Maya: Obfuscating Power Side Channels with Formal Control

ISCA'21

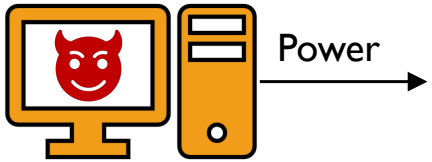
Raghavendra Pradyumna Pothukuchi, Sweta Yamini Pothukuchi, Petros G Voulgaris, Alexander Schwing, Josep Torrellas

Yale

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

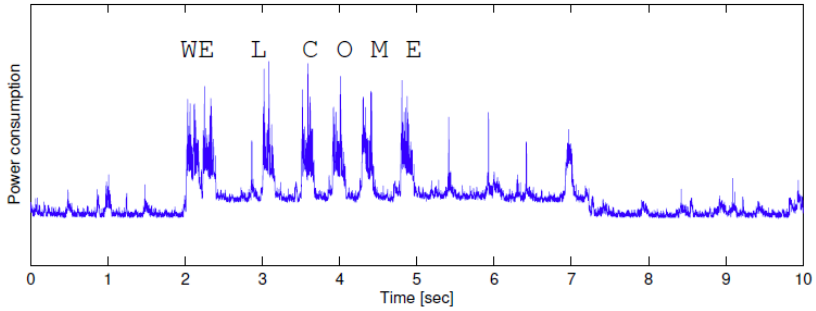
Power Side Channels

Counters, trojan chips…



Machine learning, Statistical analyses

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



[Lifshits et al, PoPETS'18]

Power is a powerful side channel!

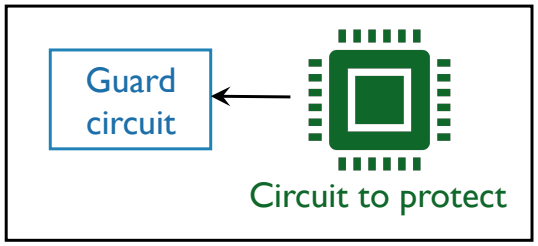
i-acoma group

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

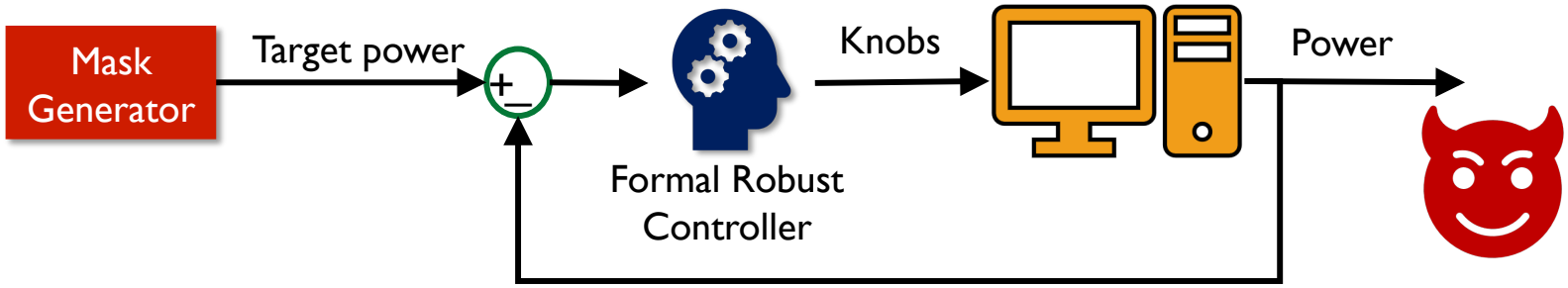
Systems in the field are left vulnerable

Typically focus on encryption

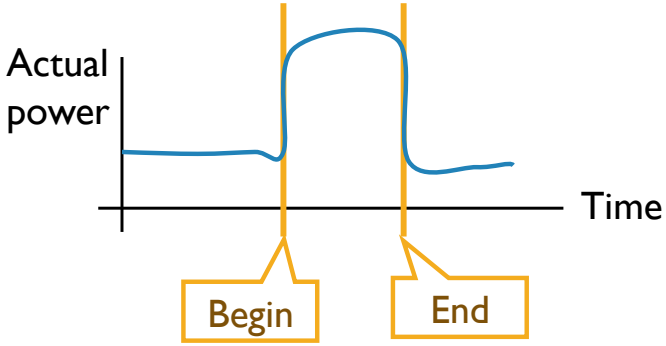
Other sensitive information (e.g., browser data) can leak through system-level power

