RFID INFOSEC Project #1, ver. 2.0  
Threat Modeling of an RFID-enabled Credit Card  
Assigned Oct. 1 and Due Oct. 15, 2008

70 pts.

Show all your work. Without proper justification and details of steps, correct answers alone may not carry full credit.

Notes:
- Minus 3 points if your homework is not stapled in the upper left-hand corner.
- Minus 2 points if you use the back of your paper. Please only use a single side.
- Minus 2 points if you present the worked problems out of order. In other words, please present the problems in the order assigned, 1, 2, 3, ...

Perform threat modeling on the described system.

Assume you want to release an RFID-enabled credit card. The card will use the ISO/IEC 14443 standard, which operates at 13.56 MHz, has a maximum legal read range of 4 inches, and can perform 3DES. Readers will be placed at different restaurants and gas stations. To use the credit card, the user will bring the credit card close to the reader. Purchases under $50 will not require a PIN number. Purchases over $50 will require the user to enter a PIN number on the reader.

Deadline #1: Oct. 8. Team representative should notify instructor that they will represent the team via email (drt@uark.edu).

Deadline #2: Oct. 10. Team representative should turn in items 1 and 2a, 2c, 2d to the instructor via email.

Deadline #3: Oct. 15. Team representative should turn in complete documentation (Items 1 through 6) of the threat modeling of the system to the instructor via email.

1. Assemble Team. Refer to the class website for the list of teams. After determining what team you are on, gather contact information such as phone number and email. After the team meets, elect a team representative. (5 pts.)

Team representative: ___________________________________________________________.

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2. Decompose the system
   a. High-level context diagram(s) (5 pts.)
   b. Next-level context diagram (More detail than high-level). (5 pts.)
   c. High-level physical view (5 pts.)
   d. List components (5 pts)

3. Determine the threats to the system
   a. Apply STRIDE (10 pts.)
   b. Create two threat trees for two threat targets (5 pts each for a total of 10 pts.)

4. Determine risk for each threat tree
   a. Apply DREAD (10 pts.)

5. Rank threats by decreasing risk (5 pts.)

6. Mitigation
   a. Assume you must respond to the threat with the highest risk
   b. Choose technique(s) to mitigate threat with the highest risk (5 pts.)
   c. Choose appropriate technologies (5 pts.)