

Side-channel Vulnerability Factor

John Demme, Adam Waksman and Robert Martin

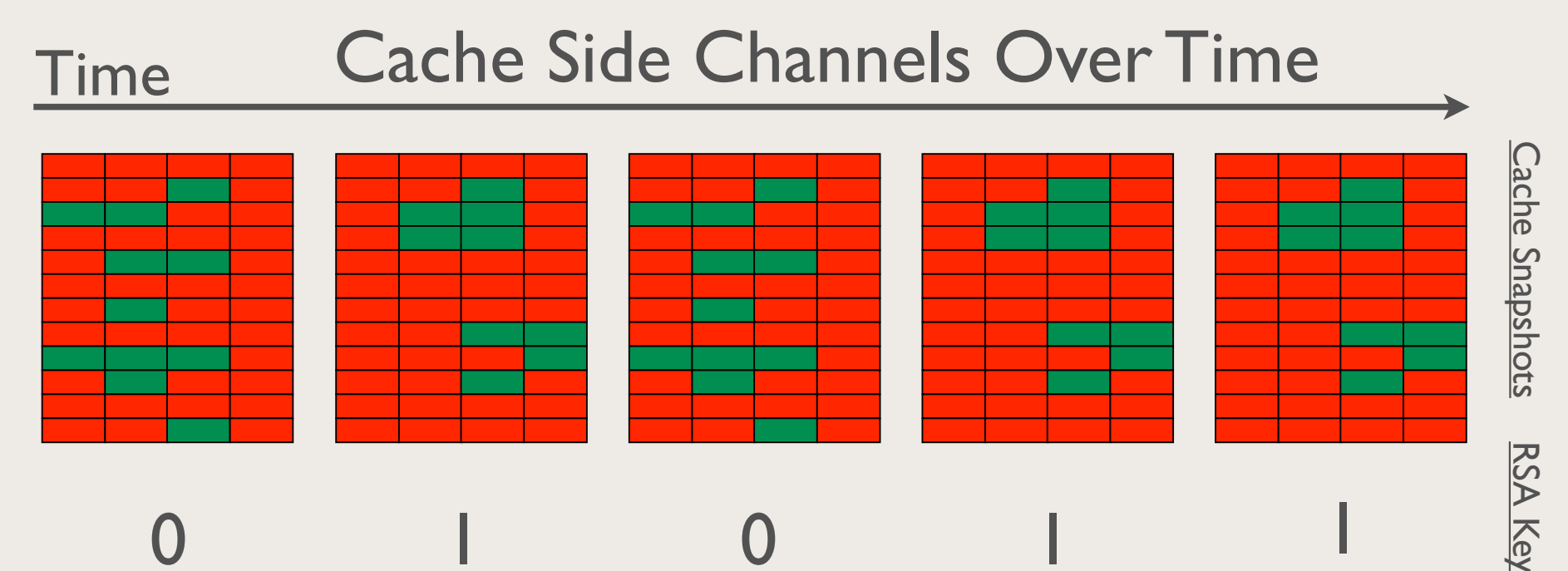