Maya: Power Reshaping for Security

Reshape the computer's power using formal control



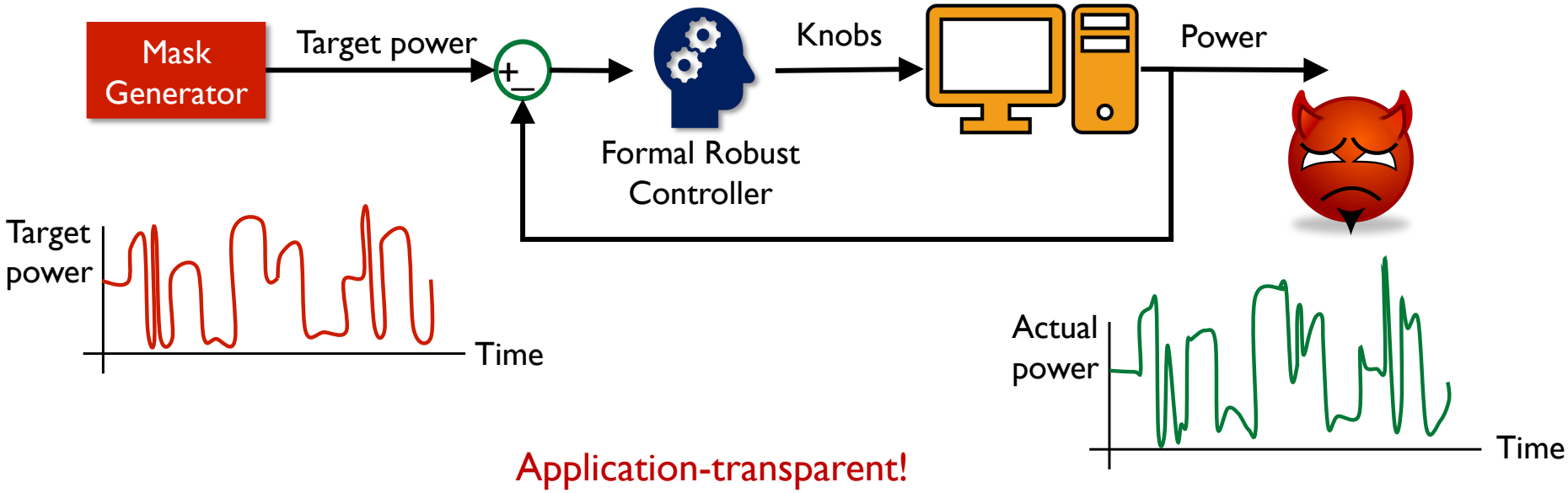
1. Dynamic voltage-frequency level
2. Idle activity level
   E.g., Intel Powerclamp
3. Power balloon level
   Matrix multiply operations mixed with sleep



i-acoma group

Maya: Power Reshaping for Security

Reshape the computer's power using formal control

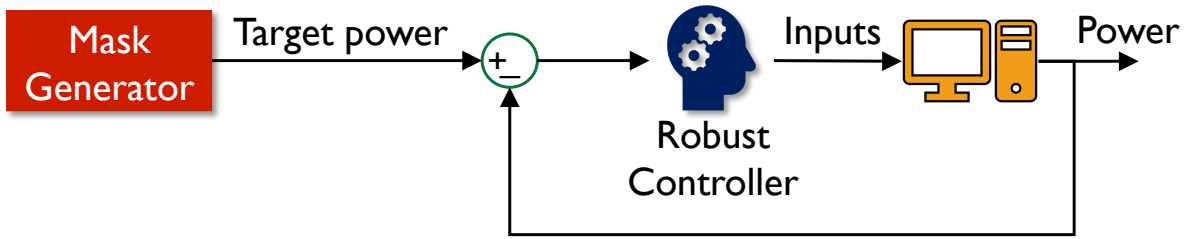


Application-transparent!

First use of formal control for side-channel defense!

i-acoma group

Maya: Robust Controller

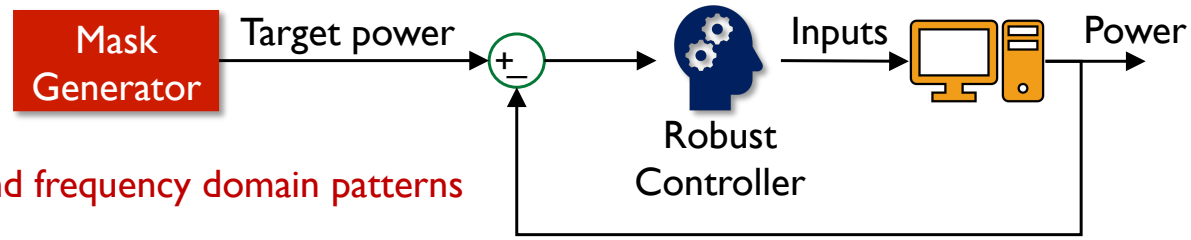


Matrices [*A, B, C, D*], and *state*

$$\left.\begin{aligned} \text{inputs} &= C \times state + D \times deviations \\ \text{state}\downarrow\text{new} &= A \times state + B \times deviations \end{aligned}\right\} \text{Every T time-units}$$

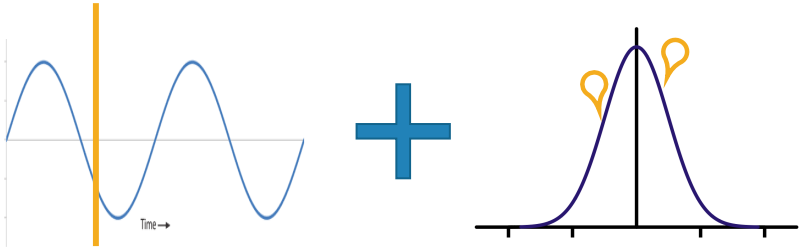
Deviations are small even when runtime conditions differ from design conditions

