Rubric
for
Homework #1

- Each problem worth 5 points
- Total minus points for a problem is along left side of page

Answers not labeled clearly: -1 overall (e.g. Problem 1 – R-1.12)
Low Readability: up to -3 per question
Lack of Clarity: up to -3 per question
Missed/wrong ideas or facts: -1 per idea/fact
Answer too long: up to -2 per question

If minus points not labeled, they are for missing ideas/facts.

Problem R-1.12

<table>
<thead>
<tr>
<th>Symmetric encryption</th>
<th>Public-key encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>- one secret shared key between each two users (requires many keys for many users)</td>
<td>-1 private key, 1 public key per user (only two keys per user)</td>
</tr>
<tr>
<td>- one key used for both encrypt/decrypt</td>
<td>- two keys used for encrypt/decrypt</td>
</tr>
<tr>
<td>- faster</td>
<td>- slower</td>
</tr>
<tr>
<td>- have to securely provide the key to both users</td>
<td>- don’t have to explicitly share secret keys</td>
</tr>
<tr>
<td>- keys are shorter</td>
<td>- requires larger keys</td>
</tr>
</tbody>
</table>

Problem R-1.13

- List three reasonable things using at least some wording from chapter (e.g. confidentiality, masquerading, etc.)

Problem R-1.20

Attack: eavesdropping, alteration
Concepts of computer security: confidentiality, integrity, assurance(?)

Problem R-1.21

- Security concern: weak password, is the signal from car encrypted?
- privacy concerns: owner can know where driver went

Problem R-1.22
Good Security: encryption/confidentiality,
Bad security: short key (makes brute force plausible), no apparent access control or authentication to get the picture file, no checksums or data correcting codes

Problem R-1.23

Attack: masquerading, pretexting

Low level of security, why?

Problem C-1.9

625 (5 x 5 x 5 x 5)

Problem C-1.9

Assuming that Barack doesn't ask twice for one bank, each communication from Barak to Tim will be unique. So 10 request messages for 10 banks. Could himself use $P_T$ on the 10 known unencrypted messages that are possible in order to see the 10 possible encrypted transmissions.

The sum of the response messages should be $900$ billion. So that means that no single amount can be greater than $900$ billion. Could himself use $P_B$ on 900 different unencrypted possibilities in order to see the 900 different possible encrypted transmissions.

Problem C-1.12

Barack can encrypt the messages with his private key while Hilary decrypts them with his public key.

Problem C-1.18

Phishing is usually clicking on a link in an email that purports to link to a website but actually is another website. The actually linked-to website is usually made to look like the site that users are familiar with.

False security could come from the fact that the computer is linking to the false website and simply using the digital certificate to verify that the user is at the false website!