TPM Sealed Storage

Seal(PCR, X)
   C = Enc_{Stpm}(x)
   T = Sig_{Stpm}(PCR, C)
   Return( C, PCR, t)
UnSeal( C, PCR', t)
   If ! Vrfy_{Stpm}((PCR',C),t)
      Return error
   If PCR != pcr'
      Return error
   Return Dec_{Stpm}(C)

TPM

<table>
<thead>
<tr>
<th>PCR</th>
<th>Sis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stpm</td>
<td>Encrypt/Decrypt</td>
</tr>
<tr>
<td>Ptpm</td>
<td></td>
</tr>
<tr>
<td>S'tpm</td>
<td></td>
</tr>
<tr>
<td>Ctpm</td>
<td></td>
</tr>
</tbody>
</table>

*** S = secret key // P = public key // mps = movie player service // p1f = play 1 frame

Secure Movie Player Example:

Client
- P m.p.s
- Play Setup
- A = Seal(PCR p1f, k)
- B = Enc Pmps(k)
- Enc (Frame)
- Play 1 Frame

Movie Player Service
- K = Dec S mps (B)
- Enc_k (Frame)

H(17 || Play1Frame) (***Now only the p1f and the movie player service can both get access to k.)
Security Usability

- Phishing
- Site key
- Conditioned Safe Ceremonies
- Phorcefield
- PwdManagers
- Device Pairing
- Security Skins

Security Indicators:

- Lock – spoofable // ignored
- Green Location bar - Spoofable // ignored
- Site Key = Image and word(not the password) mapping stored on your computer(client) in cookies. User should check to make sure that the right image and word are displayed before typing in there password.
Secure Machine Registration:

Client          Server

Username, Secret Question

Set cookie, Image, Text

If cookie is already set: Login.html

Display Image txt password

Condition - Safe Ceremonies:

Client          Bank

Register Me

Email Link

Retrieve Email

GET link

Set Cookie

......Login .........