Side Channel Attacks

Differential Power Analysis
Power Consumption

- Power consumption depends on the inputs to a circuit.
- We can reveal information about the circuit by observing the power consumption.
Data Acquisition

AES-256
Data Acquisition

- Insert a small resistor at the ground pin.
- ~ 5 - 10 ohm
Data Acquisition

- Insert a small resistor at the ground pin.
- ~ 5 - 10 ohm
- Use an oscilloscope to measure the voltage across the resistor
We can see the 16 rounds of DES on this trace.

Notice the variation in voltage between the rounds.
Power Trace
Hamming Weight Model

- Count the number of ‘1s’ in a binary number.
- Model each bit as a capacitor.
- A ‘1’ means we charge the capacitor.
- A ‘0’ means we don’t charge the capacitor.
Hamming Weight Model

- Example:
  - $0x67 = 0110\ 0111$
  - $HW(0x67) = 5$
Hamming Distance Model

- Count the number of bits that differ in two binary numbers.
- Represents an XOR gate.
- A bit that changes uses more power than one that doesn’t change.
Hamming Distance

- Example
  - $0x53 = 0101 0011$
  - $0x78 = 0111 1000$
  - $XOR(0x53, 0x78) = 0010 1011$
  - $HD(0x53, 0x78) = 4$
DPA Example: RSM

- Plaintext is masked prior to encryption.
DPA Example: RSM

- Given:
  - $M = \{0x00, 0x0F, 0x36, 0x39, 0x53, 0x5C, 0x65, 0x6A, 0x95, 0x9A, 0xA3, 0xAC, 0xC6, 0xC9, 0xF0, 0xFF\}$
  - Randomly generated offset shifts masks.
  - Offset updated after encrypting one block.
DPA Example: RSM

- Need to determine mask offset in order to mount DPA attack.
- Target address bus when reading masks from memory.
DPA Example: RSM

- Use hamming weight to guess power consumption of the least significant byte of the address.

- \( h = \text{HD}\{0x0, 0x1, 0x2, 0x3, 0x4, 0x5, 0x6, 0x7, 0x8, 0x9, 0xA, 0xB, 0xC, 0xD, 0xE, 0xF\} \)
- \( h = \{0, 1, 1, 2, 1, 2, 2, 3, 1, 2, 2, 3, 2, 3, 3, 4\} \)
DPA Example: RSM

- We expect to see a pattern like one of the following:
  - \( h = \{0, 1, 1, 2, 1, 2, 2, 3, 1, 2, 2, 3, 2, 3, 3, 4\} \)
  - \( h = \{1, 1, 2, 1, 2, 2, 3, 1, 2, 2, 3, 2, 3, 3, 4, 0\} \)
  - \( h = \{1, 2, 1, 2, 2, 3, 1, 2, 2, 3, 2, 3, 3, 4, 0, 1\} \)
  - ... 
  - \( h = \{4, 0, 1, 1, 2, 1, 2, 2, 3, 1, 2, 2, 3, 2, 3, 3\} \)
DPA Example: RSM

- Select points of interest from power trace.
- Access memory each loop iteration.
DPA Example: RSM
DPA Example: RSM

- Use Pearson Correlation Coefficient to find best offset.

<table>
<thead>
<tr>
<th>Offset</th>
<th>Correlation</th>
<th>Offset</th>
<th>Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0</td>
<td>.4634</td>
<td>0x8</td>
<td>.9347</td>
</tr>
<tr>
<td>0x1</td>
<td>-.3055</td>
<td>0x9</td>
<td>.0466</td>
</tr>
<tr>
<td>0x2</td>
<td>-.0181</td>
<td>0xA</td>
<td>.1942</td>
</tr>
<tr>
<td>0x3</td>
<td>-.4194</td>
<td>0xB</td>
<td>-.3935</td>
</tr>
<tr>
<td>0x4</td>
<td>.0386</td>
<td>0xC</td>
<td>.3599</td>
</tr>
<tr>
<td>0x5</td>
<td>-.246</td>
<td>0xD</td>
<td>-.4065</td>
</tr>
<tr>
<td>0x6</td>
<td>.1217</td>
<td>0xE</td>
<td>-.0388</td>
</tr>
<tr>
<td>0x7</td>
<td>-.1709</td>
<td>0xF</td>
<td>-.5075</td>
</tr>
</tbody>
</table>
DPA Example: RSM

● To recover the key:
  ○ Use hamming distance between key guess and masked plaintext to estimate power consumption.
  ○ Calculate the correlation coefficient between hypothetical power consumption and the measured power consumption.
● Requires many power traces.
Questions?

- For more information, see:
  - www.dpacontest.org