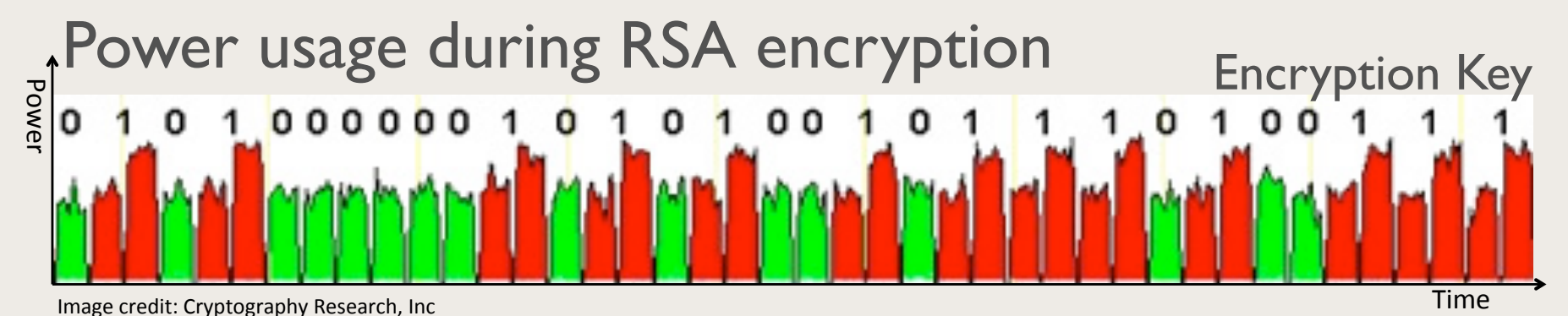
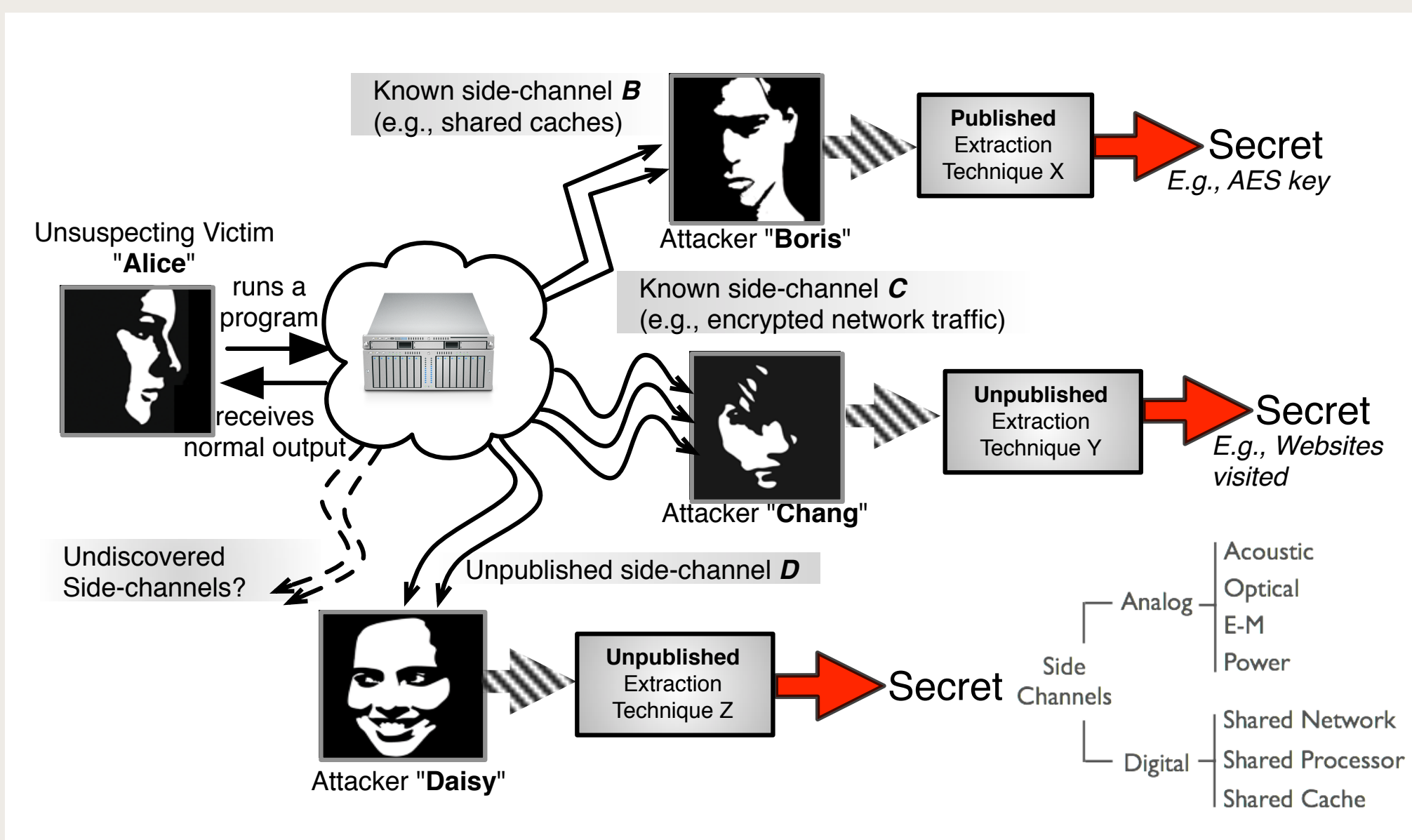
Prof. Simha Sethumadhavan, Columbia University

