**Maya: Using Formal Control to Obfuscate Power Side Channels**

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

**Power is a Powerful Side Channel**

- Counters, Trojan chips...
- Machine Learning, Statistical Analysis, Signal Processing
- Power
- Passwords, application information, browser, camera, location, cryptographic keys...

**Existing Defenses have Limitations**

- Obvious approaches are ineffective
  - E.g., Add random noise
    - Removed by averaging!
  - E.g., Measure and correct for constant power

- Intrusive changes to systems
  - Systems in the field are left vulnerable

- Typically focus on encryption
  - Sensitive data (e.g., browser data) can leak through system-level power

**Key Idea**

- Use formal control to intelligently re-shape a computer’s power, transparent to applications.
  - “Power can be shaped in any desired form, appearing to carry activity information which, in fact, is unrelated to the application.”

**Maya Architecture**

- Mask Generator
  - Creates targets to obfuscate time and frequency patterns
  - Gaussian Sinusoid: varying sinusoid + Gaussian distribution

- Formal Robust Controller
  - Actuates multiple knobs to reliably keep power close to targets

- Knobs
  - DVFS level, idle cycles, custom balloon application
  - Can be fine-grained: pipeline bubbles, power hungry ops etc.

- Excellent obfuscation!

**Experimental Highlights**

- Web page detection
  - Random knobs (51% accuracy)
  - Maya (14% accuracy)

- Deep dive: application detection
  - Original
  - Random Knobs
  - Maya

**Experimental Setup**

- Maya as admin software on three real systems

- Machine Learning (ML) based attacks
  - Detect applications, videos, and web-pages
  - Also use signal analysis (e.g., changepoint analysis)

**Other Attacks**

- Instruction profiling
  - (e.g., PLATYPUS)
  - Run instructions in a loop, and average multiple runs

- Covert channel: Power delivery network
  - Original
  - Maya

**Acknowledgments**

This work was supported by NSF grant CNS 1763658.

Acknowledgements: Kevin Colzary (UIUC), Dipanjan Das (Renesas), Tarek Abdelzaher (UIUC)