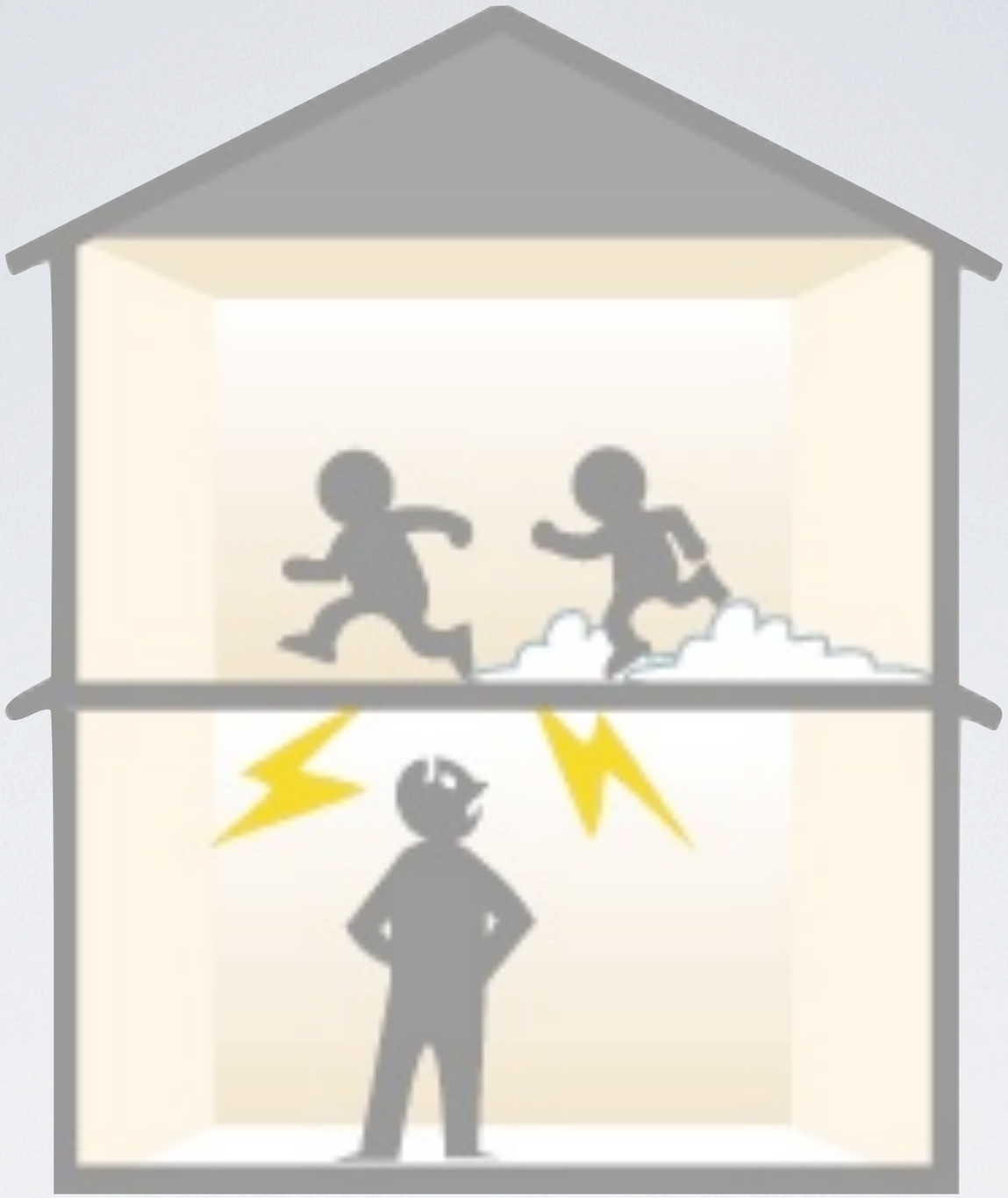
Side-channel Vulnerability Factor:
A Metric for Measuring Information Leakage

John Demme, Robert Martin,
Adam Waksman, and Simha Sethumadhavan

Computer Architecture and Security Technologies Lab
Columbia University

Information Leakage



Information Leakage

Information Leakage in Computing Systems

"Alice" uses the cloud

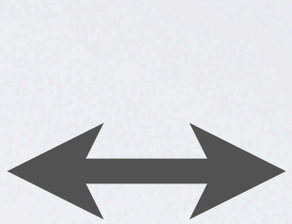
Network

Servers

Information Leakage in Computing Systems

"Alice" uses the cloud

Network

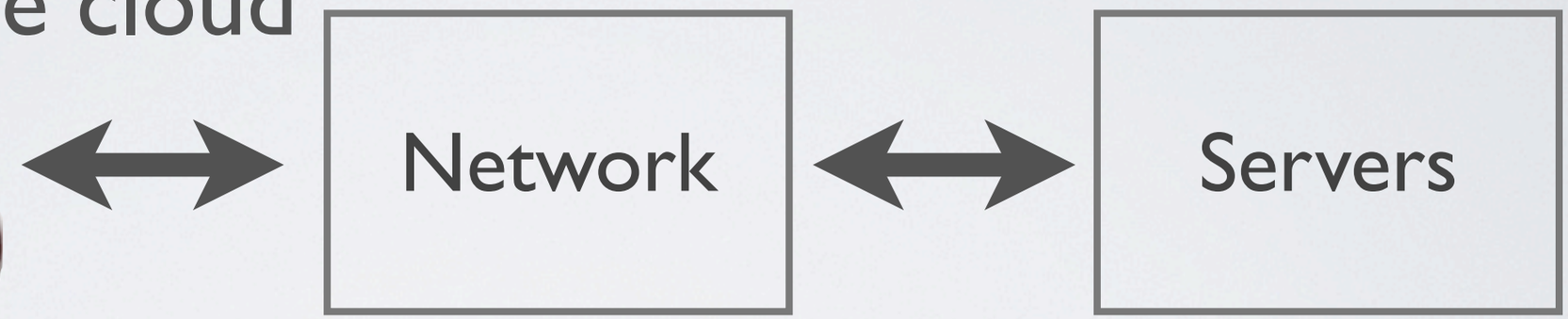


Servers

Information leakage can create side channels

Information Leakage in Computing Systems

"Alice" uses the cloud

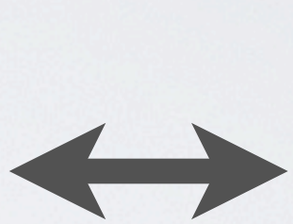


"Bob" also uses the cloud

Information Leakage in Computing Systems

"Alice" uses the cloud

Network



Servers

"Bob" also uses the cloud

Demonstrated Network Attacks

HTTPS, Skype

Information Leakage in Computing Systems

"Alice" uses the cloud

Network

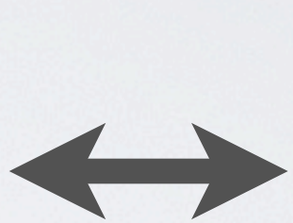
Servers

"Bob" also uses the cloud

Information Leakage in Computing Systems

"Alice" uses the cloud

Network



Servers

"Bob" also uses the cloud

Demonstrated CPU Attacks

SSH, OpenSSL

Big Problem

Side channels are unquantified.

Therefore, they are dangerous.

Contributions:

a Quantitative Approach

Contributions:
a Quantitative Approach

Given systems S_1, S_2:

Security (S_1) > Security(S_2) ?

Contributions:
a Quantitative Approach

Given systems S_1, S_2:

Security (S_1) > Security(S_2) ?

Allows performance-security tradeoffs

Outline

- Side-channels101
- Measuring Side-channels
- Cache systems: a case study
- Future work

Types of Side-Channels

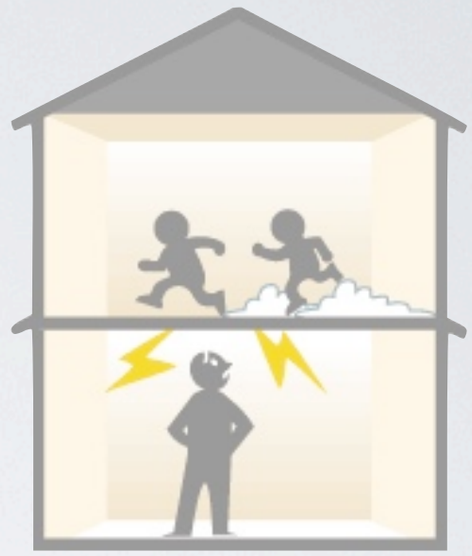
Side Channels

Types of Side-Channels

- Side Channels
  - Analog

Types of Side-Channels

- Side Channels
  - Analog
    - Acoustic



Types of Side-Channels

Side Channels

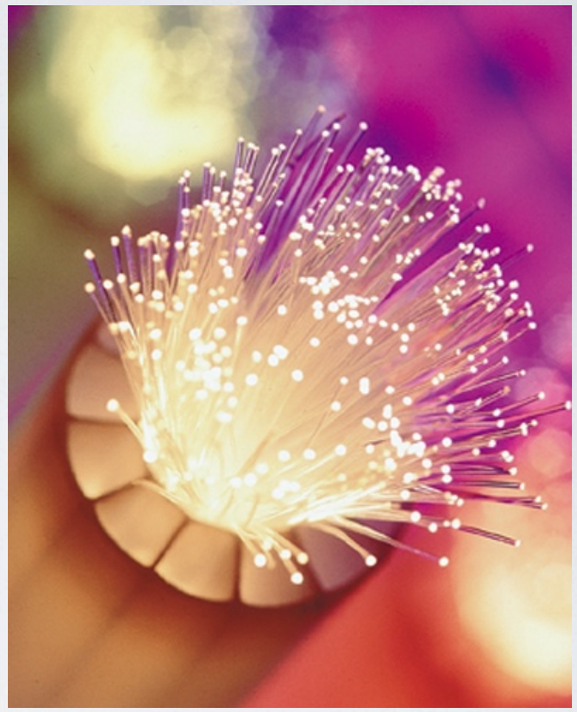
- Analog
- Acoustic

[Asonov et al. 2004]

[Backes et al. 2010]

Types of Side-Channels

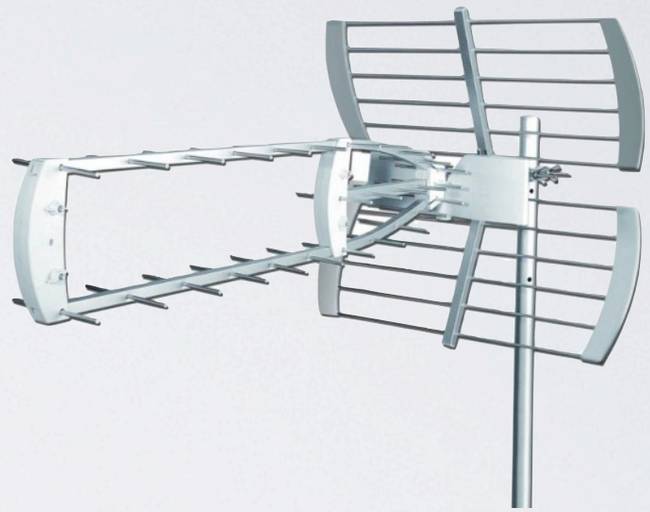
- Side Channels
  - Analog
    - Acoustic
    - Optical



[Loughry et al. 2002]

Types of Side-Channels

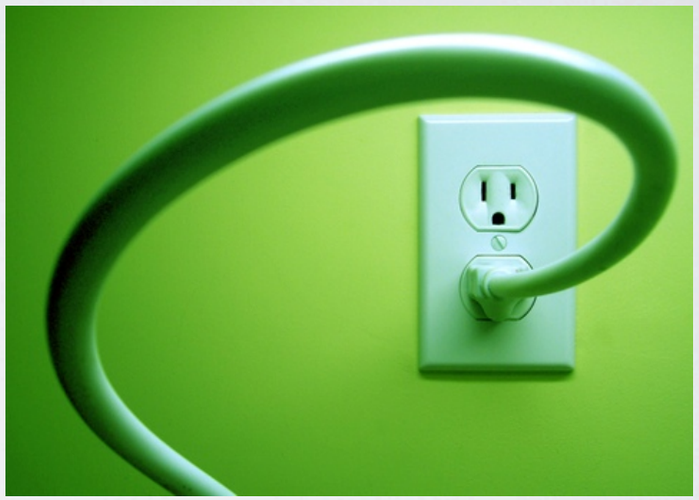
Side Channels
- Analog
  - Acoustic
  - Optical
  - E-M



[Van Eck et al. 1985]

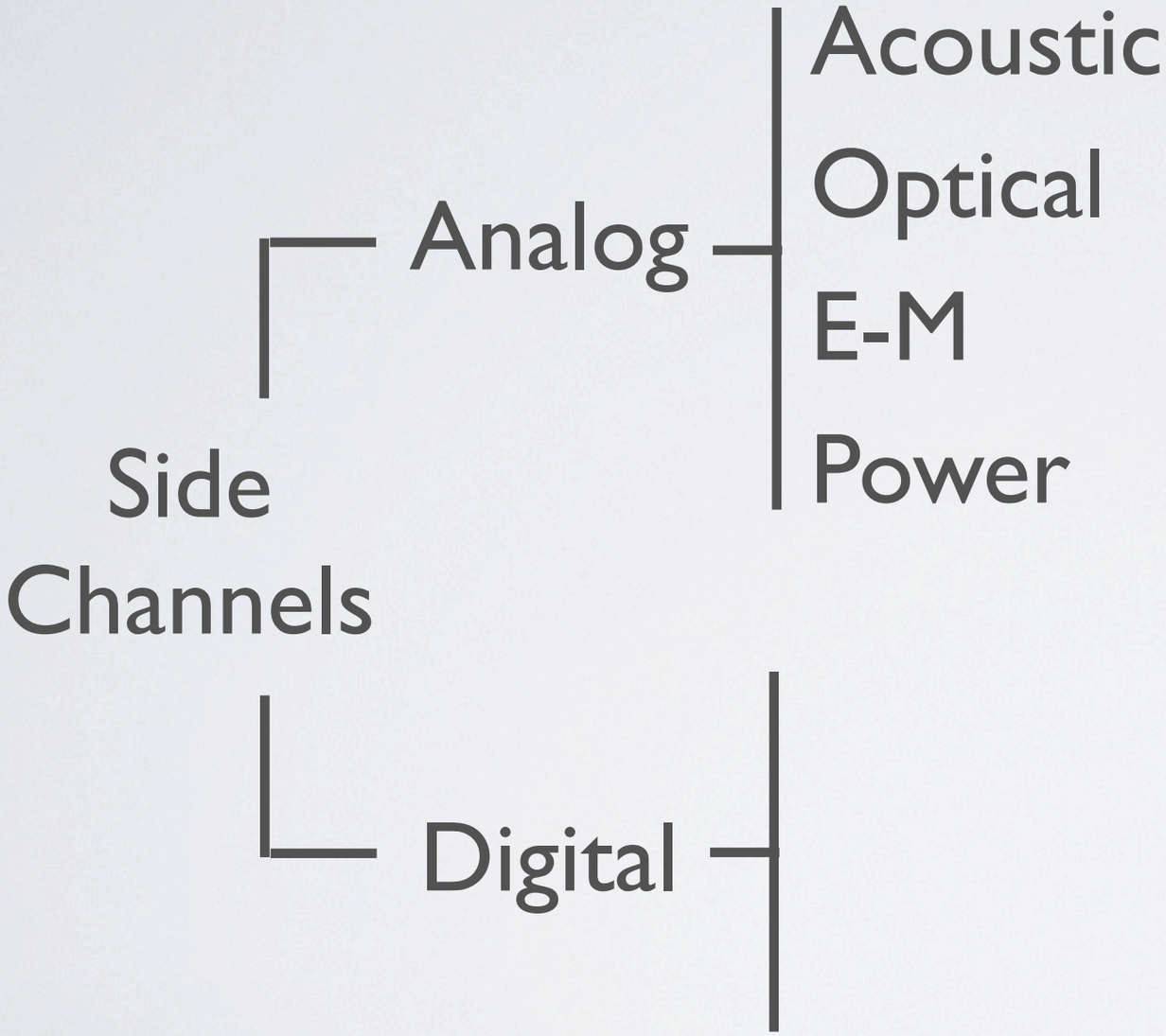
Types of Side-Channels

- Side Channels
  - Analog
    - Acoustic
    - Optical
    - E-M
    - Power



[Messerges et al. 1999]