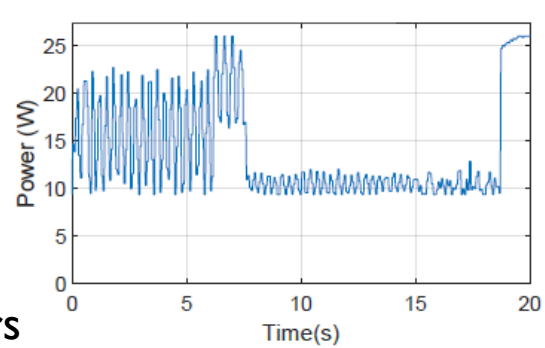
Maya: Mask Generator

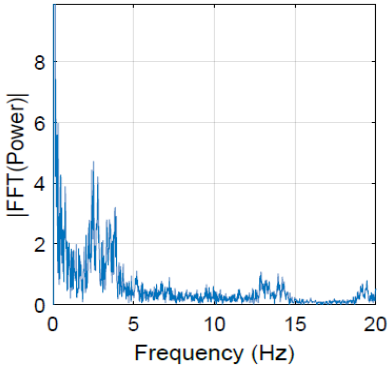


Obfuscate time and frequency domain patterns

Gaussian Sinusoid





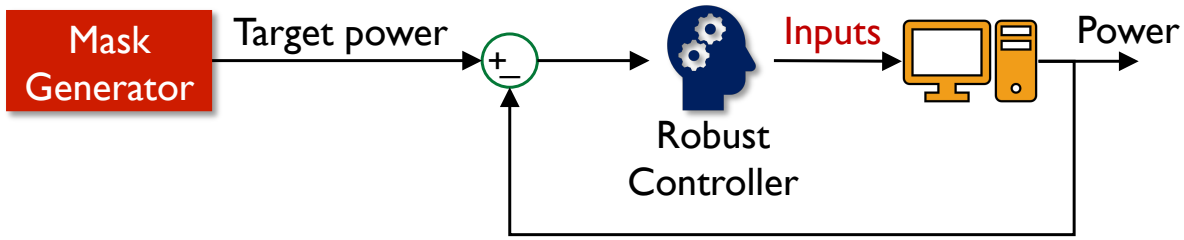


Change the sinusoid and Gaussian parameters

Original application changes will either be lost or be masked

i-acoma group

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

Cryptographic keys

(micro/nano seconds)

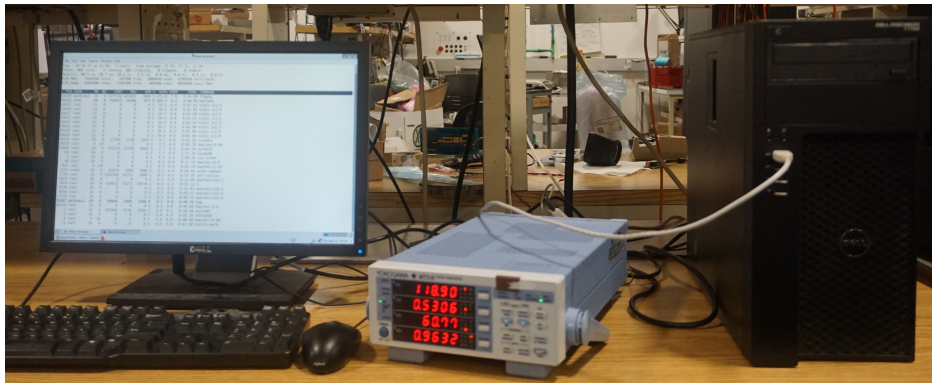
1. Dynamic voltage
2. Pipeline bubbles
3. Power microcode
   NOPs + HALT

No new hardware!

i-acoma group

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

True app# \ Predicted app#	0	1	2	3	4	5	6	7	8	9	10
0	0.85	0.06	0.06	0.00	0.00	0.00	0.00	0.00	0.02	0.00	0.02
1	0.04	0.88	0.03	0.00	0.00	0.00	0.00	0.00	0.02	0.00	0.04
2	0.01	0.01	0.89	0.00	0.00	0.00	0.00	0.00	0.08	0.00	0.00
3	0.00	0.00	0.00	0.98	0.00	0.01	0.00	0.00	0.00	0.01	0.00
4	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00
5	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00
6	0.02	0.03	0.02	0.00	0.01	0.00	0.91	0.01	0.01	0.00	0.00
7	0.00	0.00	0.00	0.00	0.00	0.01	0.00	0.99	0.00	0.00	0.00
8	0.00	0.00	0.03	0.00	0.00	0.01	0.00	0.00	0.95	0.00	0.00
9	0.00	0.00	0.00	0.01	0.00	0.05	0.00	0.00	0.00	0.94	0.00
10	0.01	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.98

