CAREER: Advanced Trace-oriented Binary Code Analysis

Dinghao Wu, Pennsylvania State University

Challenge:

- How to model cache behaviors for side channel detection?
- LRU, for example, is too complicated for program analysis.
- How to make the analysis scalable?
- How to quantify or rank the severity of the discovered vulnerabilities?

Solution:

F(p,k) >> L ≠ F(p,k') >> L

p – public information

k – secret information

F(p,k) – a symbolic memory address accessed

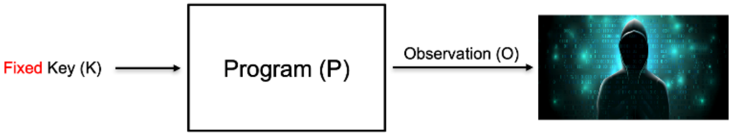
F(p,k') – replace secret k with a fresh variable k'

L – cache line width

CAREER: Advanced Trace-oriented Binary Code Analysis, Award ID#: NSF CNS-1652790

Dinghao Wu, Pennsylvania State University

A real attack can fix the input key to make it not random.



Fixed Key (K) → Program (P) → Observation (O)

Precise quantification of side channel leakage of private information using trace-based analysis and information theory.

Leakage =

$$log_2|K| - log_2|O|$$

Scientific Impact:

- A new principled method for modeling cache-based side channel vulnerabilities

Broader Impact:

- Found many new vulnerabilities in the production crypto systems
- Some of the new vulnerabilities discovered have been fixed