Types of Side-Channels



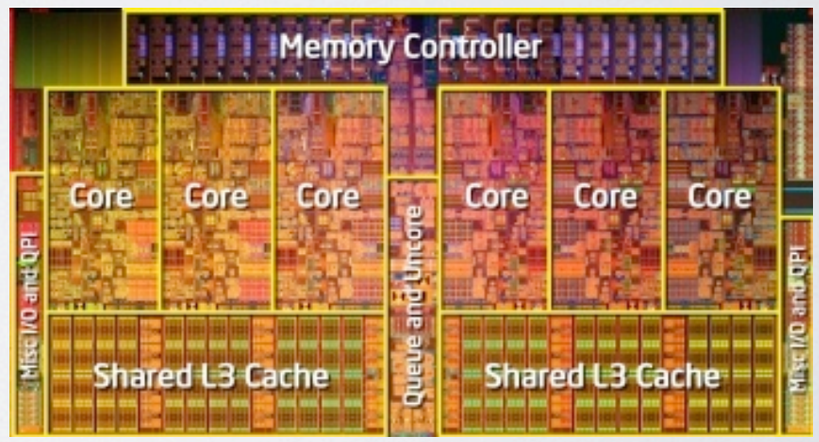
Types of Side-Channels

- Side Channels
  - Analog
    - Acoustic
    - Optical
    - E-M
    - Power
  - Digital
    - Shared Network

[Chen et al. 1999]

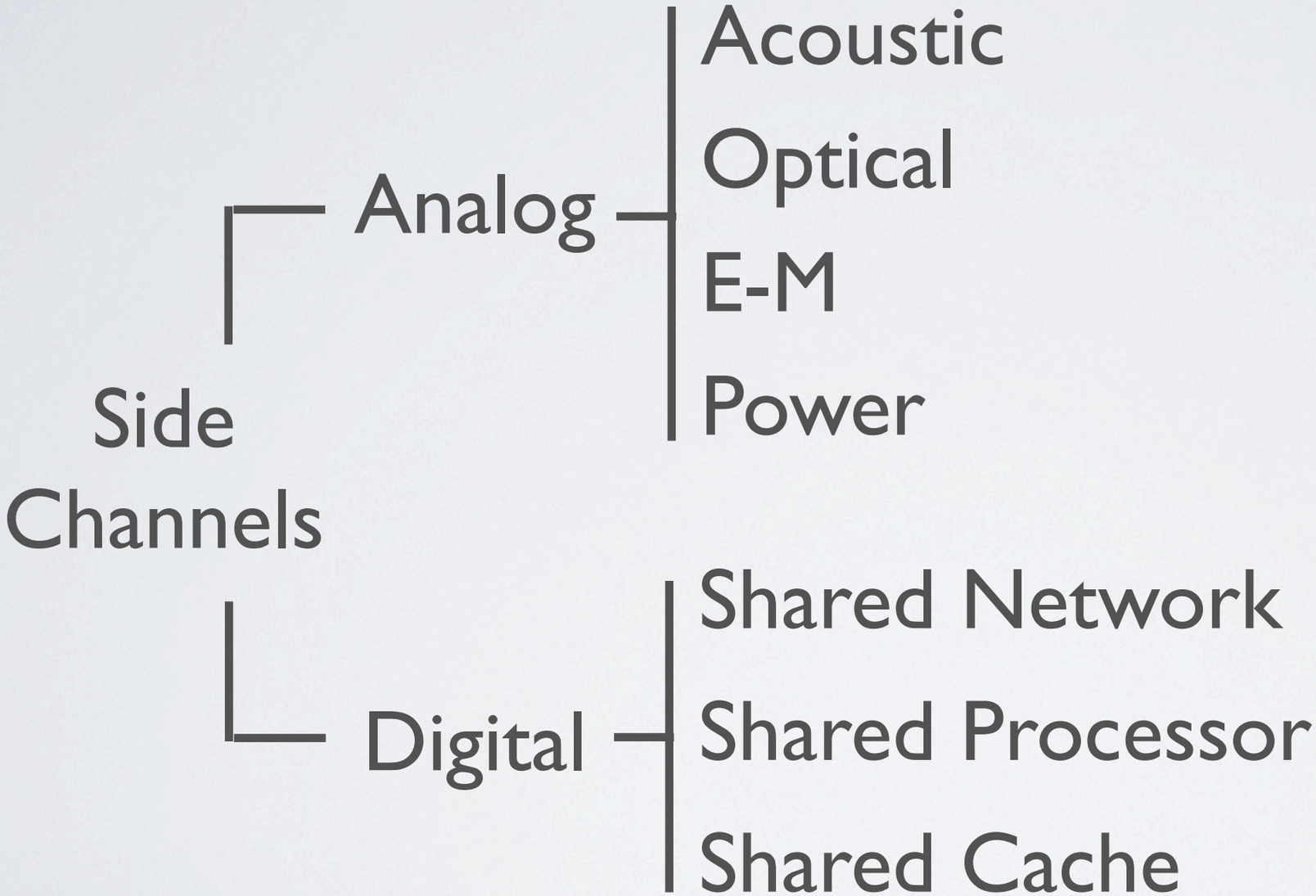
Types of Side-Channels

- Side Channels
  - Analog
    - Acoustic
    - Optical
    - E-M
    - Power
  - Digital
    - Shared Network
    - Shared Processor
    - Shared Cache

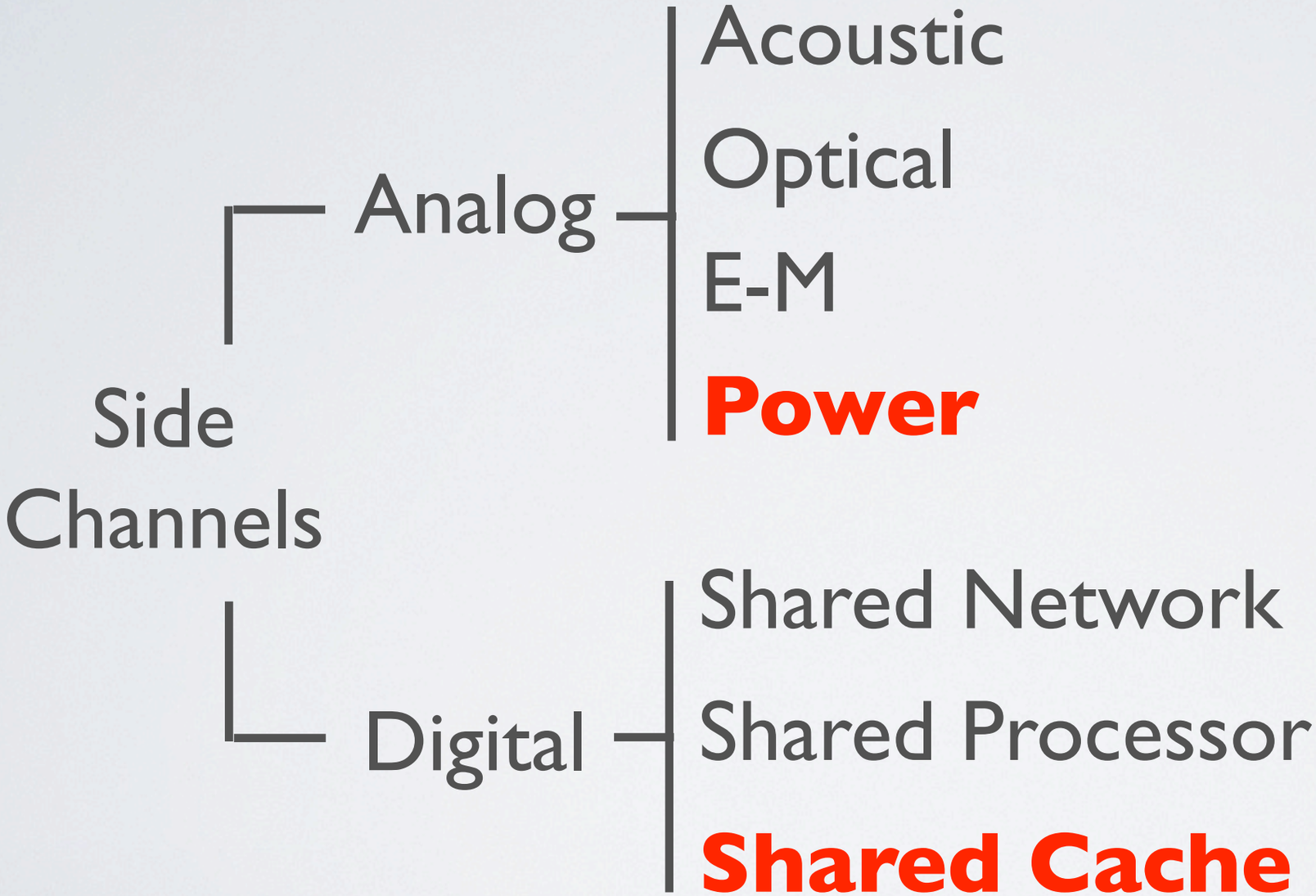


[Gullasch et al. 1999]

Types of Side-Channels



Types of Side-Channels



Power Side Channels

Power usage during RSA encryption operation

Image credit: Cryptography Research, Inc

Power spikes for periods at seemingly random points

Power Side Channels

Power usage during RSA encryption operation

Image credit: Cryptography Research, Inc

Power Side Channels

Power usage during RSA encryption operation

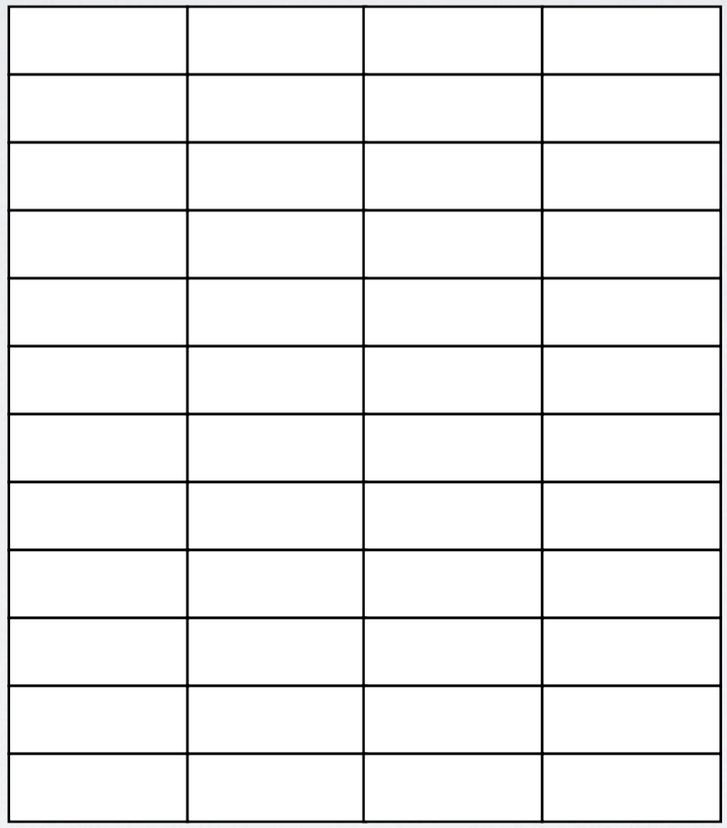
Image credit: Cryptography Research, Inc

