Test 3

Submission deadline: May 13, 2005 at 4:00pm

Note: Online submissions are encouraged. MSWord or pdf documents are preferred. You may also bring your answers to my office. Use the following command to submit your answers online:

submit wang 561test3 [your file]

This test is take home. It must be an individual work. You may, however, consult your textbook and notes. Any other form of getting help, such as consulting other textbooks or web sites, is a violation of the honor code. Providing information to others that leads to solutions is also a violation of the honor code.

Show your work and justify all your answers. Please do not write things down that are irrelevant. You will be graded not only on the correctness of your answer, but also on the clarity you express it.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Points</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

I have abided by the Academic Honor Code on this test.

Name: ______________________ Signature: ______________________ Date: ______________________
1. (20 points) The following steps are multiple-realm Kerberos exchanges. Please provide details for each item involved and explain what each item is used for. For convenience, we use comma “,” to denote concatenation.

(1) C → AS: \( ID_c, ID_{tgs}, TS_1 \)
(2) AS → C: \( E_{K_c}[K_{c,tgs}, ID_{tgs}, TS_2, LT_2, Ticket_{tgs}] \)
(3) C → TGS: \( ID_{tgsrem}, Ticket_{tgs}, Authenticator_{c,tgs} \)
(4) TGS → C: \( E_{K_c,tgs}[K_{c,tgsrem}, ID_{tgsrem}, TS_4, Ticket_{tgsrem}] \)
(5) C → TGSrem: \( ID_{vrem}, Ticket_{tgsrem}, Authenticator_{c,rem} \)
(6) TGSrem → C: \( E_{c,tgsrem}[K_{c,vrem}, ID_{vrem}, TS_6, Ticket_{vrem}] \)
(7) C → V_{vrem}: Ticket_{vrem}, Authenticator_{c,vrem}

2. The first 16 bits of the message digest in a PCP signature are transmitted in the clear.

(a) (10 points) To what extent does this compromise the security of the hash algorithm?

(b) (10 points) To what extent does it in fact perform its intended function, namely, to help determine if the correct RSA key was used to decrypt the digest?

3. Suppose that hosts A and B have IP addresses 1.1.1.1 and 3.3.3.2, respectively, where A is connected to a gateway/router RA and B is connected to a gateway/router RB. Suppose the IP addresses of RA’s two faces are 1.1.1.2 and 2.2.2.3, and the IP addresses of RB’s two faces are 2.3.2.8 and 3.3.3.1.

(a) (10 points) Describe how an IPsec packet from A to B is formed with the following requirements:

- A needs to authenticate its packet to RB.
- RA needs to encrypt the packet to form a tunnel between RA and RB.

In your description, you much specify source address and destination address in each IP header in the packet.

(b) (10 points) How many SAs are needed in (a)? Describe how these SAs could be formed dynamically?

4. (a) (10 points) In SSL, why is there a separate Change Cipher Spec Protocol, rather than including a change_cipher_spec message in the Handshake Protocol?

(b) (10 points) It was stated that the inclusion of the salt in the UNIX password scheme increases the difficulty of guessing by a factor of 4096. But the salt is stored in plaintext in the same entry as the corresponding ciphertext password. Therefore, those two characters are known to the attacker and need not be guessed. Why is it asserted that the salt increases security?

5. (20 points) The question arises as to whether it is possible to develop a program that can analyze a piece of software to determine if it is a virus. Suppose that we have
a program D that is able to this; that is, for any program P, if we run D(P), the result returned is TRUE (P is a virus) or FALSE (P is not a virus). Now consider the following program:

Program CV :=
{ ... 
    main-program := 
        {if D(CV) then goto next:
            else infect-executable;
        }
    next:
}

In this program, infect-executable is a module that scans memory for executable programs and replicates itself in those programs. Determine if D can correctly decide whether CV is a virus.