Lecture 10: Hardware-based Security
Trusted Platform Module (TPM)
What’s in a TPM?

- Non-Volatile Memory
- Volatile Memory
- Execution Engine
- RNG
- Key Generation
- Crypto Engines
- Authorization
- Non-Volatile Memory

I/O

Trusted Platform Module (TPM)

Tamper-Resistant Packaging
What’s in a TPM?

- Key Generation
- RNG
- Execution Engine
- Volatile Memory

I/O

Crypto Engines
Authorization
Non-Volatile Memory

Trusted Platform Module (TPM)

Tamper-Resistant Packaging
Volatile Memory

- PCR Banks
- In-use keys
- Sessions
- Etc.
Platform Configuration Register (PCR)

- Contain hashes of programs
- Attestation: TPM2_Quote()
- Modified by TPM2_Extend():
  \[ PCR_{new} = H(PCR_{old} \parallel data_{new}) \]
Non-Volatile Memory

- Platform Seed
- Endorsement Seed
- Storage Seed
- Monotonic Counters
- Etc.
Seeds used for attestation, etc

- Endorsement seed used to derive endorsement keys (EKS)
- Manufacturer attests validity of EKs
- EKs used to attest other TPM-derived values including
  - other keys: TPM2_Certify()
  - audit logs: TPM2_GetSessionAuditDigest()
Binding and Sealing
Bitlocker

Enter the password to unlock this drive

Press the Insert key to see the password as you type.
ARM TrustZone

Diagram showing the separation of non-trusted and trusted domains, including compartments for software, data, and hardware, with a debug interface.
Android Full Disk Encryption
Android Full Disk Encryption
Enclaves

- Isolated computing environments
- Access hardware-derived keys
- Provide attestation
Isolation
Attestation
SGX in use
Vulnerabilities

Trustworthiness of Trusted Code

Side Channels

**Algorithm 1** Fixed-window exponentiation

**Input:** $a, e, N \in \mathbb{N}$

**Output:** $x \leftarrow a^e \mod N$

1. Precompute $g[i] \leftarrow a^i$ for $1 \leq i \leq 2^k$
2. Let $e = (e_j, e_{j-1}, \ldots, e_1, e_0)$ be the base $2^k$ representation of the exponent $e$ with $e_j \neq 0$
3. Initialize $x \leftarrow e_j$
4. for $i \leftarrow j - 1$ down to 0 do
5. \hspace{1em} $x \leftarrow x^{2^k} \mod N$
6. \hspace{1em} if $e_i \neq 0$ then
7. \hspace{2em} $x \leftarrow g[e_i] \cdot x \mod N$
8. \hspace{1em} end if
9. end for
## Comparison of Hardware Solutions

<table>
<thead>
<tr>
<th>Adversary</th>
<th>Attack</th>
<th>TPM</th>
<th>TrustZone</th>
<th>SGX</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>direct probing</td>
<td>n/a (OS measured)</td>
<td>access checks on TLB misses</td>
<td>Access checks on TLB misses</td>
</tr>
<tr>
<td>OS</td>
<td>page faults</td>
<td>n/a (OS measured)</td>
<td>secure page tables</td>
<td>X</td>
</tr>
<tr>
<td>OS</td>
<td>cache timing</td>
<td>n/a (OS measured)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Another container</td>
<td>direct probing</td>
<td>n/a</td>
<td>n/a (secure world trusted)</td>
<td>access checks on TLB misses</td>
</tr>
<tr>
<td>Another container</td>
<td>cache timing</td>
<td>n/a</td>
<td>n/a (secure world trusted)</td>
<td>X</td>
</tr>
<tr>
<td>PeriTpheral</td>
<td>DMA</td>
<td>X</td>
<td>bus bounces accesses</td>
<td>IOMMU bounces DMA</td>
</tr>
<tr>
<td>Physical attacker</td>
<td>Physical DRAM</td>
<td>X</td>
<td>n/a (on-chip SRAM only)</td>
<td>memory encryption</td>
</tr>
</tbody>
</table>
So where are we?
So where are we?
And now...

**SECURITY TIPS**

(print out this list and keep it in your bank safe deposit box)

- Don't click links to websites
- Use prime numbers in your password
- Change your password manager monthly
- Hold your breath while crossing the border
- Install a secure font
- Use a 2-factor smoke detector
- Change your maiden name regularly
- Put strange USB drives in a bag of rice overnight
- Use special characters like & and %
- Only read content published through tor.com
- Use a burner's phone
- Get an SSL certificate and store it in a safe place
- If a border guard asks to examine your laptop, you have a legal right to challenge them to a chess game for your soul.