Attackers look for correlation between secret key & observed patterns

Cache Side Channels

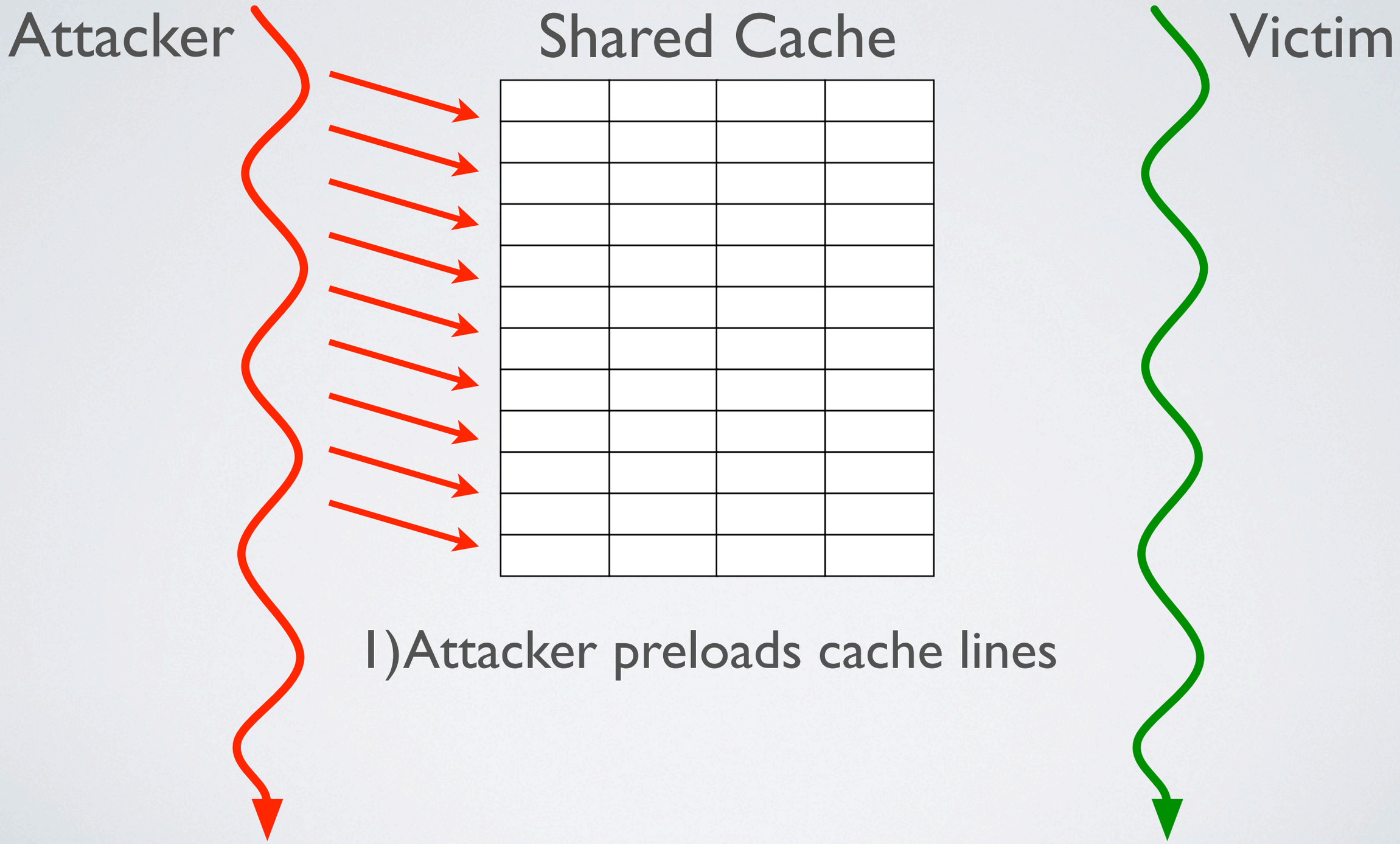
Attacker

Shared Cache



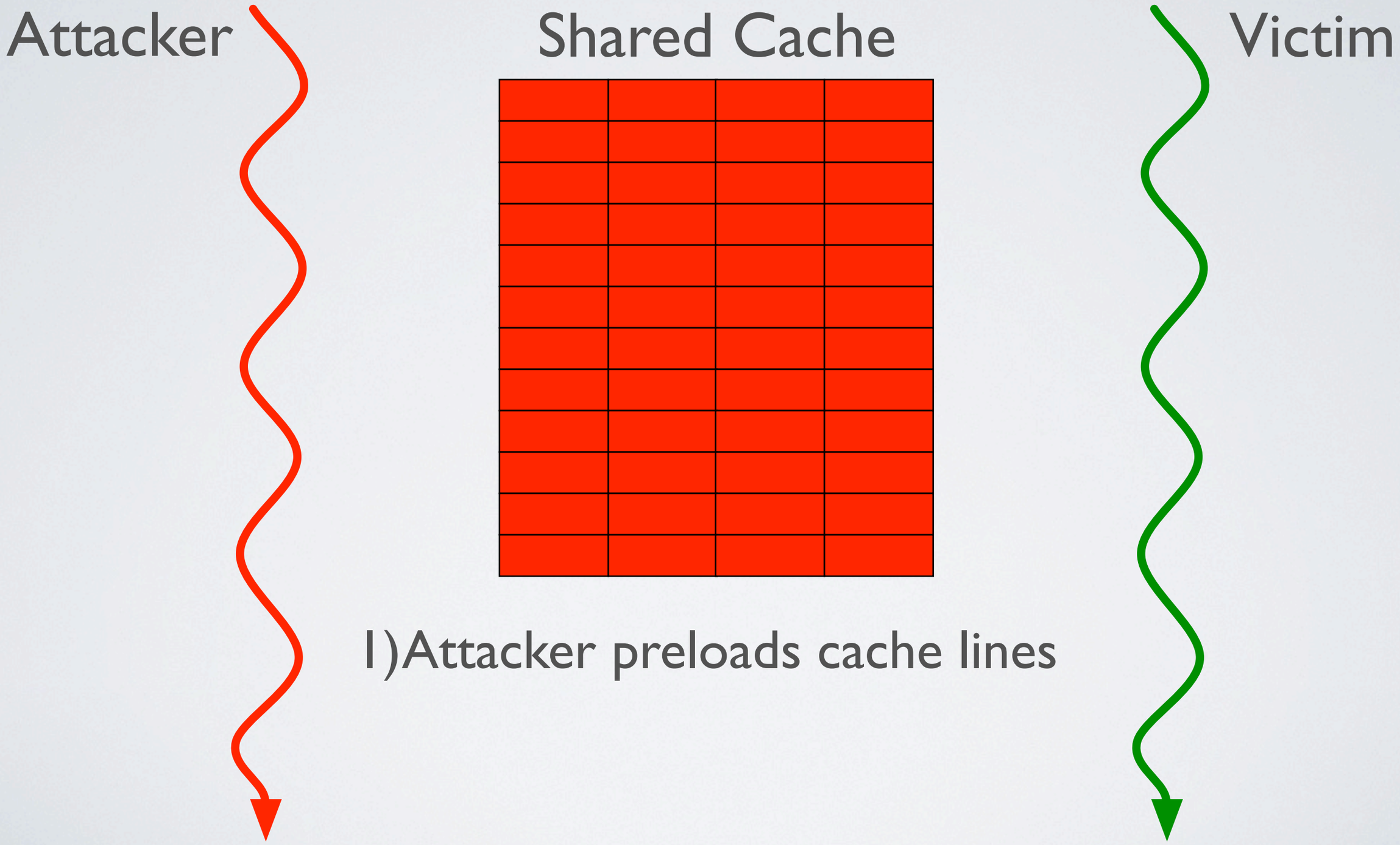
Victim

Cache Side Channels



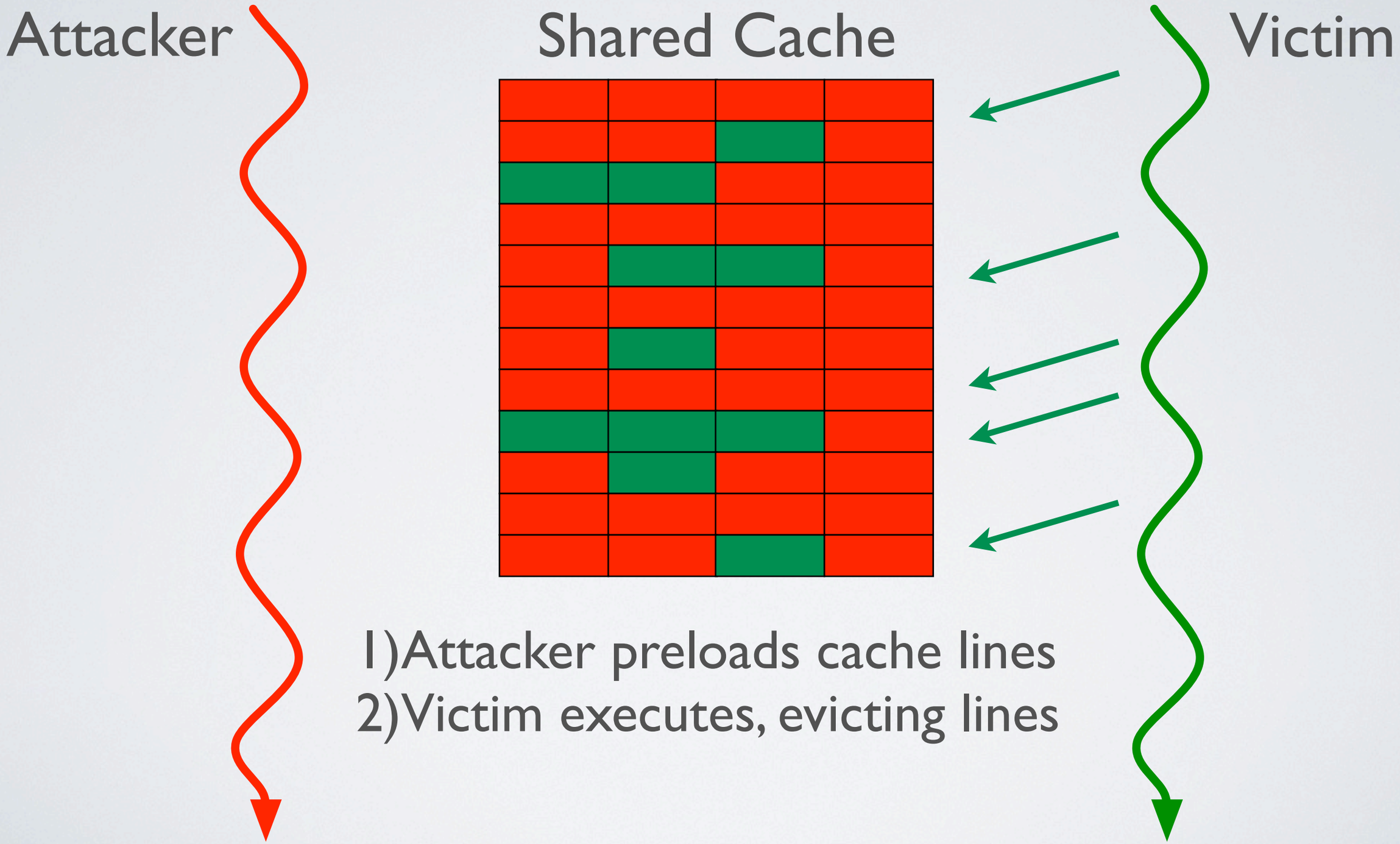
1) Attacker preloads cache lines

Cache Side Channels



1) Attacker preloads cache lines

Cache Side Channels

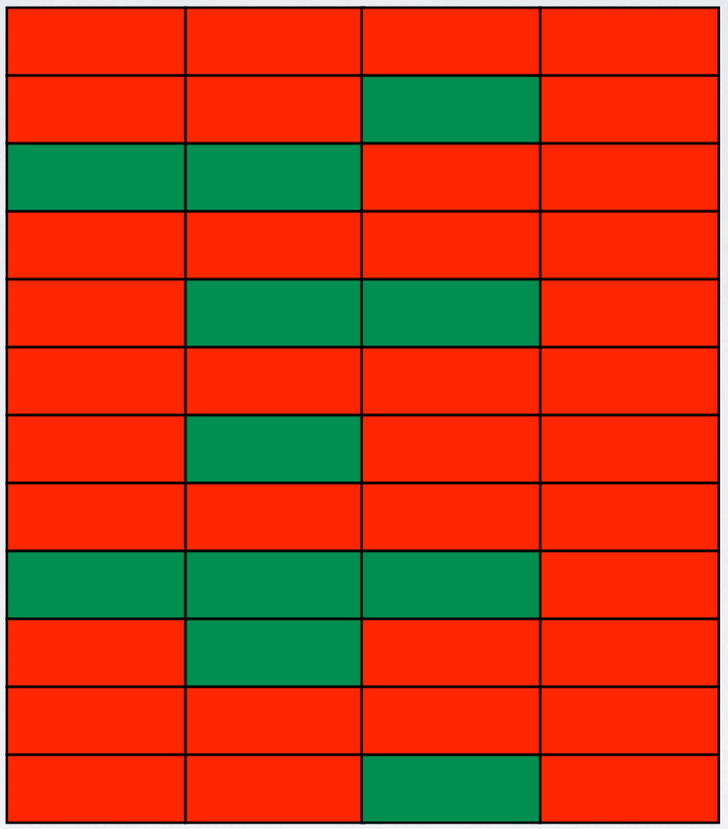


1)Attacker preloads cache lines
2)Victim executes, evicting lines

Cache Side Channels

Attacker

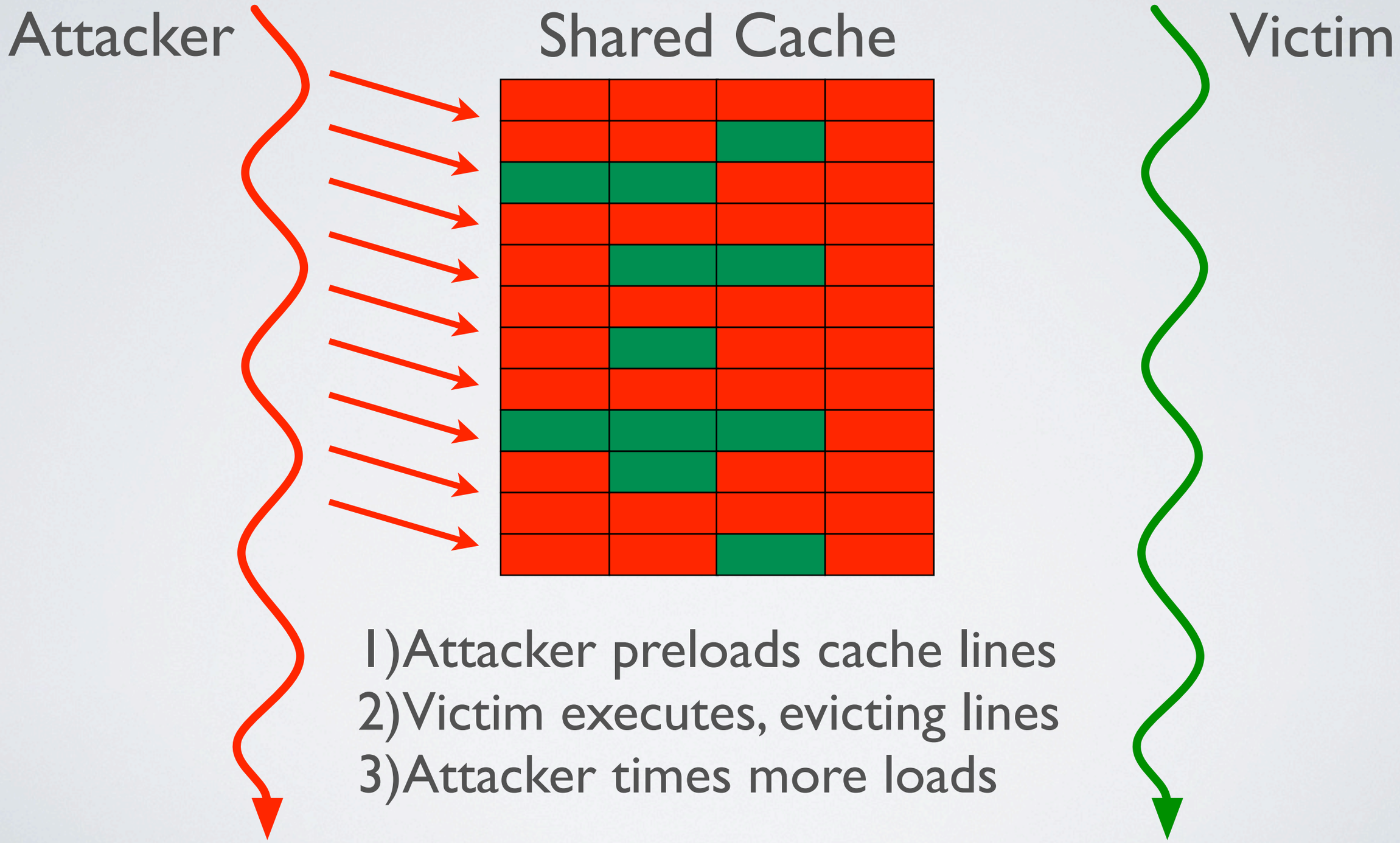
Shared Cache



Victim

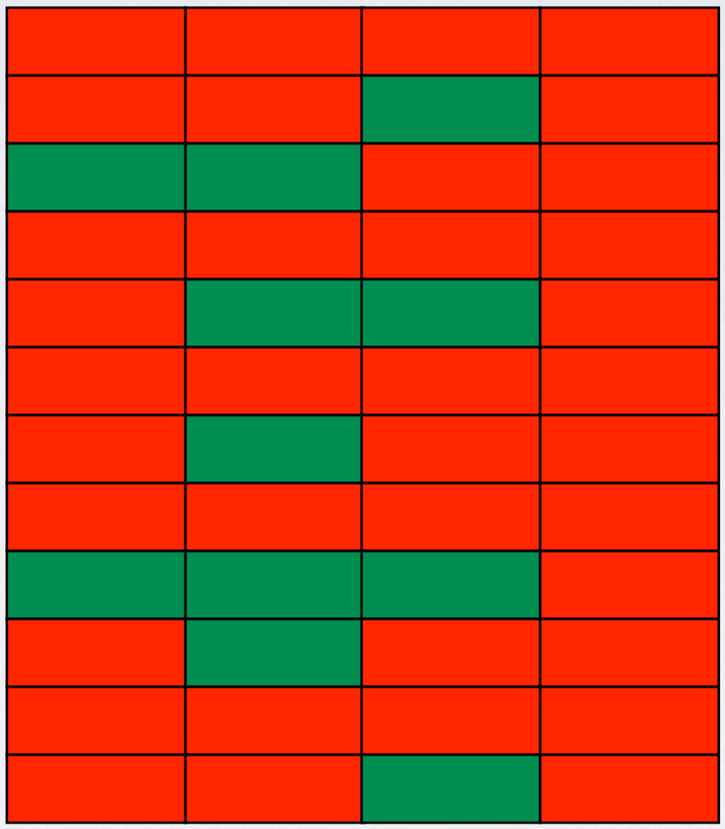
1)Attacker preloads cache lines
2)Victim executes, evicting lines
3)Attacker times more loads

Cache Side Channels



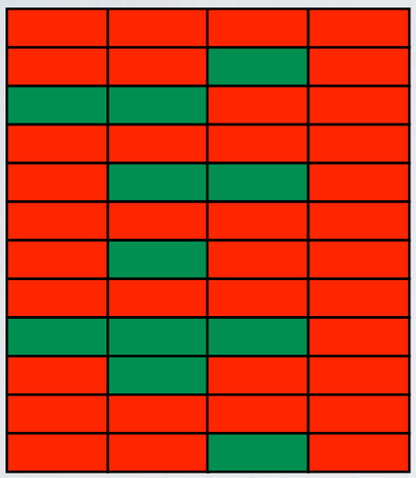
1)Attacker preloads cache lines
2)Victim executes, evicting lines
3)Attacker times more loads

