No class on Wednesday (holiday)
- HW 2 due tonight (11:59 pm)

Kerberos: schemes for securing

Nonces

\[ N_B \leftarrow \{ [N_B, m] \} \]

A \rightarrow B

Timestamps

\[ A \rightarrow \{ [t, m] \} \]

A \rightarrow B

Sequence numbers

\[ A \rightarrow \{ [s, m] \} \]

A \rightarrow B

<table>
<thead>
<tr>
<th></th>
<th>Nonces</th>
<th>Timestamps</th>
<th>Sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replay</td>
<td>√</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>Reflection</td>
<td>√</td>
<td>maybe</td>
<td>×</td>
</tr>
<tr>
<td>Deletion/Drop</td>
<td>√</td>
<td>X</td>
<td>√</td>
</tr>
<tr>
<td>Dos</td>
<td>×</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Traffic Analysis</td>
<td>×</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Traffic Analysis
Diagram of Kerberos conversation

1. $A, B, t, Na$

2. $\{[T_{a,b}]\}_{k_A}$
   $\{[T_{a,b}]\}_{k_B}$

3. $\{[A, B, t]\}_{k_{A,B}}$

4. $\{[A, B, t+1]\}_{k_{A,B}}$

$T_{a,b} = (A, B, k_{A,B}, t, t_{exp}, Na, ipaddr_i)$

Note about notation used:

1. "I Alice want a session key for use with Bob. It's now time $t$ and here's a challenge $Na$".

Pros:
- very concise and precise notation
- can be used in academic papers

Cons:
- could mean something completely different
- two messages that could normally never collide could collide under condensed notation
  (this could enable attack)
• From a security point of view, the Kerberos authentication server represents a huge security risk, since it stores everybody's password.

• This system is subject to an offline brute force attack (i.e., attacker sniffing an encrypted packet).

Weaknesses in Kerberos:

- Didn't use message authentication code to authenticate each message. A checksum is used, but this is not cryptographically secure.

- Random number generator is seeded with srand (time(0)) — the seed has a granularity of seconds, so it is easily guessable.

- System could benefit from public key.

- Could use SSL to establish encrypted channel.

Strengths of Kerberos:

- Removing users (for example, if someone gets fired) is simple.