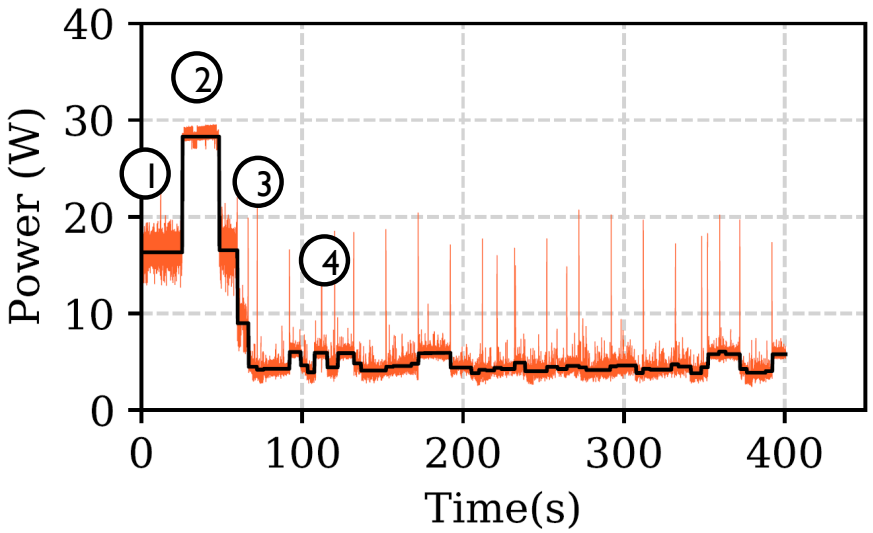
Accuracy 94%

ML is very effective

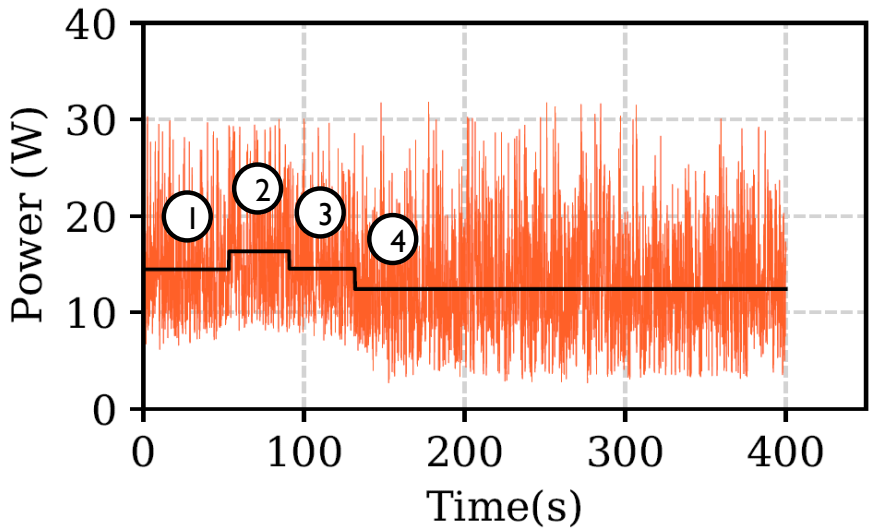
i-acoma group

Random Noise

Baseline power signal



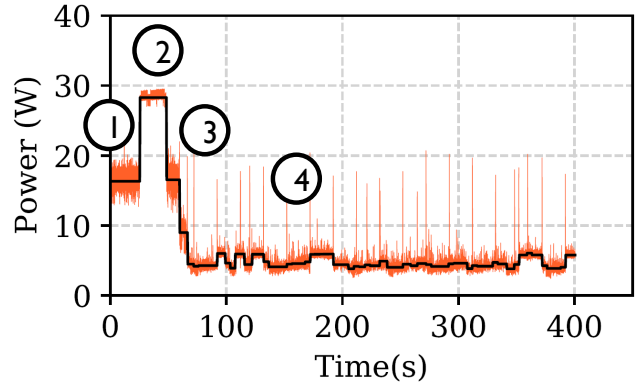
Random Noise



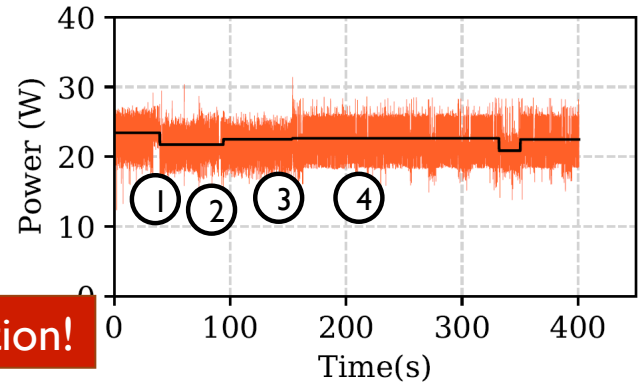
Maya Constant

True app# \ Predicted app#	0	1	2	3	4	5	6	7	8	9	10
0	0.56	0.05	0.03	0.07	0.02	0.04	0.08	0.04	0.03	0.03	0.04
1	0.04	0.39	0.06	0.10	0.05	0.08	0.10	0.05	0.07	0.03	0.04
2	0.04	0.01	0.69	0.02	0.05	0.01	0.01	0.03	0.06	0.02	0.05
3	0.03	0.03	0.02	0.59	0.03	0.03	0.05	0.02	0.07	0.09	0.05
4	0.03	0.03	0.02	0.08	0.61	0.02	0.05	0.02	0.10	0.02	0.01
5	0.02	0.02	0.00	0.02	0.01	0.71	0.05	0.02	0.07	0.08	0.00
6	0.08	0.06	0.04	0.04	0.06	0.04	0.40	0.10	0.04	0.11	0.03
7	0.02	0.02	0.03	0.03	0.01	0.02	0.09	0.63	0.06	0.06	0.02
8	0.01	0.05	0.00	0.02	0.03	0.04	0.03	0.01	0.75	0.06	0.00
9	0.01	0.01	0.03	0.03	0.01	0.05	0.06	0.03	0.03	0.75	0.01
10	0.03	0.06	0.01	0.03	0.03	0.04	0.03	0.05	0.02	0.03	0.68

Baseline



Maya Constant



