Test 3

Submission deadline: May 15 at 4:00pm online

Note: Only online submissions are accepted unless you hand in your test to Olsen 201 by May 14 (Friday) before 3:30pm. MSWord or pdf documents are preferred. But you may also scan your answers and submit them. Use the following command:

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>30</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100</strong></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) \( C \rightarrow AS:\) \( ID_c, ID_{tgs}, TS_1 \)
   (2) \( AS \rightarrow C:\) \( E_{K_c}[K_{c,tgs}, ID_{tgs}, TS_2, LT_2, Ticket_{tgs}] \)
   (3) \( C \rightarrow TGS:\) \( ID_{tgsrem}, Ticket_{tgs}, Authenticator_{c,tgs} \)
   (4) \( TGS \rightarrow C:\) \( E_{K_c,tgs}[K_{c,tgsrem}, ID_{tgsrem}, TS_4, Ticket_{tgsrem}] \)
   (5) \( C \rightarrow TGS_{rem}:\) \( ID_{vrem}, Ticket_{tgsrem}, Authenticator_{c,vrem} \)
   (6) \( TGS_{rem} \rightarrow C:\) \( E_{c,tgsrem}[K_{c,vrem}, ID_{vrem}, TS_6, Ticket_{vrem}] \)
   (7) \( C \rightarrow V_{vrem}:\) \( Ticket_{vrem}, Authenticator_{c,vrem} \)

2. (20 points) Phil Zimmermann chose IDEA, three-key triple DES, and CAST-128 as symmetric encryption algorithms for PGP. AES was not invented at that time. Give reasons why each of the following symmetric encryption algorithms is suitable or unsuitable for PGP: AES, two-key triple DES, Blowfish, and RC5.

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) (20 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. (10 points) Suppose in Problem 3 there is another router RC between RA and RB. Consider the following IPsec packet:

   \[
   \text{IP Header 1} | \text{AH} | \text{IP Header 2} | \text{ESP} | \text{IP Header 3} | \text{Data}
   \]

   where IP header 1 contains RC as source and B as destination, IP Header 2 contains RA as source and RB as destination, and IP Header 3 contains A as source and B as destination. Is this a valid IPsec packet? Justify your answer.

5. (20 points) Which of the ISAKMP Exchange Types corresponds to the aggressive Oakley key exchange? For the Oakley aggressive key exchange, indicate which parameters in each message go in which ISAKMP payload types.