Cache Side Channels



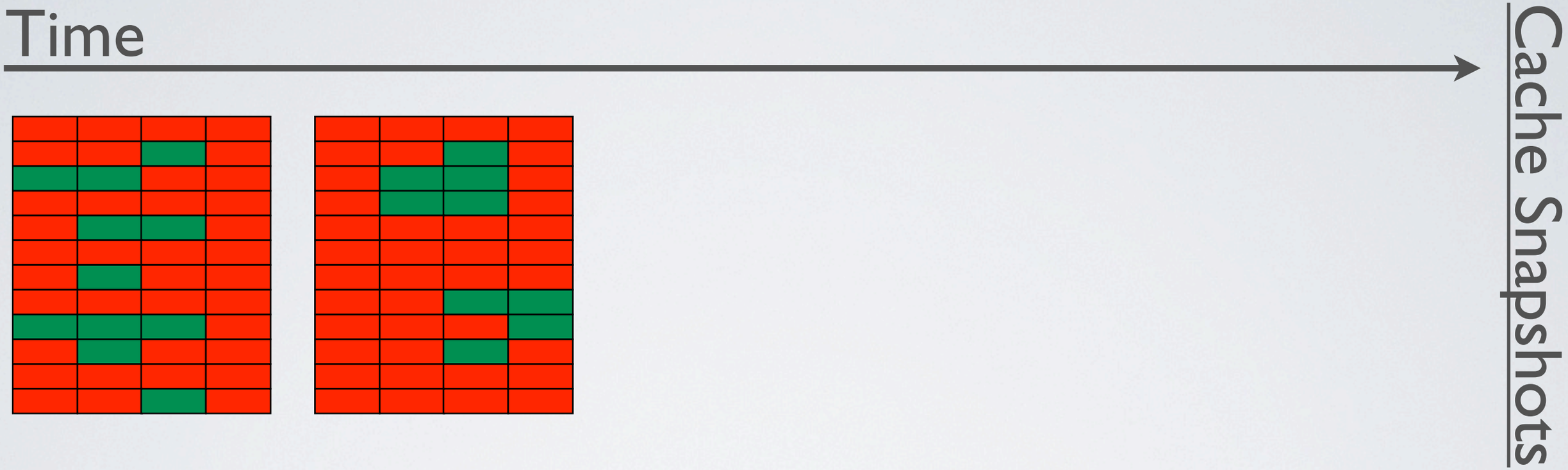
Cache Side Channels

Time

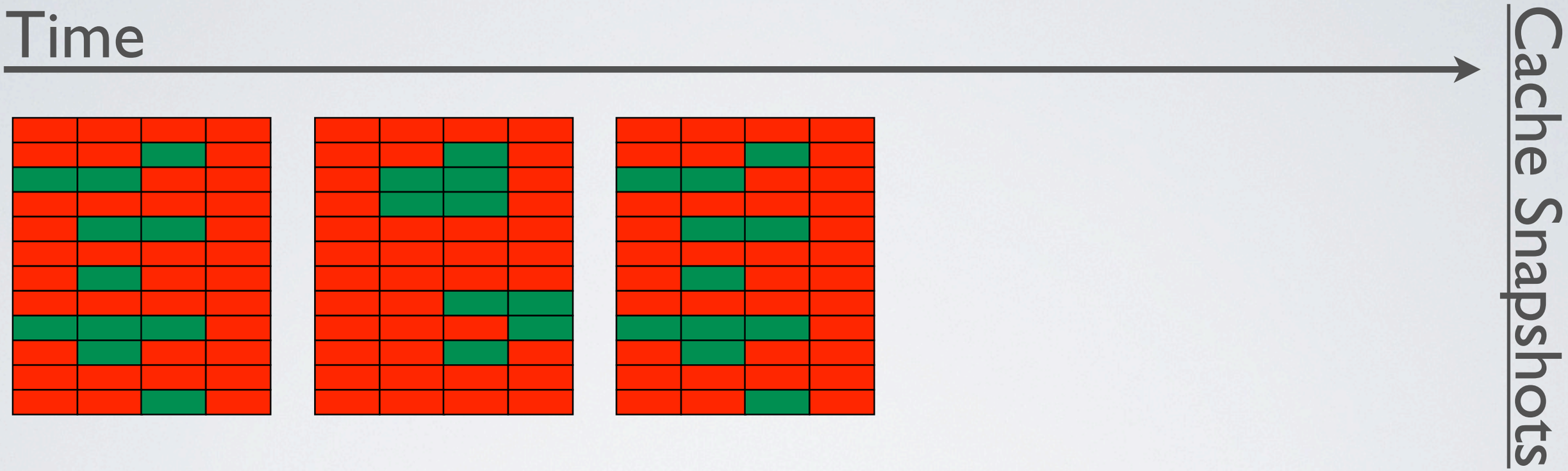


Cache Snapshots

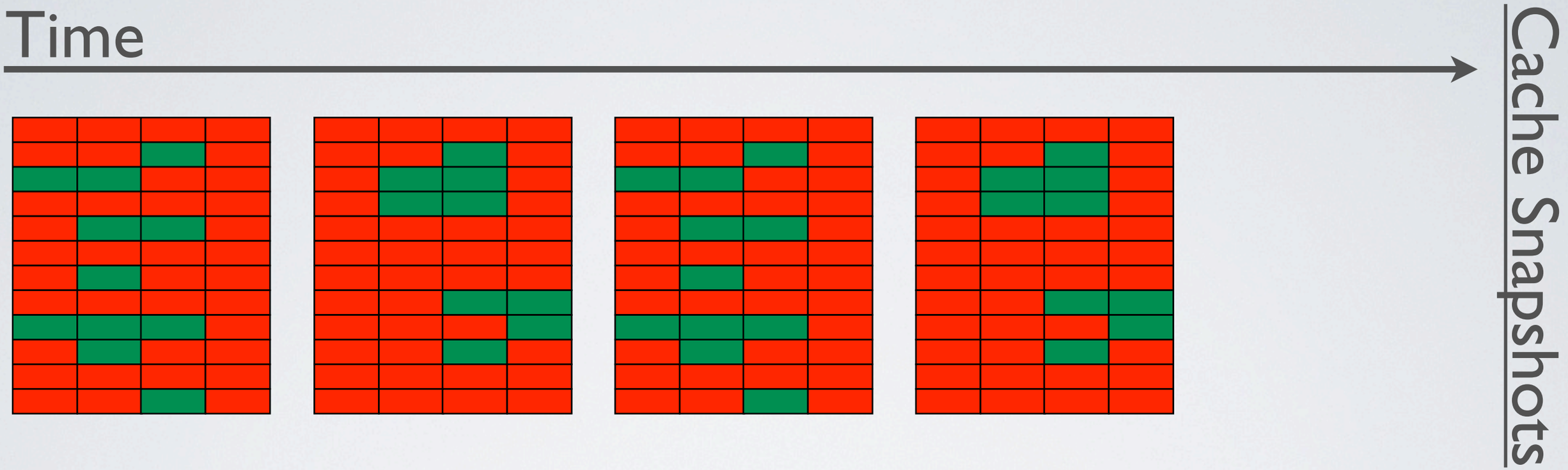
Cache Side Channels



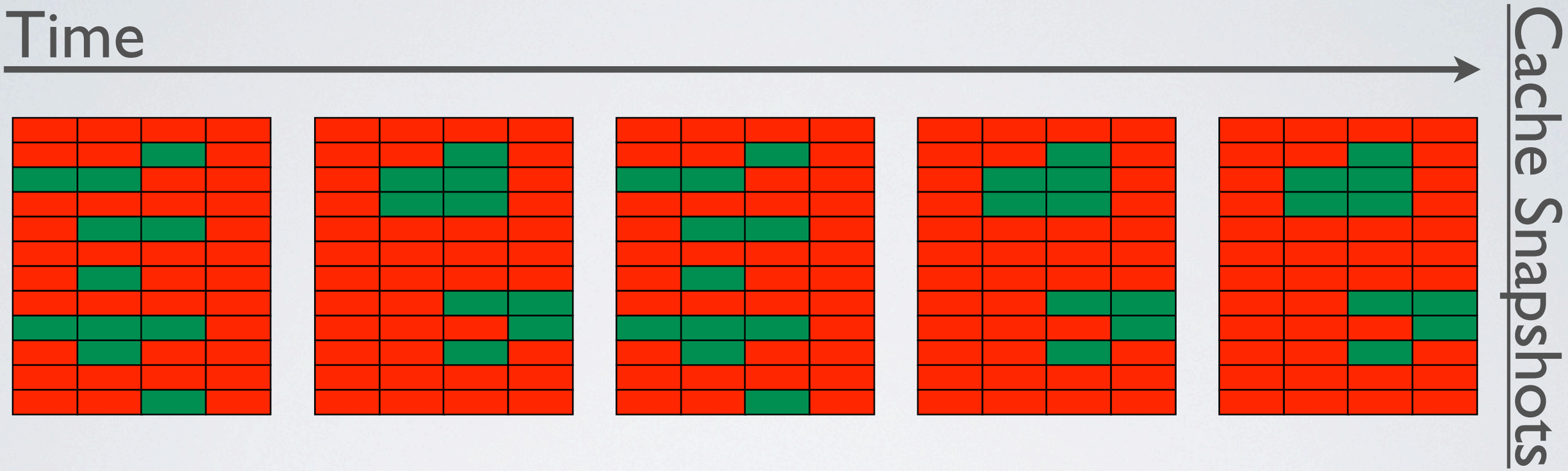
Cache Side Channels



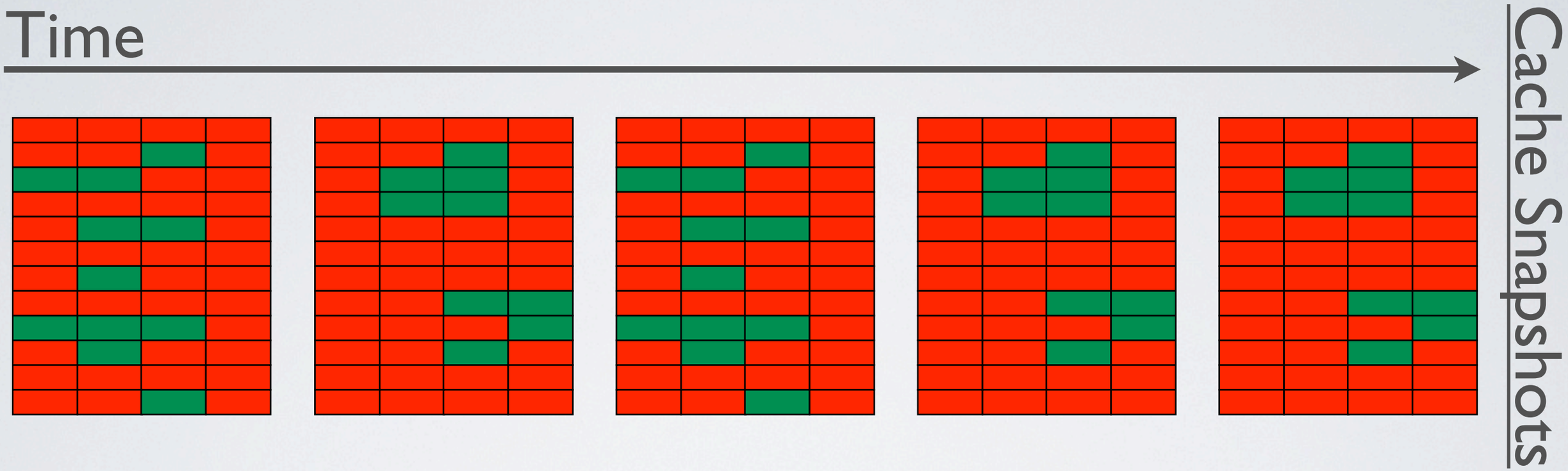
Cache Side Channels



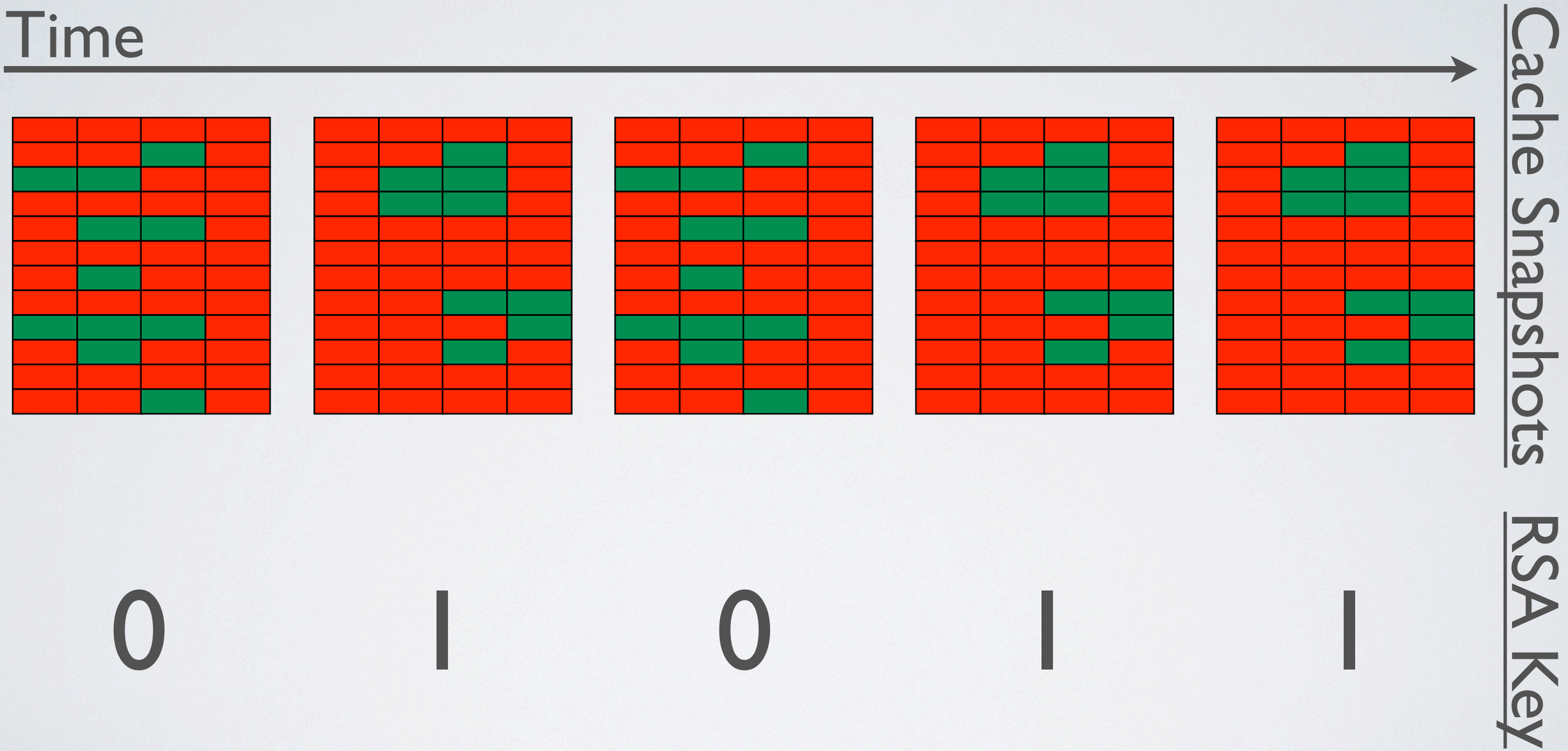
Cache Side Channels



Cache Side Channels