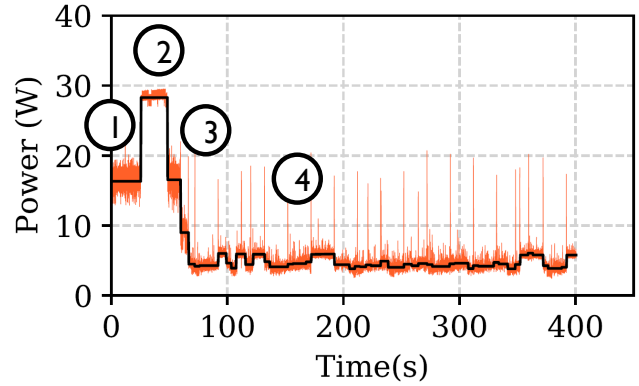
Accuracy 62%

Maya Constant leaks information!

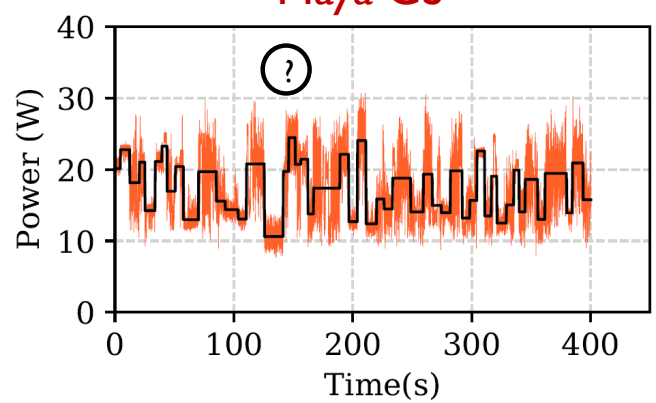
Maya Gaussian Sinusoid (GS)

True label \ Predicted label	0	1	2	3	4	5	6	7	8	9	10
0	0.07	0.07	0.08	0.08	0.10	0.11	0.07	0.11	0.12	0.05	0.12
1	0.06	0.13	0.14	0.06	0.05	0.13	0.05	0.11	0.08	0.10	0.09
2	0.11	0.06	0.11	0.06	0.12	0.15	0.06	0.13	0.04	0.05	0.12
3	0.08	0.07	0.11	0.08	0.06	0.12	0.06	0.11	0.09	0.10	0.11
4	0.09	0.08	0.08	0.05	0.15	0.13	0.07	0.10	0.05	0.12	0.07
5	0.06	0.08	0.12	0.06	0.10	0.14	0.06	0.08	0.07	0.11	0.14
6	0.04	0.05	0.06	0.08	0.08	0.12	0.11	0.10	0.10	0.12	0.15
7	0.06	0.10	0.07	0.07	0.05	0.12	0.06	0.11	0.14	0.10	0.12
8	0.05	0.06	0.09	0.05	0.07	0.07	0.07	0.07	0.24	0.10	0.11
9	0.06	0.11	0.11	0.07	0.05	0.08	0.05	0.09	0.09	0.24	0.07
10	0.07	0.11	0.06	0.07	0.05	0.15	0.04	0.11	0.06	0.08	0.20

Baseline



Maya GS

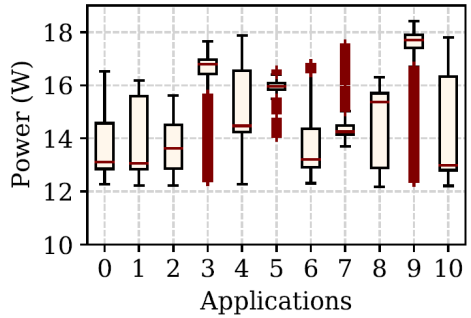


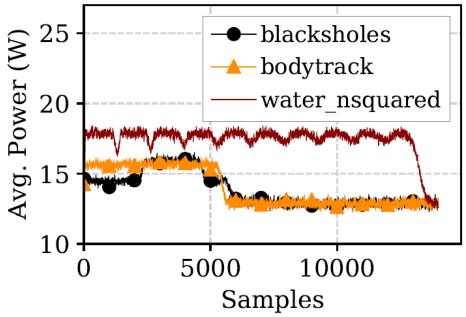
Accuracy 14%

Excellent obfuscation!

