Maya: Obfuscating Power Side Channels with Formal Control

ISCA’21

Raghavendra Pradyumna Pothukuchi, Sweta Yamini Pothukuchi, Petros G Voulgaris, Alexander Schwing, Josep Torrellas
Power Side Channels

Counters, trojan chips...

Power

Machine learning, Statistical analyses

Passwords, application information, browser, camera, location, crypto keys ...

Power is a powerful side channel!
Existing Power Defenses

Obvious approaches are ineffective
E.g., Adding random power activity
E.g., Measure and correct for constant power

Intrusive changes to hardware, algorithms and software
Systems in the field are left vulnerable
Typically focus on encryption
Other sensitive information (e.g., browser data) can leak through system-level power
Maya: Power Reshaping for Security

Reshape the computer’s power using formal control

1. Dynamic voltage-frequency level
2. Idle activity level
   E.g., Intel Powerclamp
3. Power balloon level
   Matrix multiply operations mixed with sleep
**Maya: Power Reshaping for Security**

Reshape the computer’s power using formal control

- **Application-transparent!**
- **First use of formal control for side-channel defense!**
Maya: Robust Controller

Matrices \([A, B, C, D]\), and state

\[
\text{inputs} = C \times \text{state} + D \times \text{deviations}
\]

\[
\text{state}_{\text{new}} = A \times \text{state} + B \times \text{deviations}
\]

Deviations are small even when runtime conditions differ from design conditions
Maya: Mask Generator

Obfuscate time and frequency domain patterns

Gaussian Sinusoid

Change the sinusoid and Gaussian parameters

Original application changes will either be lost or be masked
Maya: Configurable Inputs

Protecting personal data
(milliseconds)
1. Dynamic voltage-frequency level
2. Idle activity level
   Idle threads from kernel
3. Power balloon level
   Matrix multiply operations mixed with sleep

No new hardware!

Cryptographic keys
(micro/nano seconds)
1. Dynamic voltage
2. Pipeline bubbles
3. Power microcode
   NOPs + HALT
Implementation Highlights

Maya as admin software on three real systems

Machine Learning (ML) based attacks
Detect applications, videos, webpages
Attacks are adaptive i.e., trained using traces collected when Maya is running
Alternative Defenses

Random Noise: Randomly set frequency, idleness and power balloon levels

Maya Constant: Obfuscated with a constant target

Maya Gaussian Sinusoid: Obfuscated with a Gaussian Sinusoid target

ML-based attack: application detection

11 choices

Train with “Random Noise” traces and “Maya” traces
Random Noise

How many predicted to be of label

Among all signals labeled

Accuracy 94%
ML is very effective
Random Noise

Baseline power signal

Random Noise

[Graphs showing power over time with annotations and labels]
Maya Constant

Accuracy 62%  Maya Constant leaks information!
### Maya Gaussian Sinusoid (GS)

<table>
<thead>
<tr>
<th>True label</th>
<th>Predicted label</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.07 0.07 0.08 0.08 0.10 0.11 0.07 0.11 0.12 0.05 0.12</td>
</tr>
<tr>
<td>1</td>
<td>0.06 0.13 0.14 0.06 0.05 0.13 0.05 0.11 0.08 0.10 0.09</td>
</tr>
<tr>
<td>2</td>
<td>0.11 0.06 0.11 0.06 0.12 0.15 0.06 0.13 0.04 0.05 0.12</td>
</tr>
<tr>
<td>3</td>
<td>0.08 0.07 0.11 0.08 0.06 0.12 0.06 0.11 0.09 0.10 0.11</td>
</tr>
<tr>
<td>4</td>
<td>0.09 0.08 0.08 0.05 0.15 0.13 0.07 0.10 0.05 0.12 0.07</td>
</tr>
<tr>
<td>5</td>
<td>0.06 0.08 0.12 0.06 0.10 0.14 0.06 0.08 0.07 0.11 0.14</td>
</tr>
<tr>
<td>6</td>
<td>0.04 0.05 0.06 0.08 0.08 0.12 0.11 0.10 0.10 0.12 0.15</td>
</tr>
<tr>
<td>7</td>
<td>0.06 0.10 0.07 0.07 0.05 0.12 0.06 0.11 0.14 0.10 0.12</td>
</tr>
<tr>
<td>8</td>
<td>0.05 0.06 0.09 0.05 0.07 0.07 0.07 0.07 0.24 0.10 0.11</td>
</tr>
<tr>
<td>9</td>
<td>0.06 0.11 0.11 0.07 0.05 0.08 0.05 0.09 0.09 0.24 0.07</td>
</tr>
<tr>
<td>10</td>
<td>0.07 0.11 0.06 0.07 0.05 0.15 0.04 0.11 0.06 0.08 0.20</td>
</tr>
</tbody>
</table>

**Accuracy 14%**  **Excellent obfuscation!**
Average Analysis

Random Noise

Maya Constant

Maya Gaussian Sinusoid

Power (W)

Applications

Power (W)

Applications

Power (W)

Applications

Avg. Power (W)

Samples

Avg. Power (W)

Samples

Avg. Power (W)

Samples
Effectiveness of Formal Control

Average analysis of GS masks

Average analysis of actual power

![Graphs showing average analysis of GS masks and actual power](image-url)
Instruction Profiling

Key aspect of PLATYPUS analysis

Baseline

Maya GS

Maya can hide instruction profiling!
New Covert Channel

[Shao et al, SIGMETRICS’20]

1. Transmitter computer
2. Transmitter’s power outlet
3. Oscilloscope (Sampling and digitization)
4. Receiver laptop
5. Receiver’s power outlet

Maya completely prevents information exfiltration
Takeaways

• Power side channels are an important threat to privacy
  • Need simple and effective defenses ready for deployment

• Maya uses formal control to shape power and hide activity

• Real system implementations are effective
  • Evades adaptive machine learning attacks and signal analysis

Shao et al, SIGMETRICS’20: “[Maya] offers a perfect defense against [the new attack]”

Full paper: Details about the mask generator, other attacks and more!
Releasing the source code and a technical report on formal controller design!
Backup
Impact on Power Consumption

29% lower power
Impact on Application Performance

47% longer time
Threat Model

- Attackers seek information from power measurements
  - Counters, unprivileged information, physical access, remote signals…

- Attackers can adapt to the defense algorithm

- The defense must be running on an uncompromised part
  - Random seed is protected