<http://castl.cs.columbia.edu>

How much information do digital computer systems leak?

In a digital side-channel attack, an attacker is able to gather information leaking about a victim's execution through some computing resource they share.

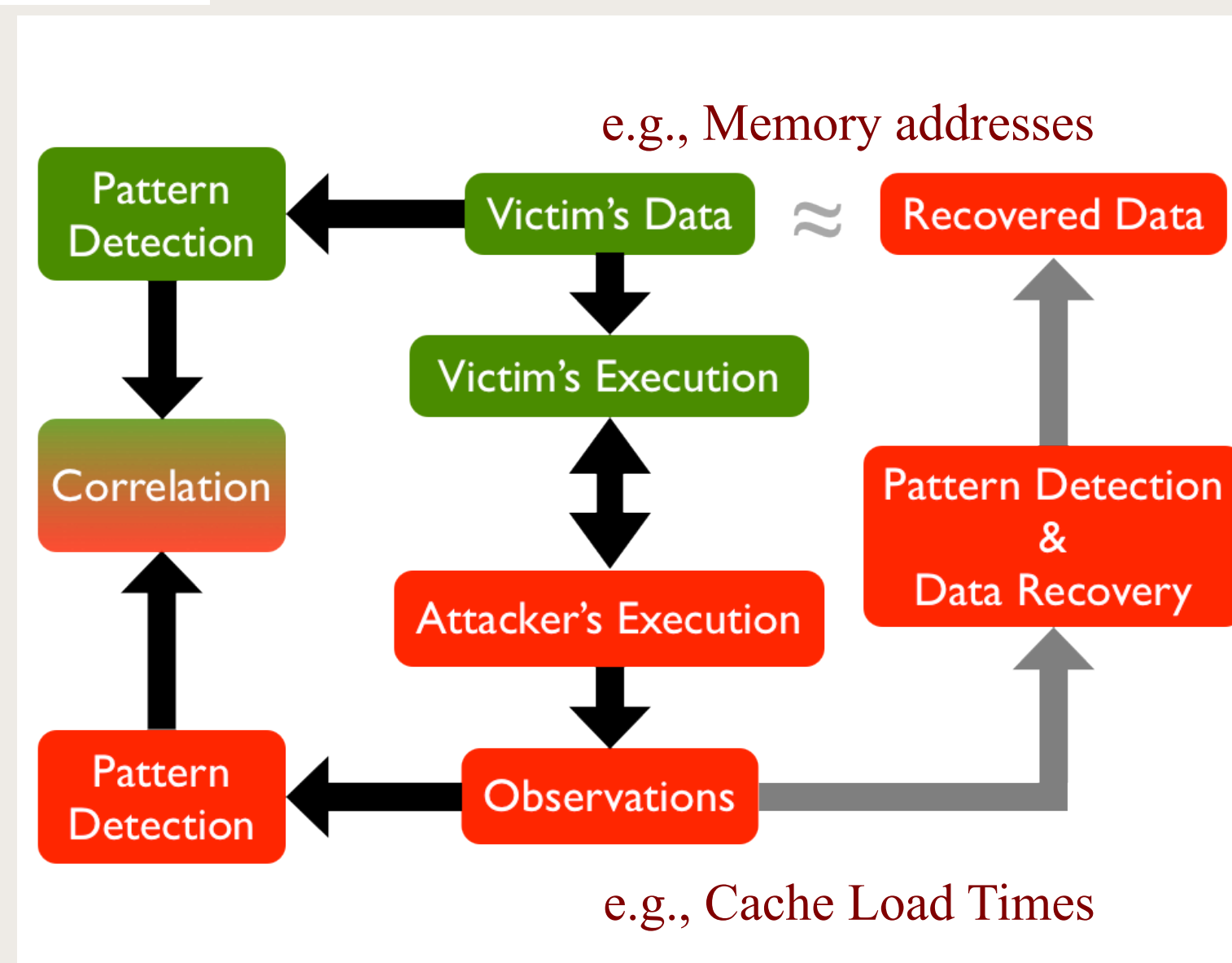
Insight: Attacker's correlate measured patterns to victim's secrets.



