasible to have signatures for every possibility.
    - Heavy workload processing: signature based worm detection requires deep packet inspection of traffic which is often too slow and computationally expensive.

9. Explain how B, C, and X will verify the integrity of the update.

    - If the signature provided by a node is that node's private key applied to the message it is sending, upon receiving a message, one can apply the previous node's public key to the signature to see if the result equals the message data sent. If it doesn't, then one of two things occurred. Either the key applied to create the signature was not the right key (failure to authenticate the previous node), or the message was tampered with along the way (failure of integrity). Either way, the recipient does not want to trust the received message and should ignore it. Each node can process each signature in this manner.

10. Discuss how you would protect a DNS client from receiving a spoofed DNS response from a malicious attacker, instead of the authentic response from the legitimate DNS server.

    - Similar to the previous question, the DNS server could provide a signed certificate from the authoritative server, so the recipient could make sure the DNS response is trustworthy. In fact, the user could use DNS over TLS (DoT) or DNS over HTTPS (DoH), two current community efforts.