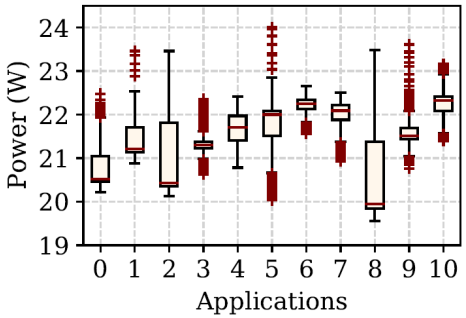
Average Analysis

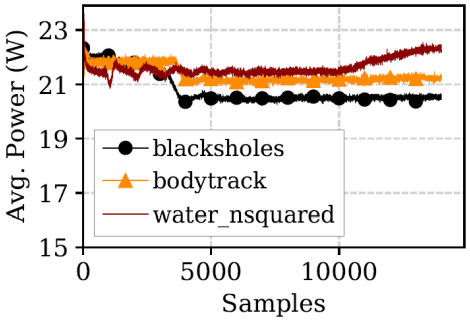
Random Noise



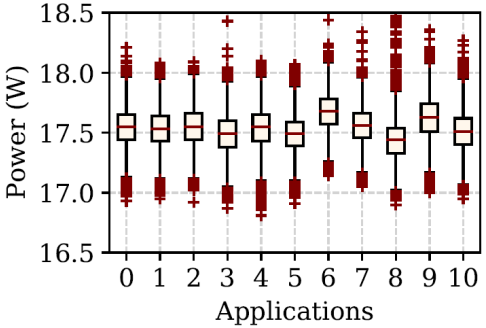


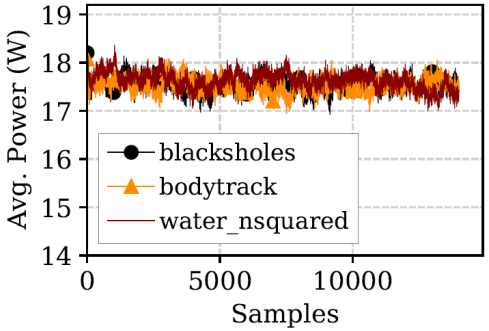
Maya Constant





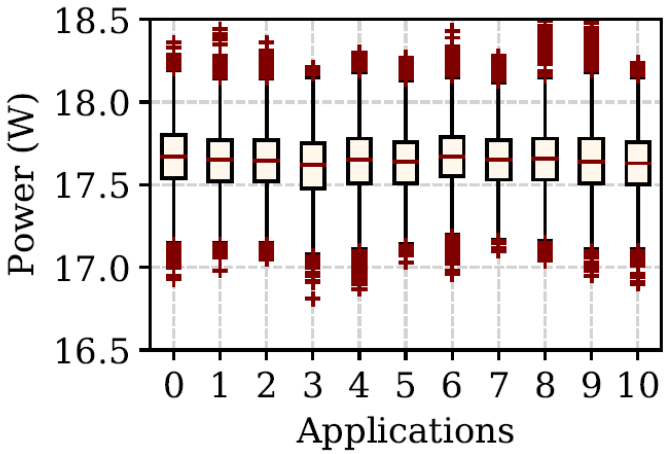
Maya Gaussian Sinusoid



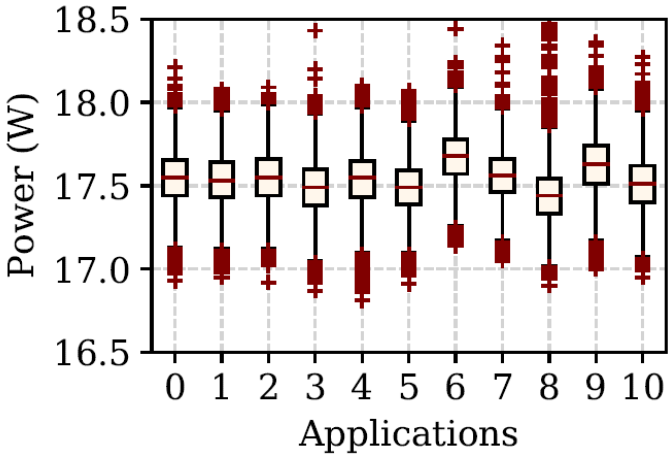


Effectiveness of Formal Control

