Generic Scalar Multiplication

Input: Integer $k$ and generator $G$
Output: $P = kG$

$K = \text{Encode}(k)$
$S'_0 = \text{Init}(G)$
for $K_i \in K = \{K_1, K_2, \ldots, K_n\}$ do
$S'_i = \text{Select}(S'_{i-1}, K_i)$
$S'_i = \text{Process}(S'_i)$
$P = \text{Finalize}(S'_n)$
return $P$

Attack Input and Direction

$K = \text{Encode}(k)$
$S'_0 = \text{Init}(G)$
for $K_i \in K = \{K_1, K_2, \ldots, K_n\}$ do
$S'_i = \text{Select}(S'_{i-1}, K_i)$
$S'_i = \text{Process}(S'_i)$
$P = \text{Finalize}(S'_n)$
return $P$

Generic trace
An OTA assumes each execution of the process operation leaks about the state $S_i$: $\text{Process}(S_i) \rightarrow L_i(S_i)$. A generic trace is composed by a sequence of $L_i$: $(L_1, L_2, \ldots, L_n)$.

Controlled Side-Channels

<table>
<thead>
<tr>
<th>Page</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>nop</td>
</tr>
<tr>
<td>P2</td>
<td>nop</td>
</tr>
<tr>
<td>P3</td>
<td>nop</td>
</tr>
</tbody>
</table>

PageTracer: Tracks the sequence of executed memory pages [4].

CopyCat: Counts # executed instructions at each tracked page [5].

Analyzed Open Source Libraries

**libgcrypt**

Double-and-add always

$R = 0$
for $i = \lceil \log_2 k \rceil$ downto 0 do
$R = 2R$
$T = R + G$
$R = \text{cond}\_\text{assign}(T, R, K_i)$
return $R$

**mbedTLS**

Comb method

$K = \text{Encode}(k)$
$P = \text{Precompute}(G)$
$R = \text{Select}(K_1, P)$
for $K_i \in K$, $i = 2, 3, \ldots, n$ do
$R = 2R$
$T = \text{Select}(K_i, P)$
$R = R + T$
return $R$

**wolfSSL**

Montgomery ladder

$R = G, S = 2G$
for $i = \lceil \log_2 k \rceil$ downto 0 do
if $k_i = 0$
$S = R + S, R = 2R$
else
$R = R + S, S = 2S$
return $R$

Leakage Analysis

For each library we enumerated the memory pages used by the selected process operations highlighted above. We evaluated the difficulty of an OTA for each memory page combination using both PageTracer and CopyCat side-channels.

The percentages below correspond to the ratio of combinations that fall into Ideal and Insecure settings.

<table>
<thead>
<tr>
<th>Attack</th>
<th>Ideal</th>
<th>Insecure</th>
<th>Max bias</th>
</tr>
</thead>
<tbody>
<tr>
<td>PageTracer</td>
<td>0</td>
<td>87%</td>
<td>50%</td>
</tr>
<tr>
<td>CopyCat</td>
<td>50%</td>
<td>98%</td>
<td>30%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attack</th>
<th>Ideal</th>
<th>Insecure</th>
<th>Max bias</th>
</tr>
</thead>
<tbody>
<tr>
<td>PageTracer</td>
<td>84%</td>
<td>99%</td>
<td>62%</td>
</tr>
<tr>
<td>CopyCat</td>
<td>99%</td>
<td>100%</td>
<td>24%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attack</th>
<th>Ideal</th>
<th>Insecure</th>
<th>Max bias</th>
</tr>
</thead>
<tbody>
<tr>
<td>PageTracer</td>
<td>0</td>
<td>69%</td>
<td>52%</td>
</tr>
<tr>
<td>CopyCat</td>
<td>47%</td>
<td>94%</td>
<td>24%</td>
</tr>
</tbody>
</table>

References