Class Note: May 3, 2007

Sony DRM (Cont.)

Music Makers | DRM Makers | Users
---|---|---
-efficacy | -large install base | -security
-acceptability | -efficacy | -reliability
-have much to lose | -extracting other value | -privacy
 → conservative | -have little to lose | -control

To stop DRM from running in your PC:
1. Disable autorun
2. Hold down SHIFT when inserting CD
3. Use magic marker trick

Economics & Security

<table>
<thead>
<tr>
<th>In US</th>
<th>In UK</th>
</tr>
</thead>
</table>
Burdens of proof in ATM dispute: | Bank | Customers |
Result: | -Banks secured ATM | -Banks believed ATMs secured |
| -Little fraud | -A lot of fraud |
| -Total loss to security | -Insider fraud |
| Was less |

Egress Filtering: discard outbound packets w/ impossible source address.

However, ISP don’t benefit from this, so they usually don’t do much about it.
### Security Software:

<table>
<thead>
<tr>
<th></th>
<th>Attacker</th>
<th>Defender</th>
</tr>
</thead>
<tbody>
<tr>
<td>Goals:</td>
<td>- find 1 unpatched security bug</td>
<td>- find &amp; fix all bugs</td>
</tr>
<tr>
<td>Resources</td>
<td>- 1 person</td>
<td>- 1000 people</td>
</tr>
<tr>
<td>Total bugs:</td>
<td></td>
<td>1 million</td>
</tr>
<tr>
<td>Found:</td>
<td>- 1</td>
<td>1000</td>
</tr>
<tr>
<td>Odd of Success:</td>
<td>99.9%</td>
<td>0.1%</td>
</tr>
</tbody>
</table>

#### Ways to find defenders
1. Automated bug fixing
2. Type safe language
3. Small TCB
4. Bug finding tools

#### CAPTCHAs:
- computer goal: computer cannot break
- usability:
  - blind
  - deaf
  - foreign
  - kids?
  - healthy natives

**Idea:**
Show six images, where one is totally different from other 5. Ask the user to tell which one is odd.

#### Major themes in System Security
- Understand goals and threat model
- Design the system for security
- Implement for security
  - automate where possible