Cache Side Channels



Key Observation

Attackers look for patterns

Side-channel Vulnerability Factor

Measuring information leakage

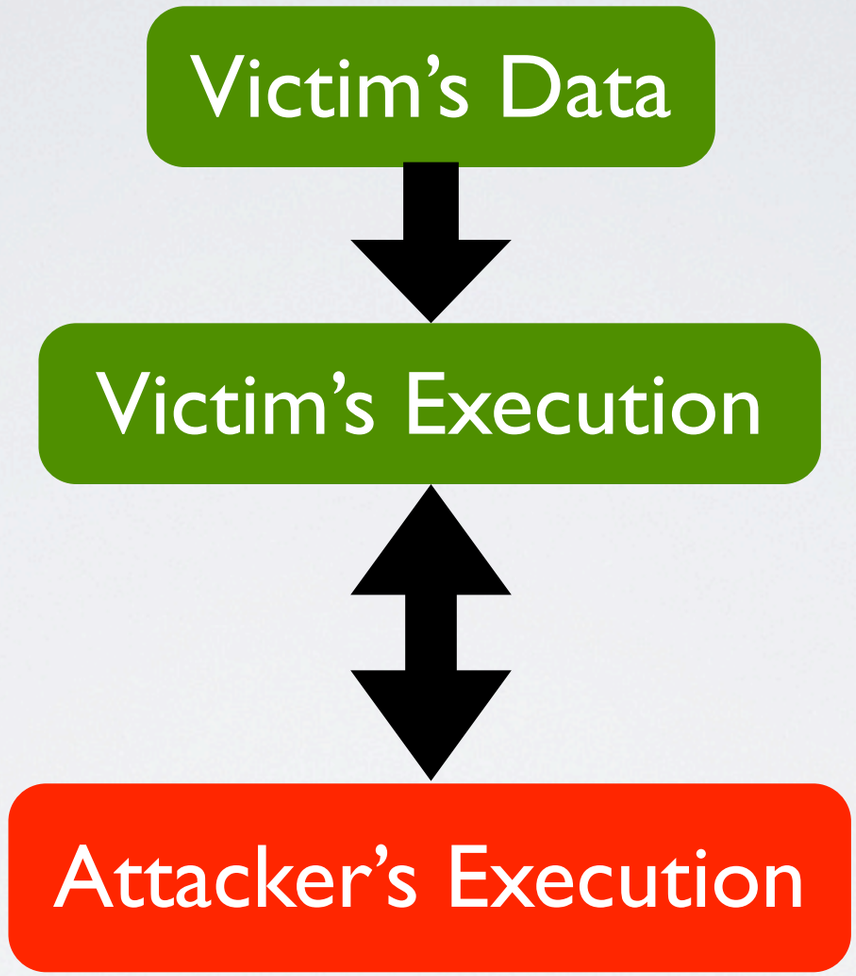
Generalizing Attacks

Generalizing Attacks

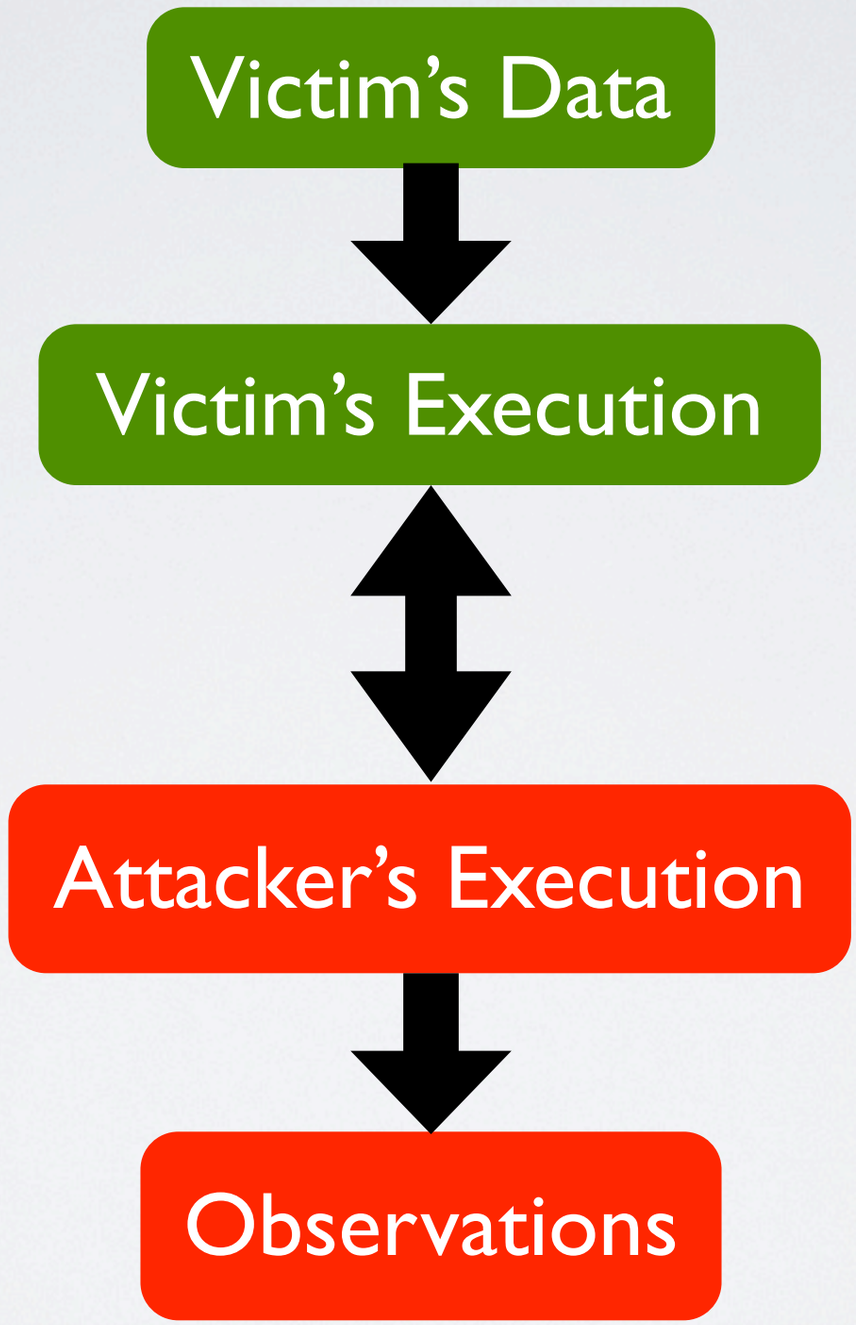
Victim's Data

Generalizing Attacks

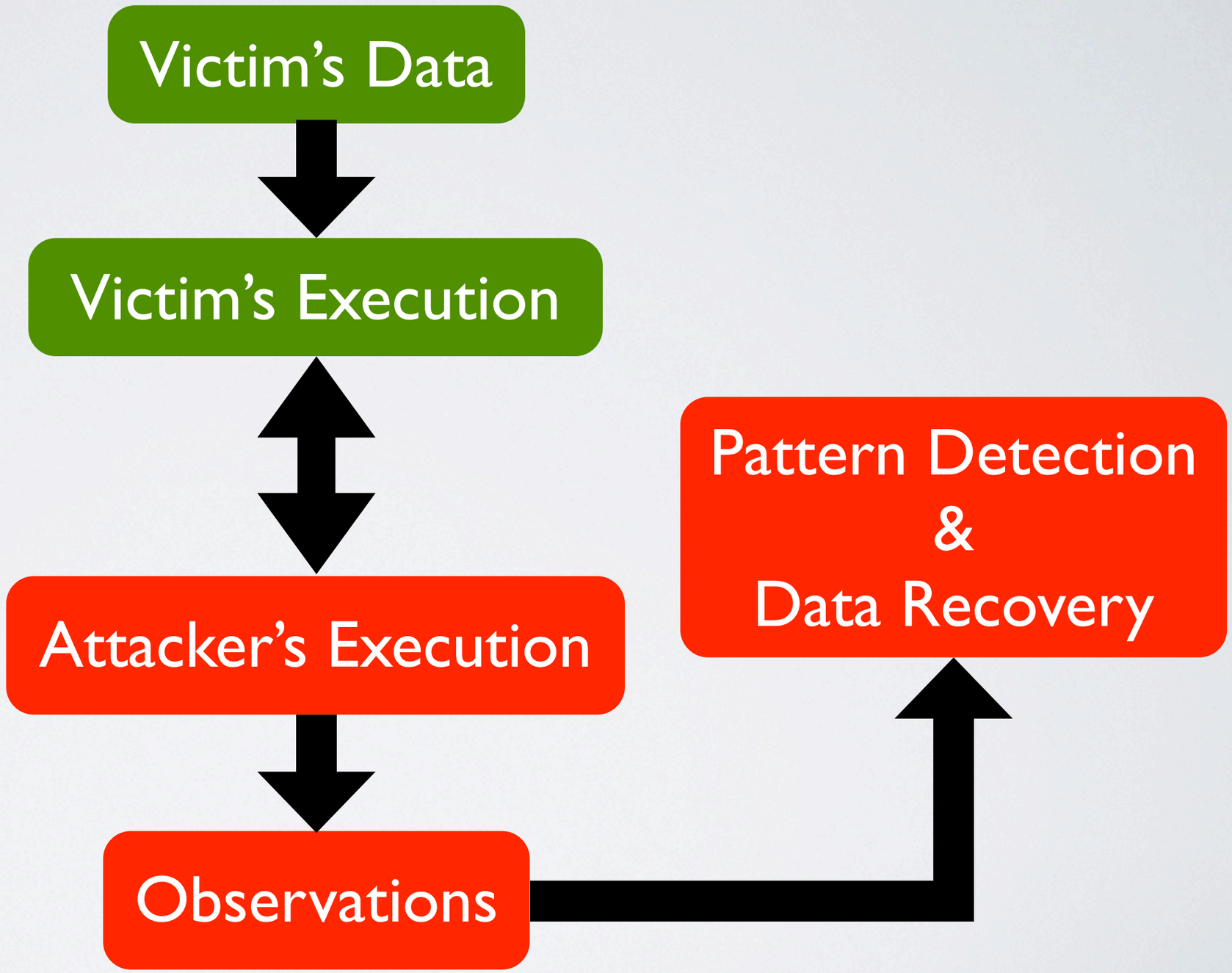
Generalizing Attacks



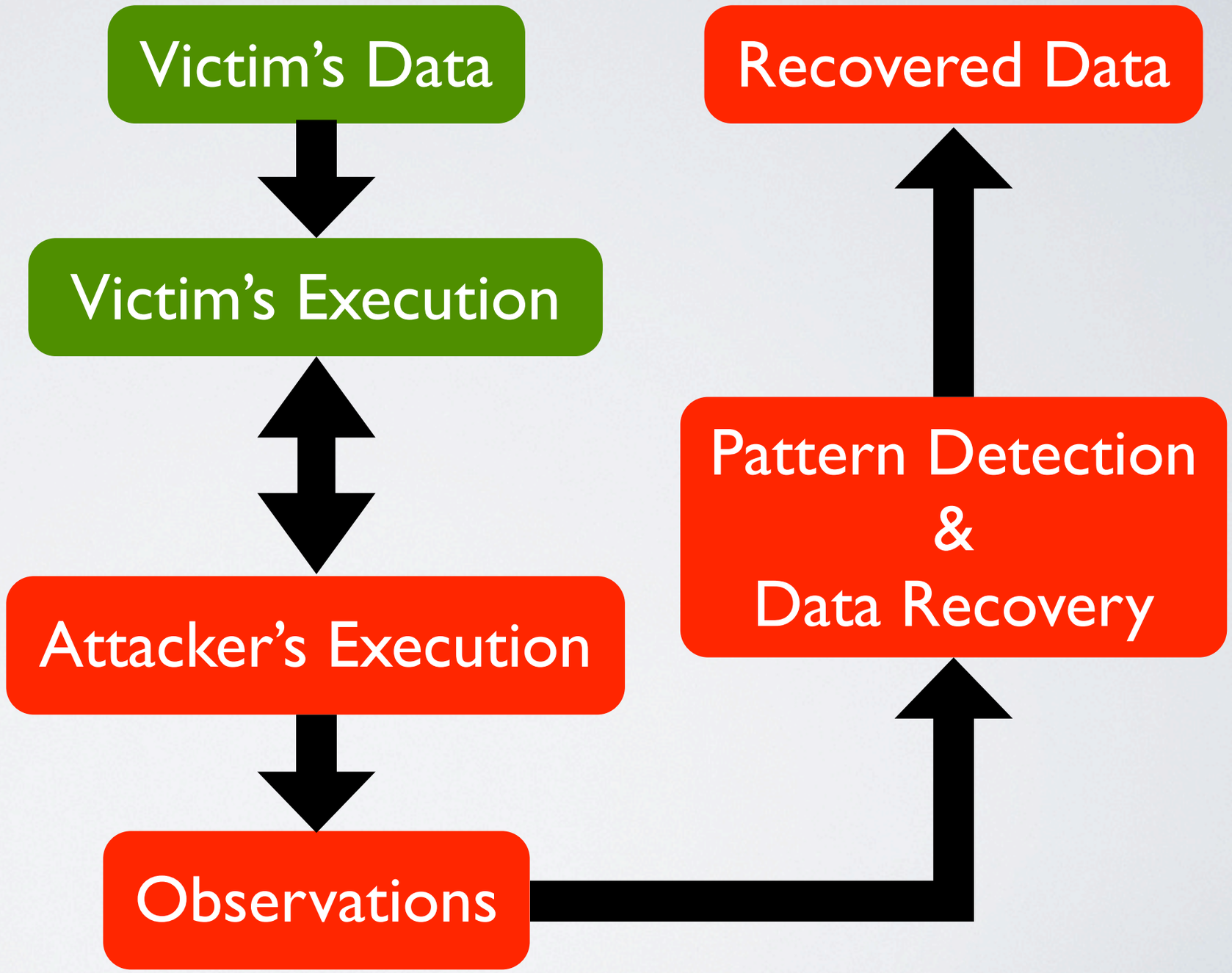