Average analysis of GS masks



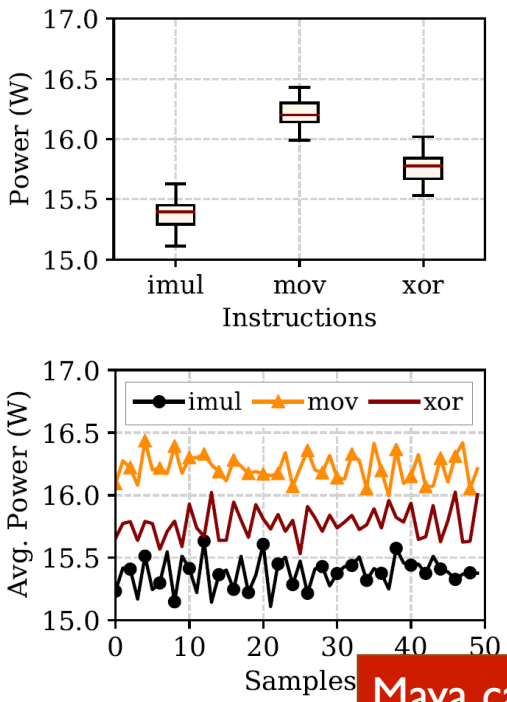
Average analysis of actual power



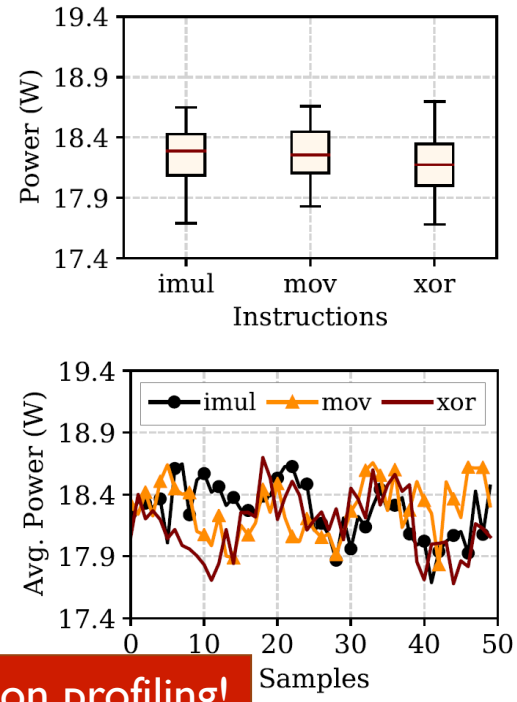
Instruction Profiling

Key aspect of PLATYPUS analysis

Baseline



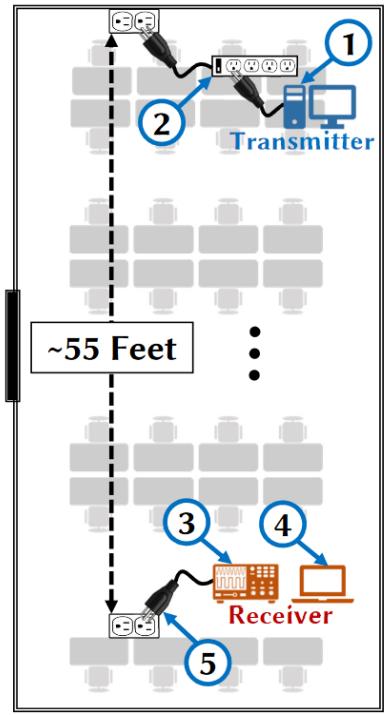
Maya GS

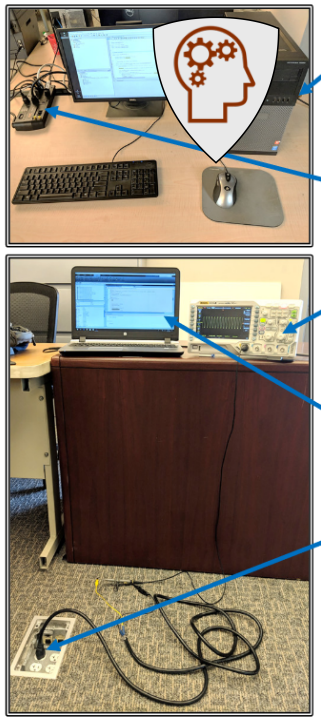


Maya can hide instruction profiling!