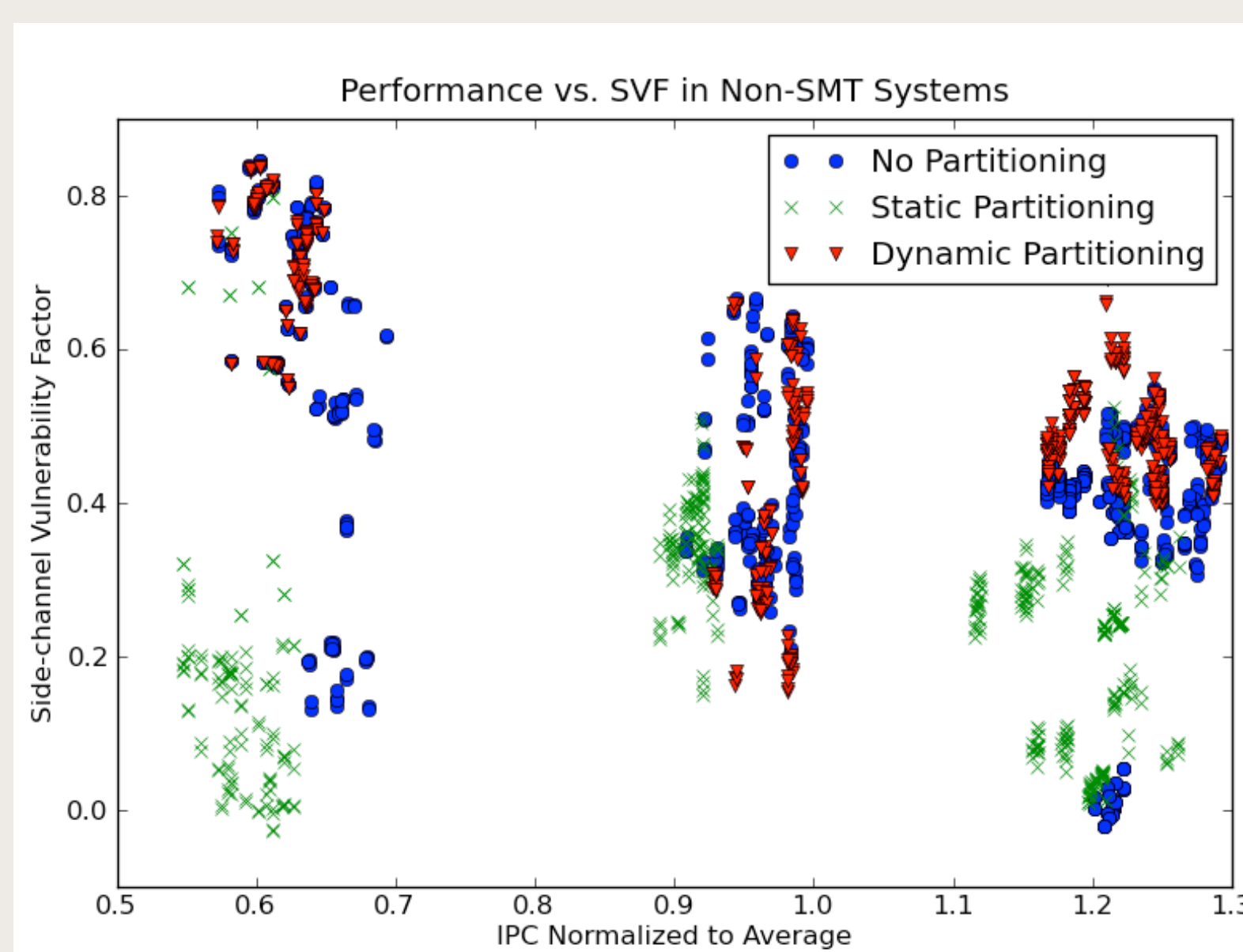
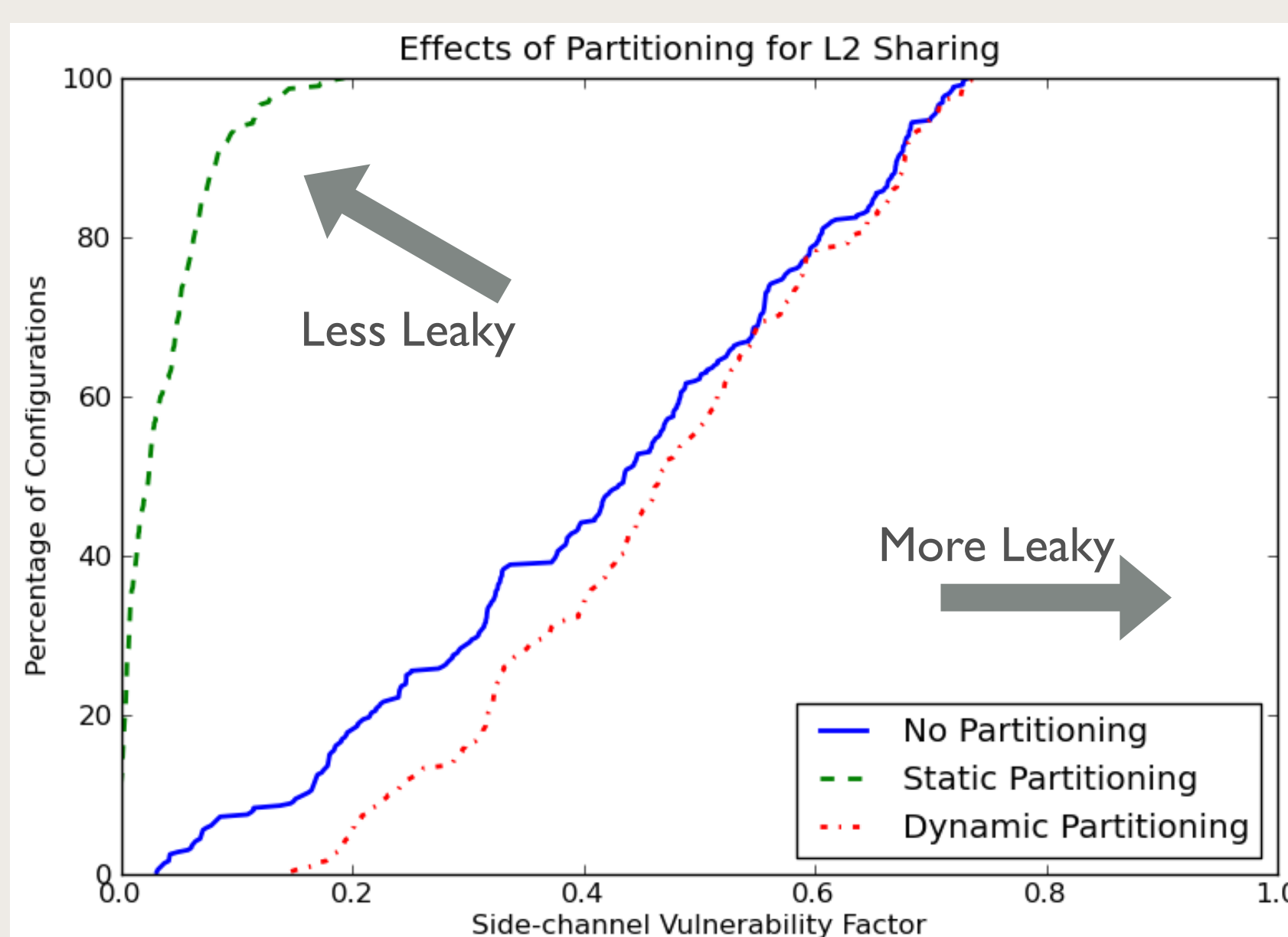
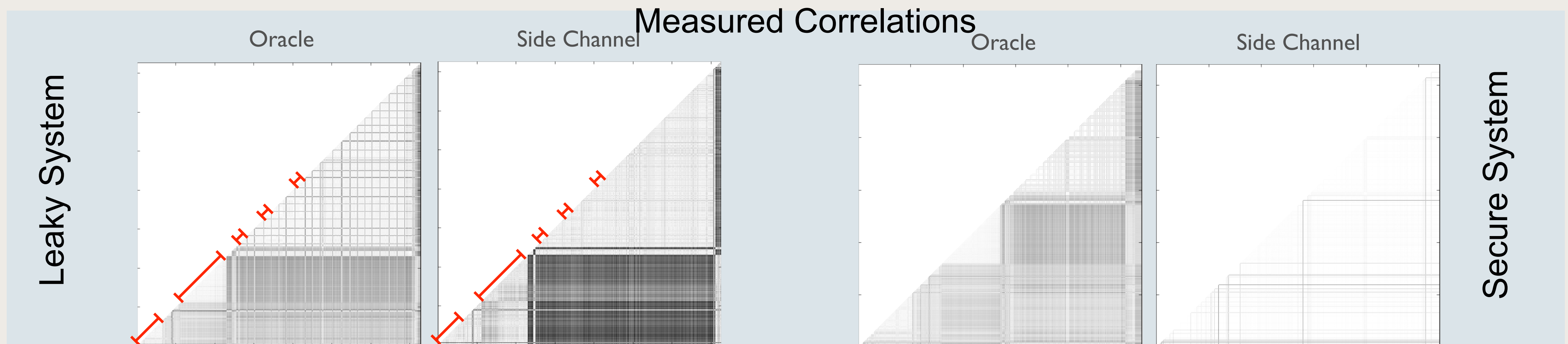
Side Channel Vulnerability Factor

is the **correlation** between:

patterns in attacker observations
and
patterns in victim's execution.



Allows early design-phase leakage analysis, e.g., using processor simulators.



Some Surprising Simulation Results

Static partitioning of some resources is not helpful.

Dynamic partitioning can hurt.

Performance & security need not always be tradeoffs



2012 Science of Security

Community Meeting

Nov. 29-30, 2012

National Harbor, MD

<http://cps-vo.org/group/sosmtg>

Vote Here