Generalizing Attacks



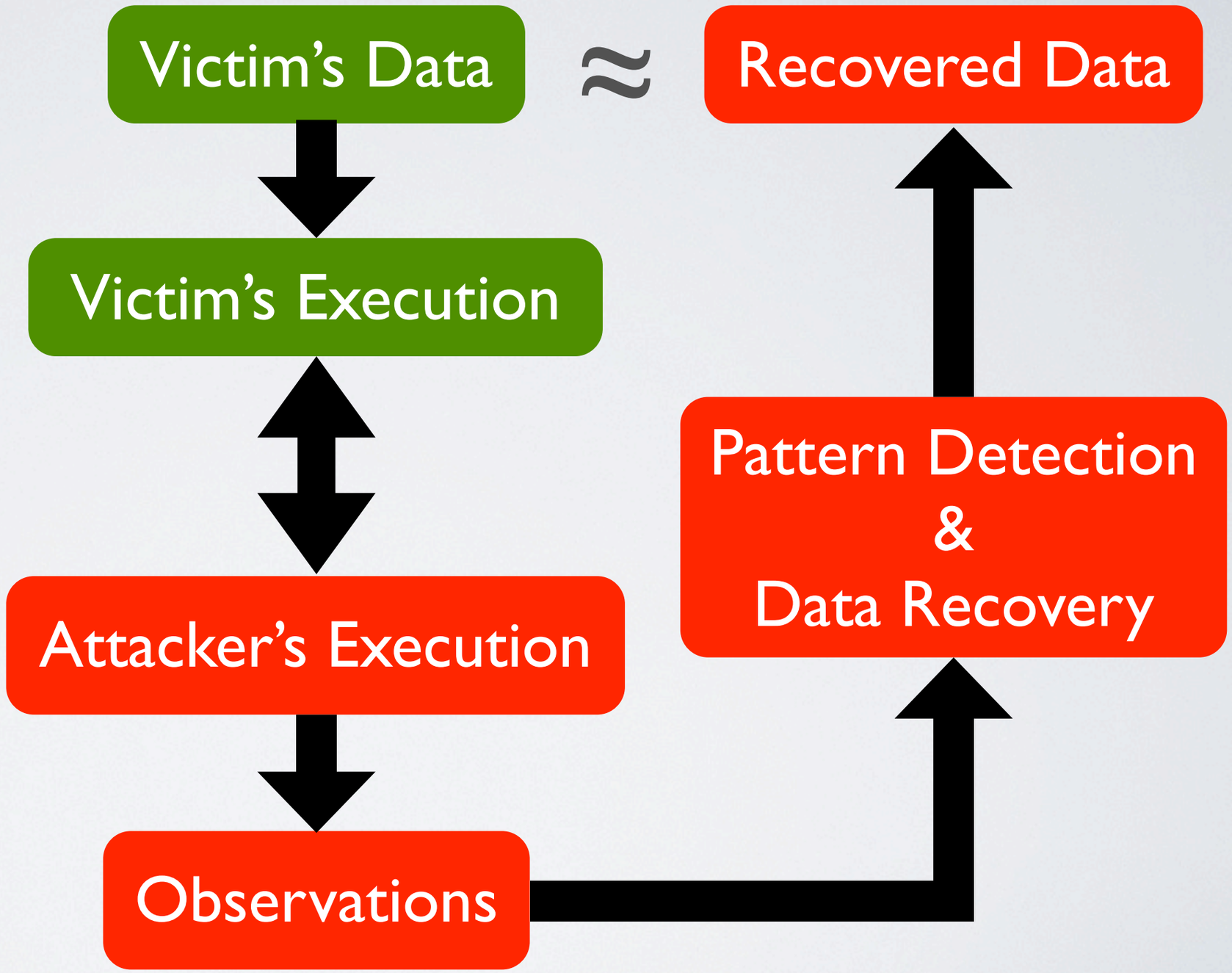
Generalizing Attacks



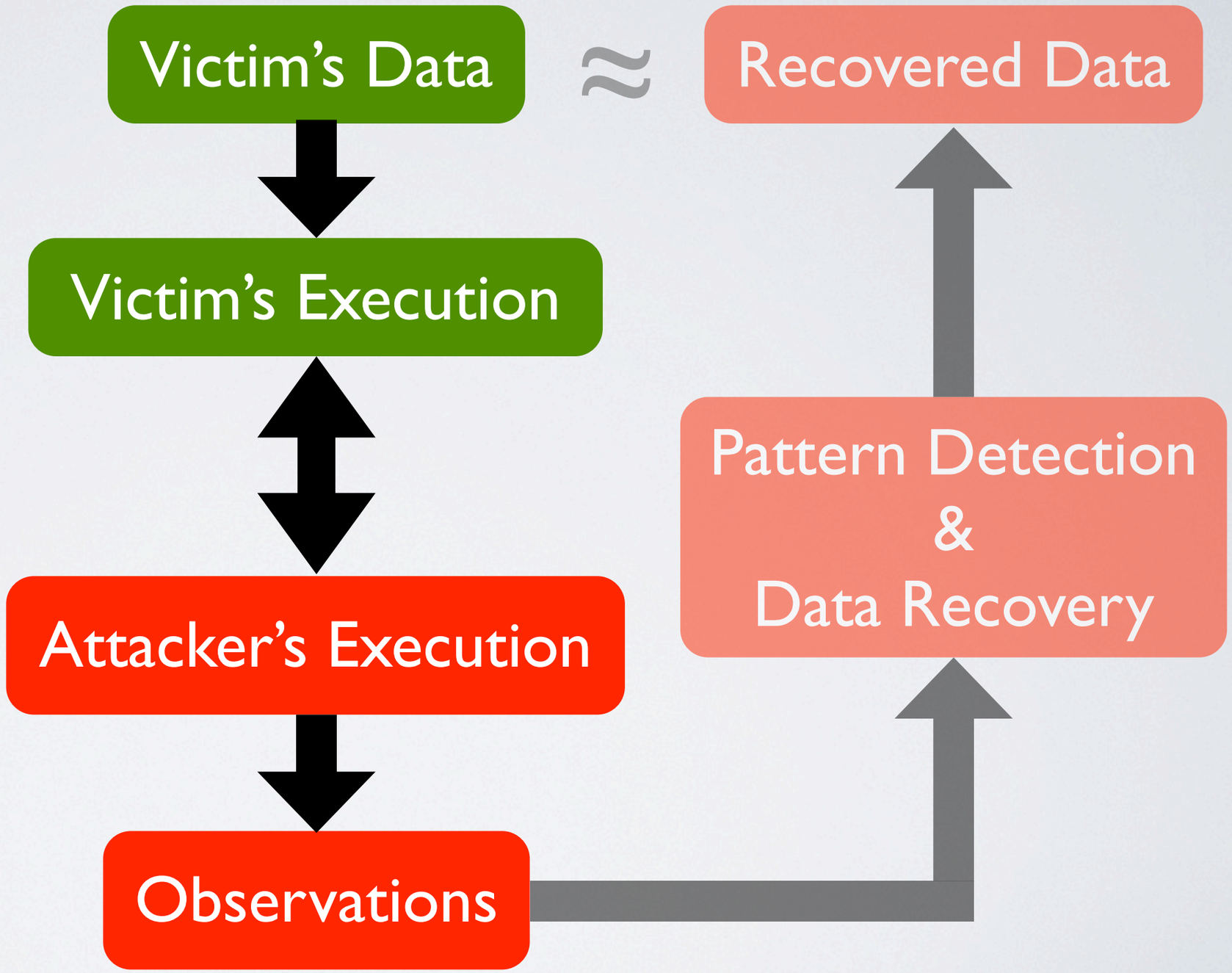
Generalizing Attacks



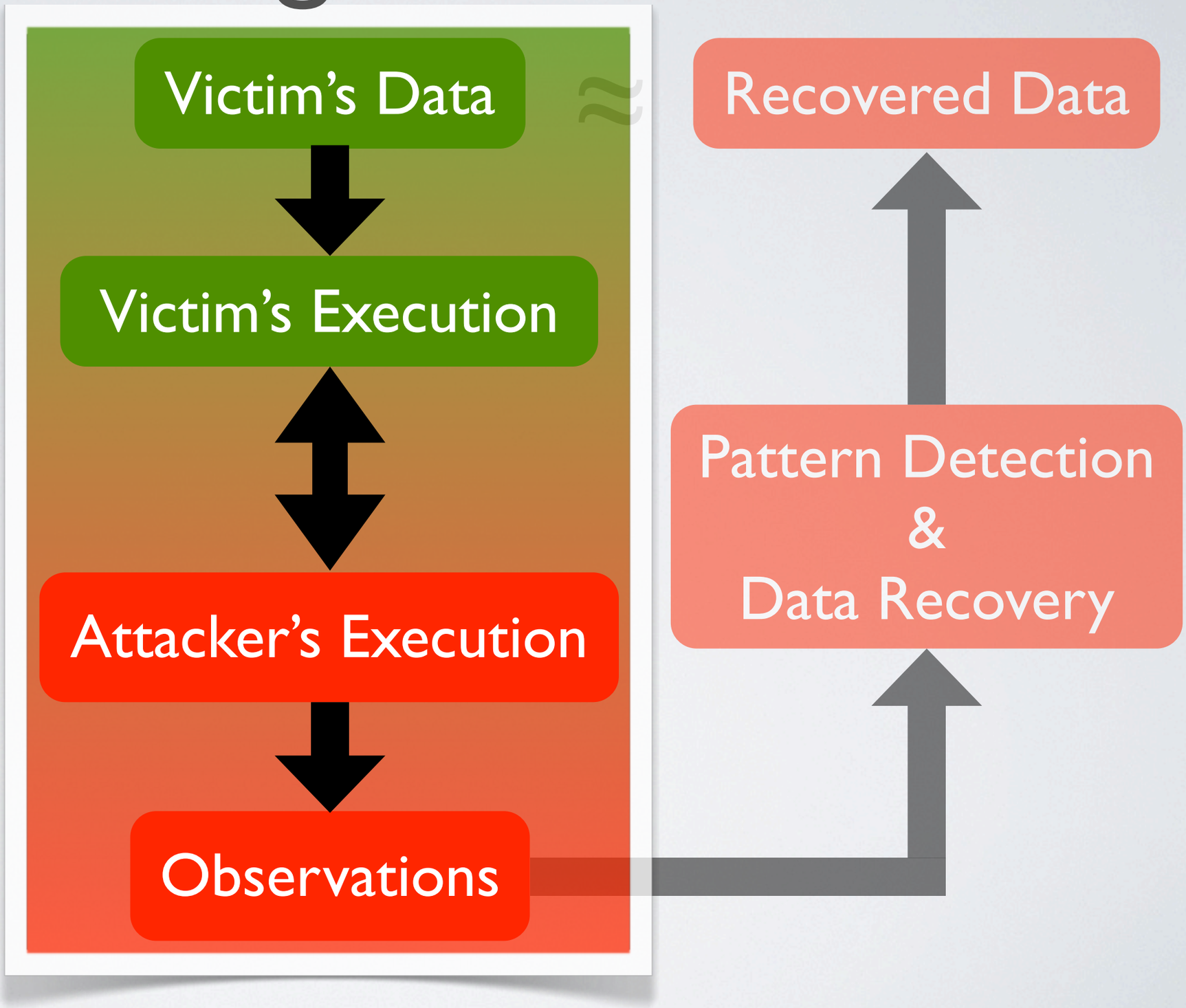
Generalizing Attacks



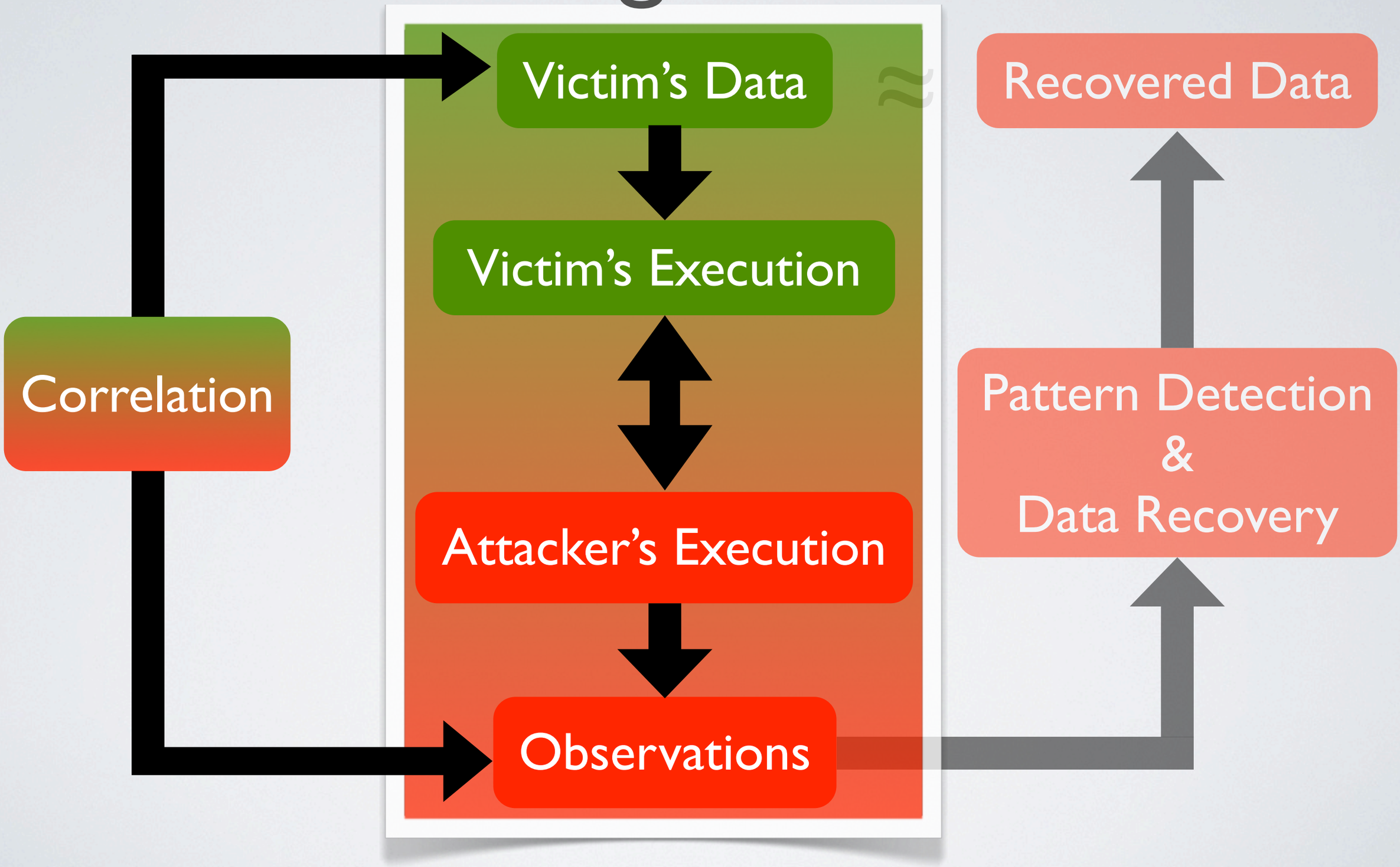
Measuring Leakiness



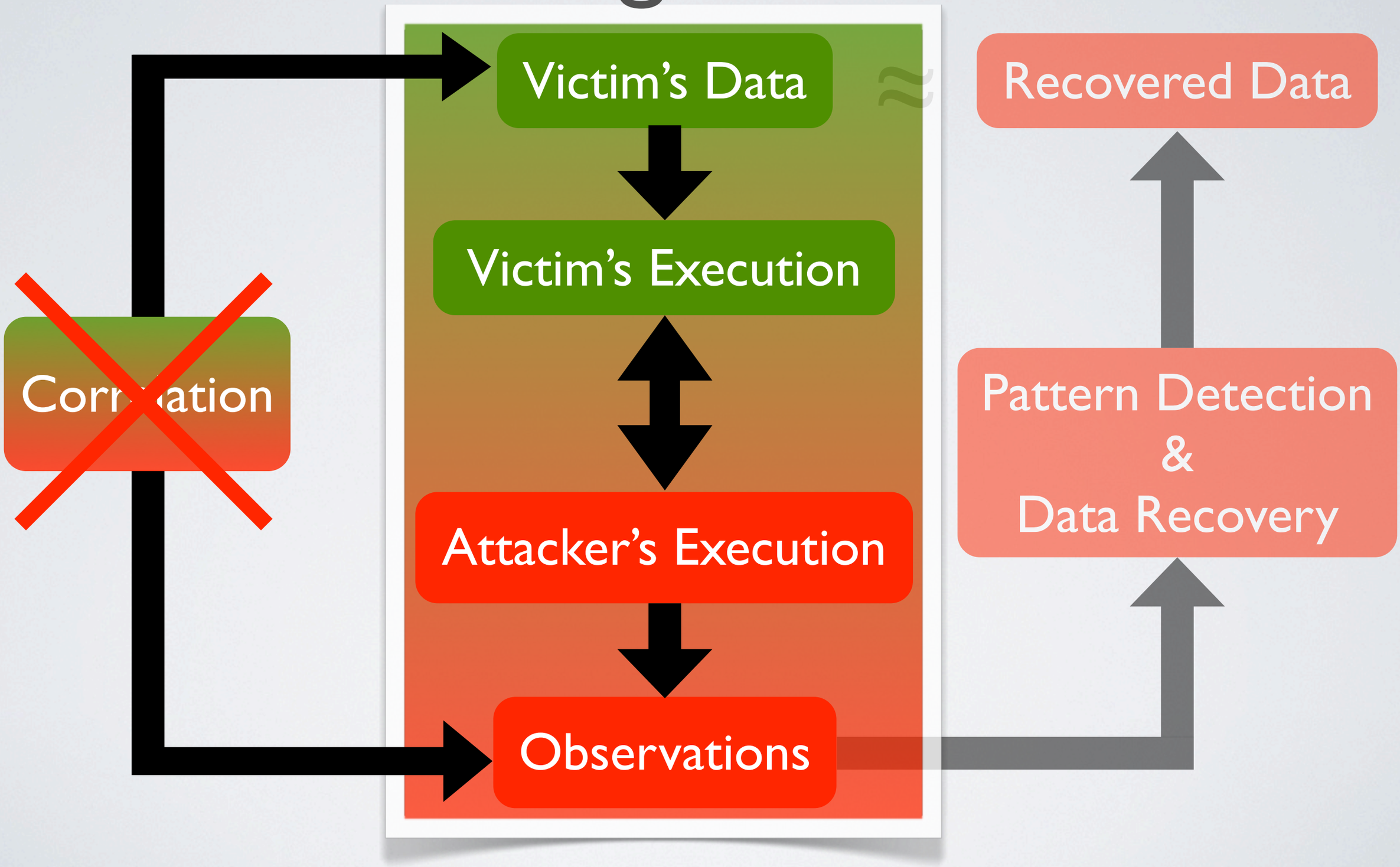
Measuring Leakiness



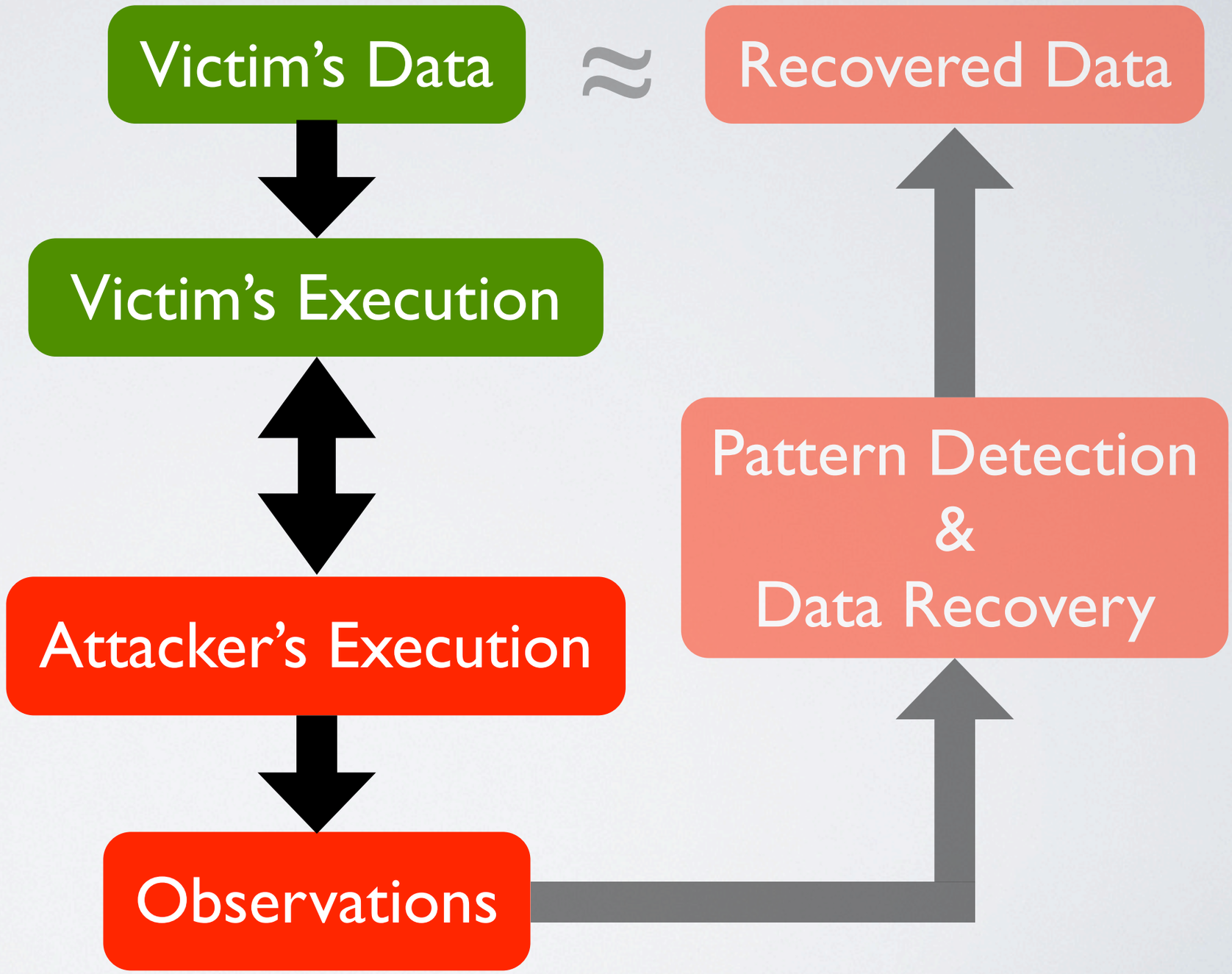
Measuring Leakiness



