Remote Attestation
- Sealed Storage
- Flicker

Consider: Bad guy wants to roll back the database.
How to prevent this?
- add some notion of ‘time’
- TPM is going to have ‘counter’
Whenever sealing \( SS_T \), TPM increases counter ‘\( ctr \)’, and puts the value of \( ctr \) into \( E \).
\[ E (P_{ss}, h_t || | K_t) \]
• **Flicker**: an infrastructure for executing security-sensitive code in complete isolation. Flicker does not require a new OS or even a VMM.

```
<table>
<thead>
<tr>
<th>App</th>
<th>App</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>PAL</td>
<td></td>
</tr>
<tr>
<td>TPM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

* PAL: Piece of Application Logic

• **SKINIT**: allows a regular system to boot and later on switch to trusted code.

```
SKINIT (p, n)
h = H(p[0] \ldots p[n - 1])
jmp p
```

* disables interrupts
* disables DMA access to P
* disables debugging

```
Input Space
SS_{SSL}  | Encrypted Data
Output Space
Decrypted Data
saved information
SSL_Decrypt
PAL
: completely self-contained
```

• **To enter PAL:**
  1. Copy inputs to PAL
  1.5. Zero output area
  2. Save return state to saved info
     - registers
     - base table pointers
     - other basic state
  3. SKINIT (PAL, n)
     h = H (PAL, n);

• **To exit PAL:**
  1. Write output to output area
  2. EXTEND (output area)
  3. EXTEND (000...0): indicates the end of PAL
  4. Restore OS state from saved area
     (saved information)

* Extend Operation
```
EXTEND (p, n)
h = H (h | | p[0], \ldots, p[n - 1])
```