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

i-acoma group

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

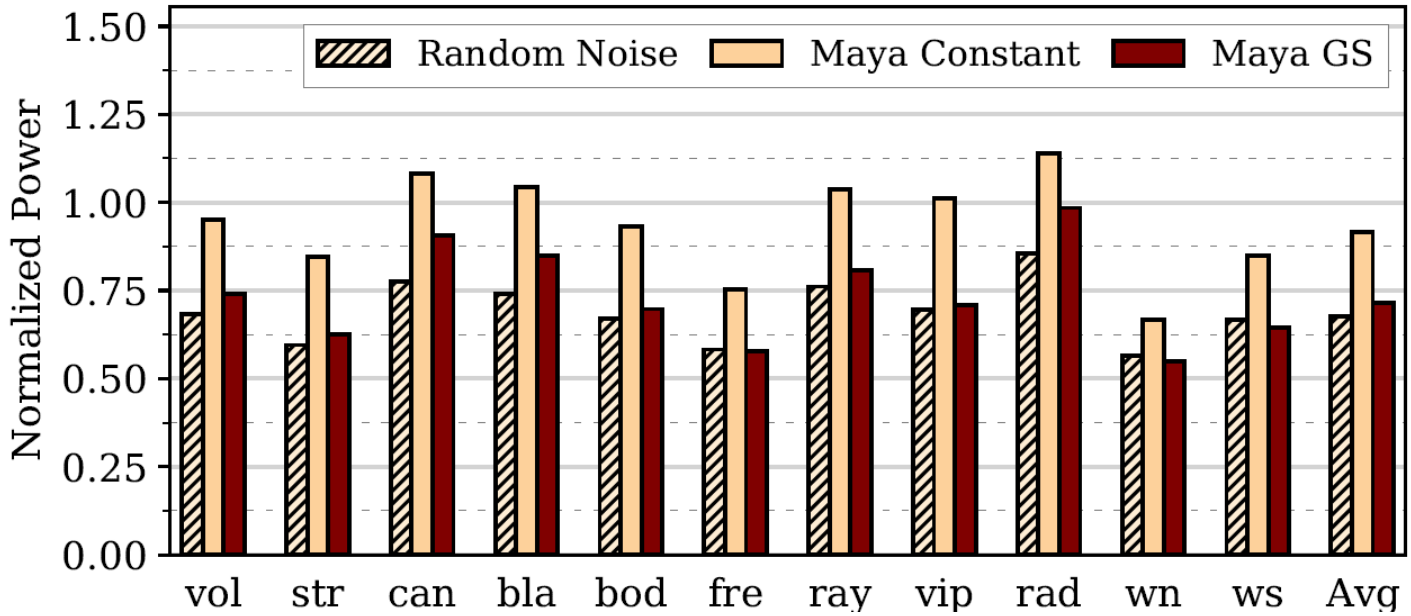
Shao et al, SIGMETRICS'20: "[Maya] offers a perfect defense against [the new attack]"

Full paper: Details about the mask generator, other attacks and more!

Releasing the source code and a technical report on formal controller design!

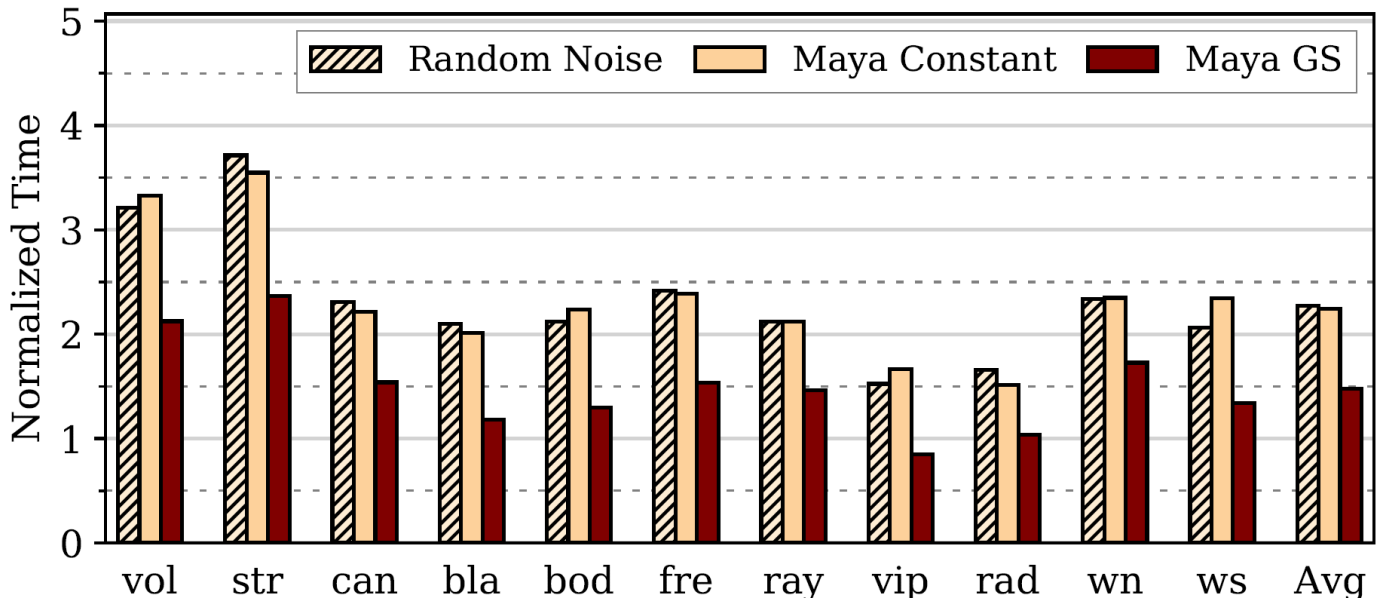
Backup

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