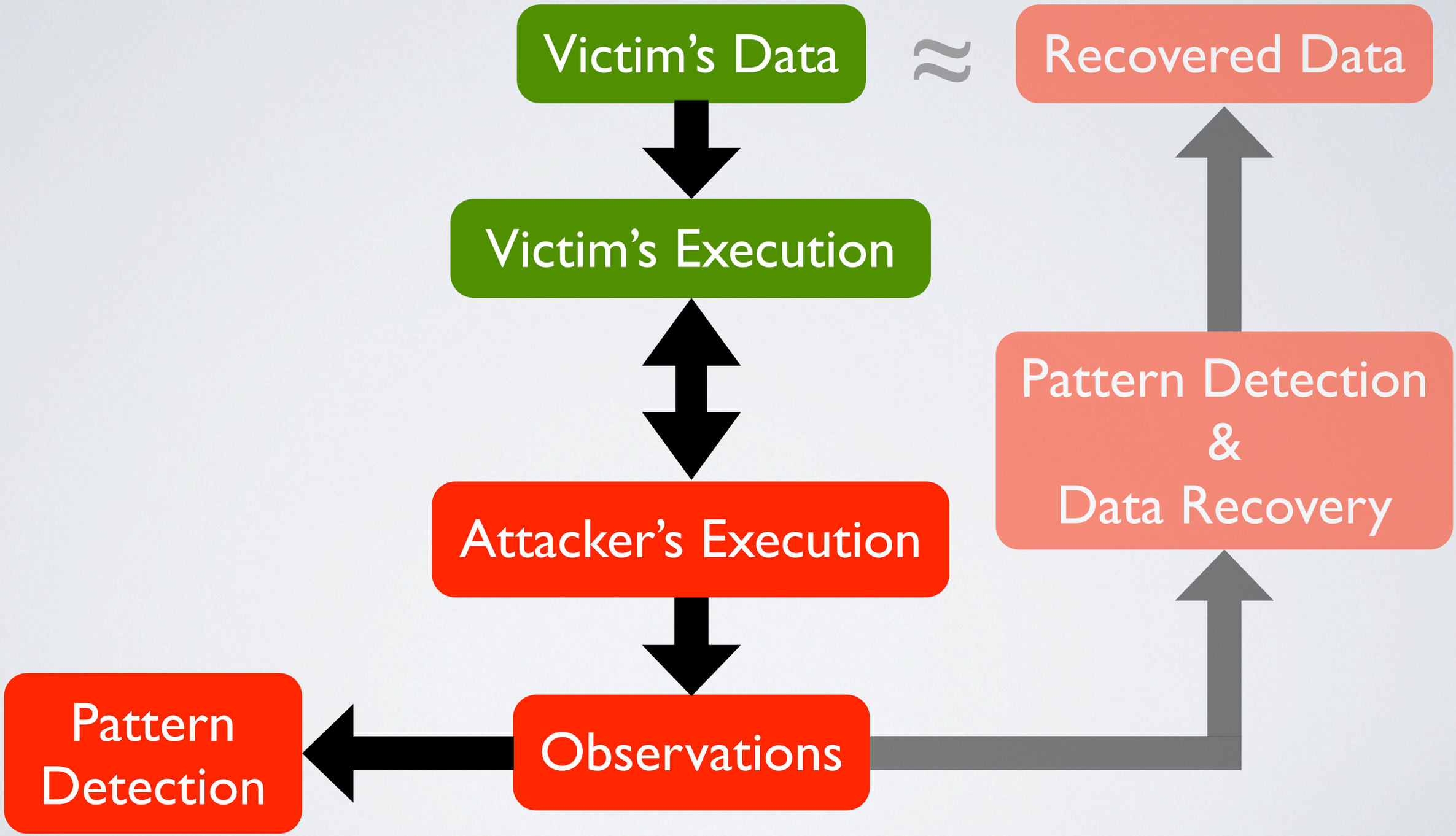
Measuring Leakiness



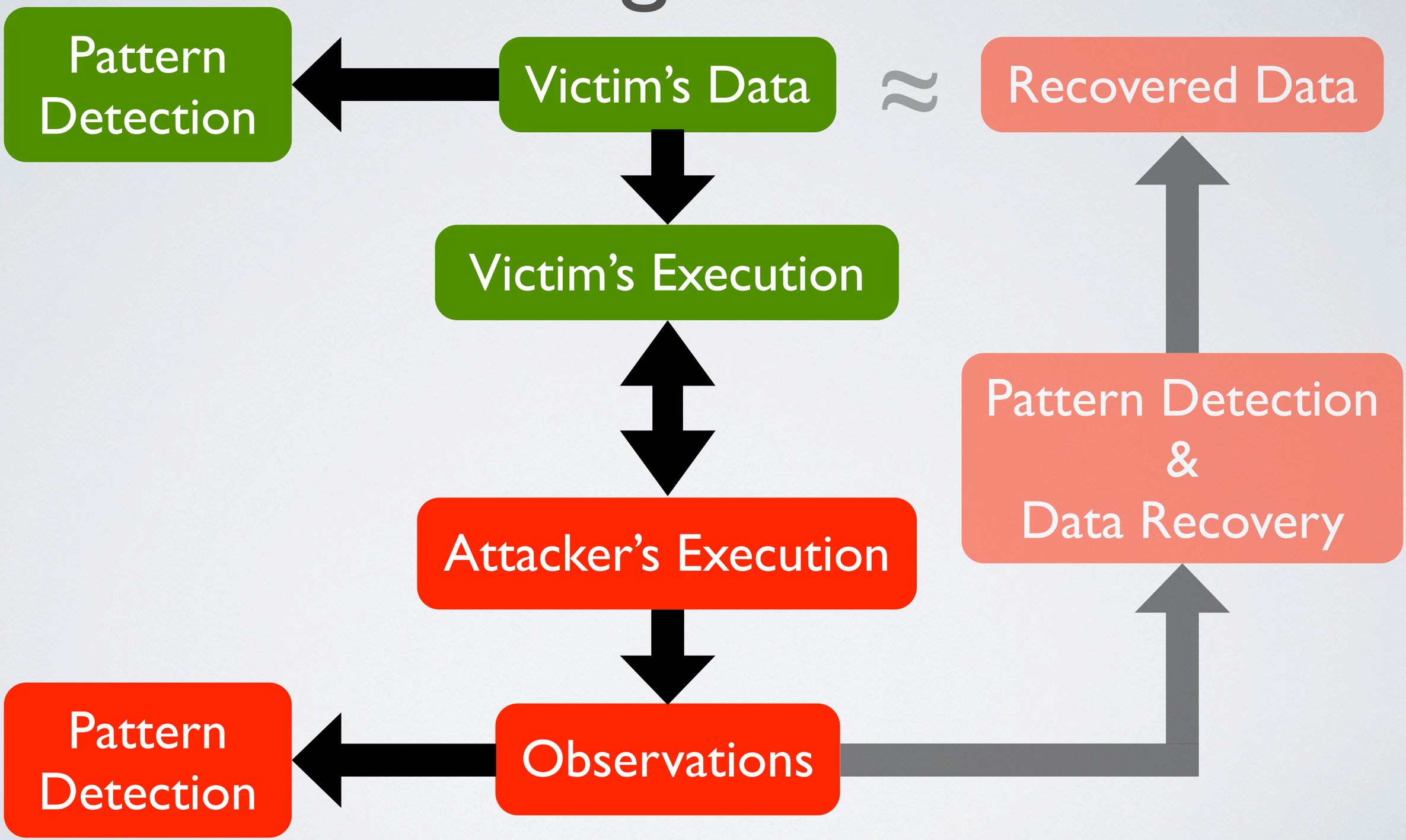
Measuring Leakiness



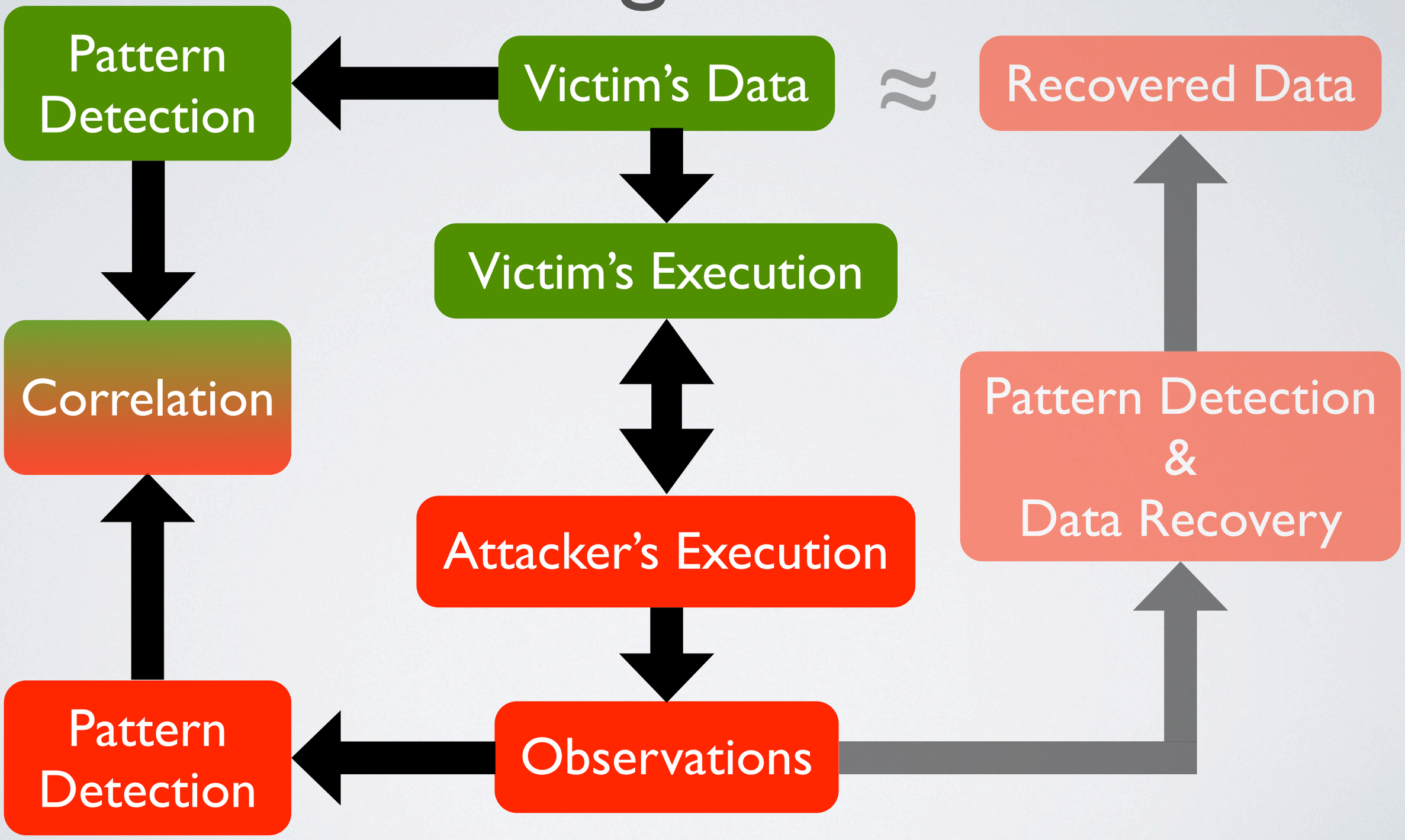
Measuring Leakiness



Measuring Leakiness

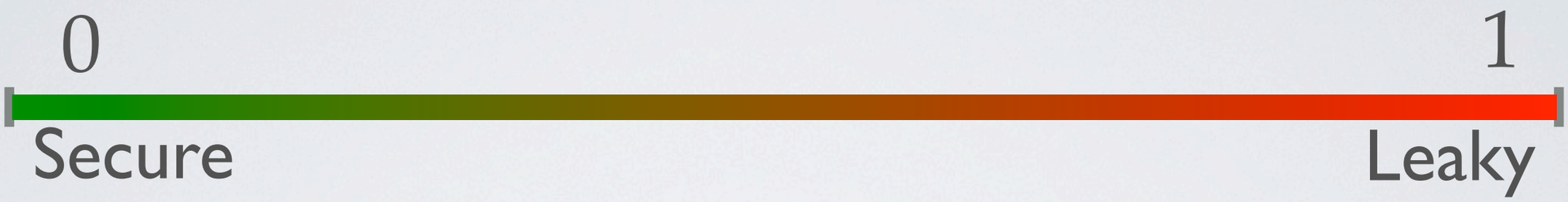


Measuring Leakiness

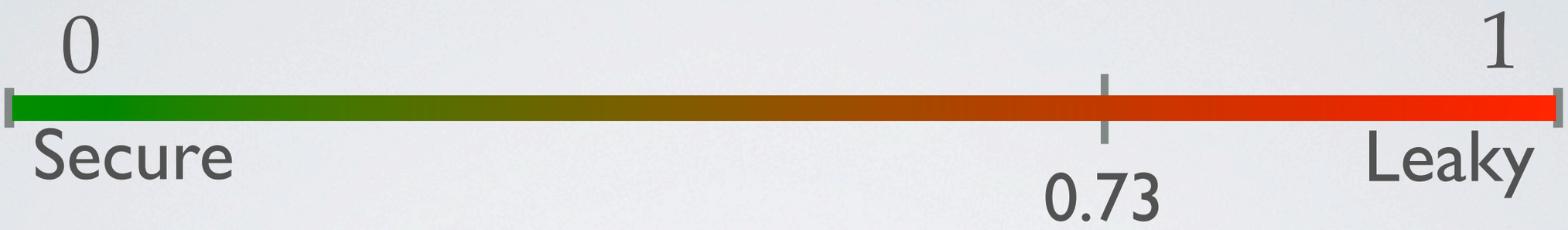


SVF is the **correlation** between **patterns** in attacker observations and **patterns** in victim's execution

SVF Effectiveness

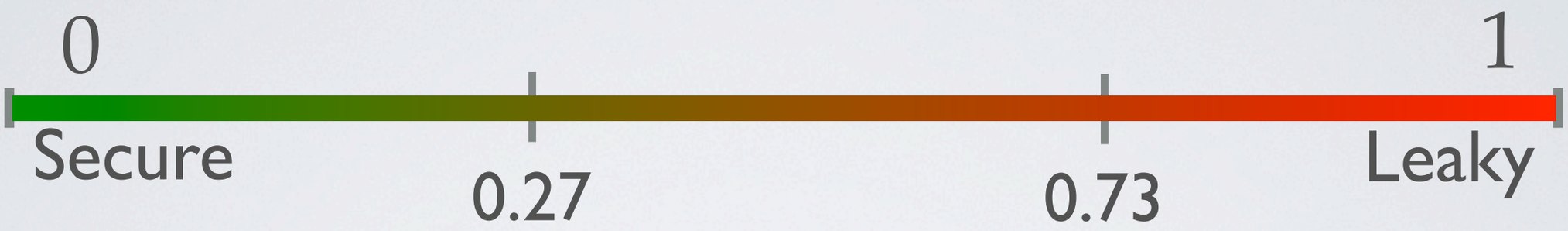


SVF Effectiveness



Similar to system attacked by [C. Percival 2005]

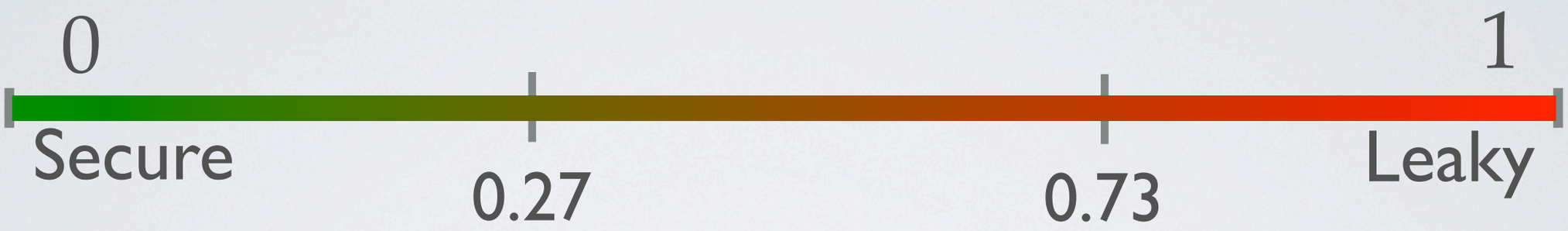
SVF Effectiveness



Similar to system attacked by [Gullash et al. 2011]

Similar to system attacked by [C. Percival 2005]

SVF Effectiveness

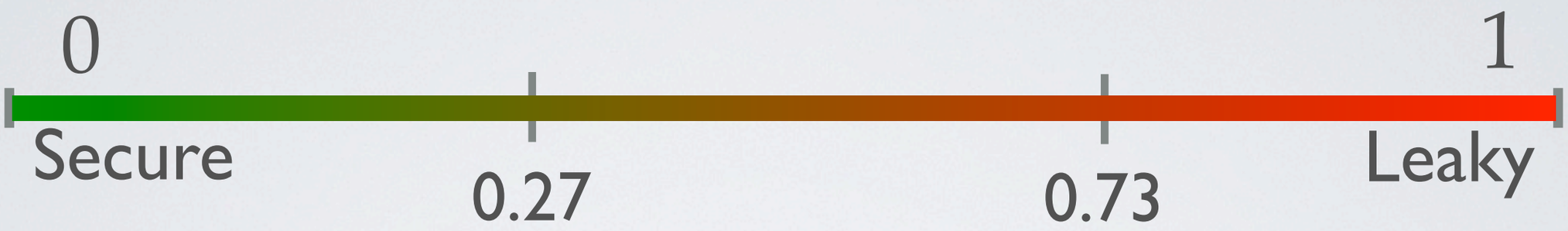


Similar to system attacked by [Gullash et al. 2011]

Similar to system attacked by [C. Percival 2005]

Required an artificial neural network to classify measurements

SVF Effectiveness



Similar to system attacked by [Gullash et al. 2011]

Required an artificial neural network to classify measurements

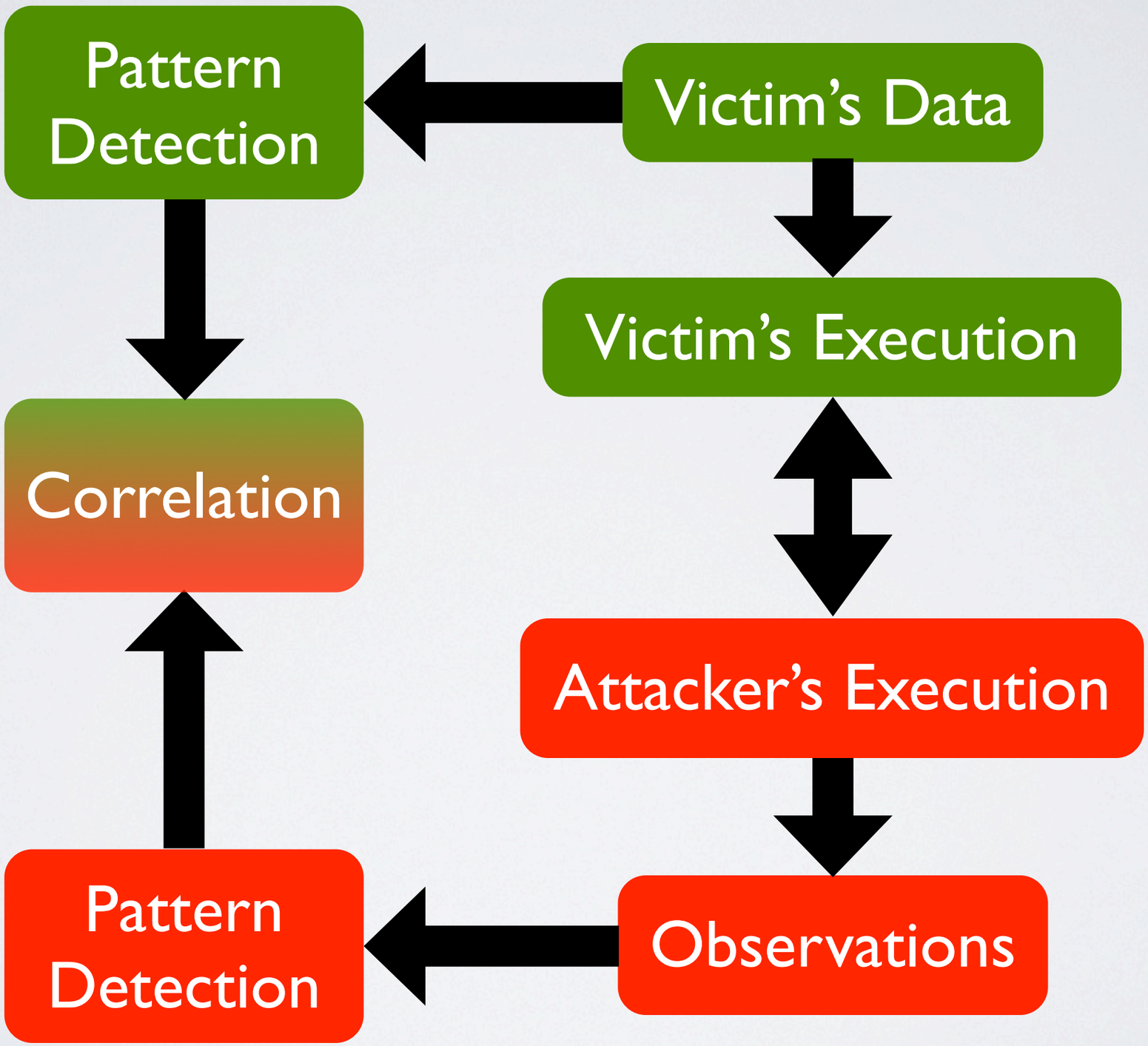
Similar to system attacked by [C. Percival 2005]

Patterns visible by the naked eye

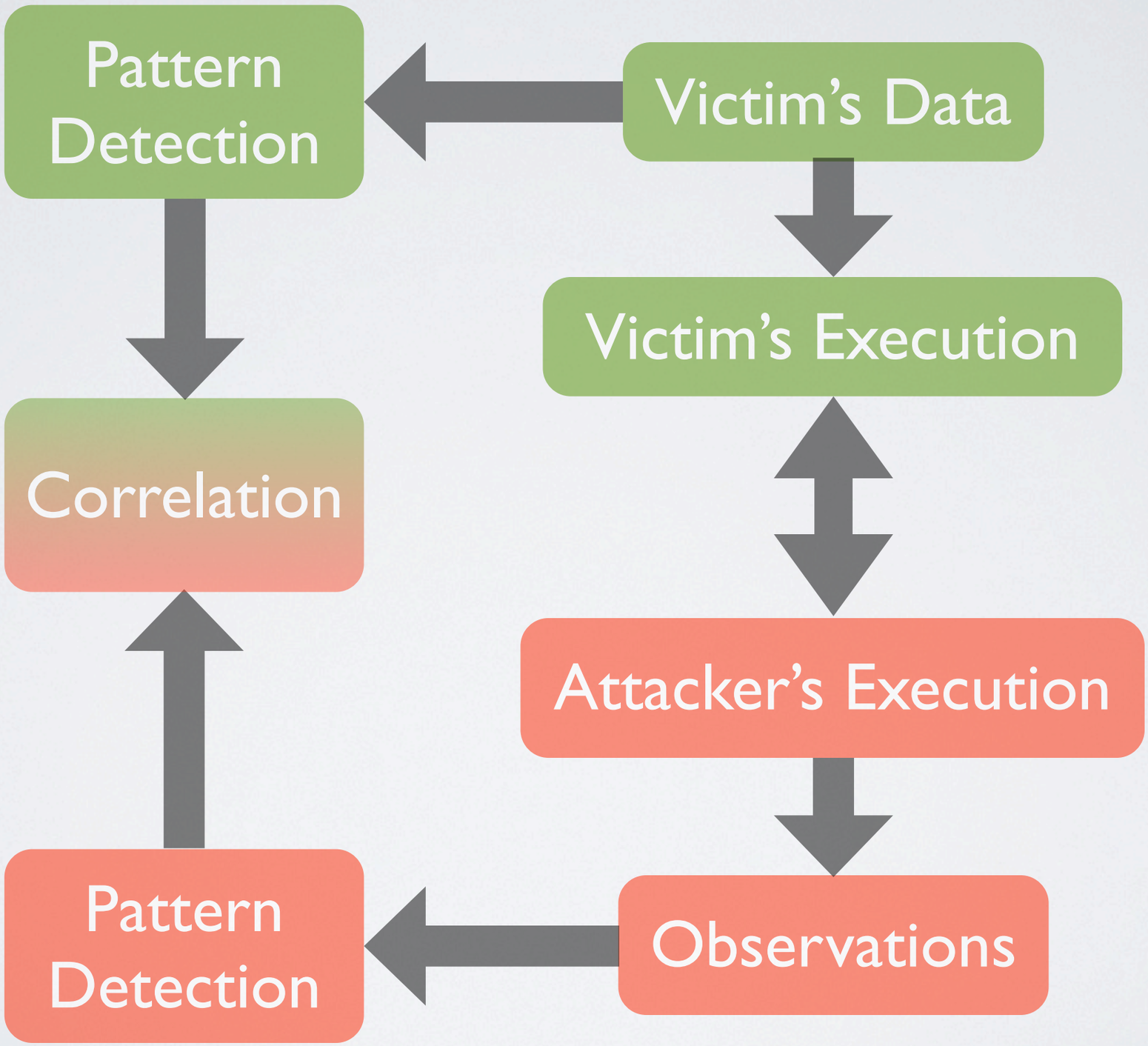
Cache Side Channels

SVF Illustration

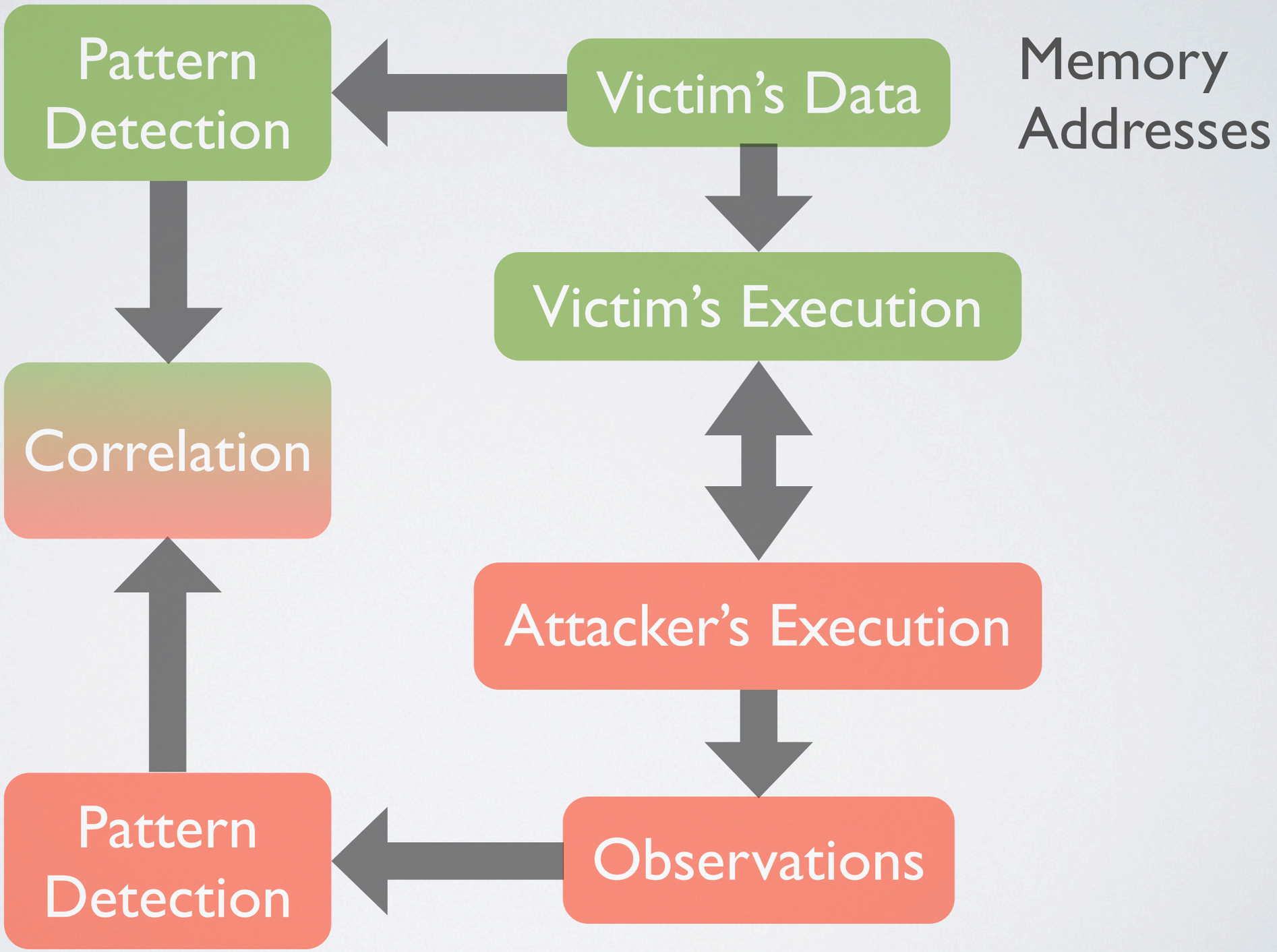
Using SVF


Pattern Detection
Victim's Data
Victim's Execution
Correlation
Attacker's Execution
Pattern Detection
Observations

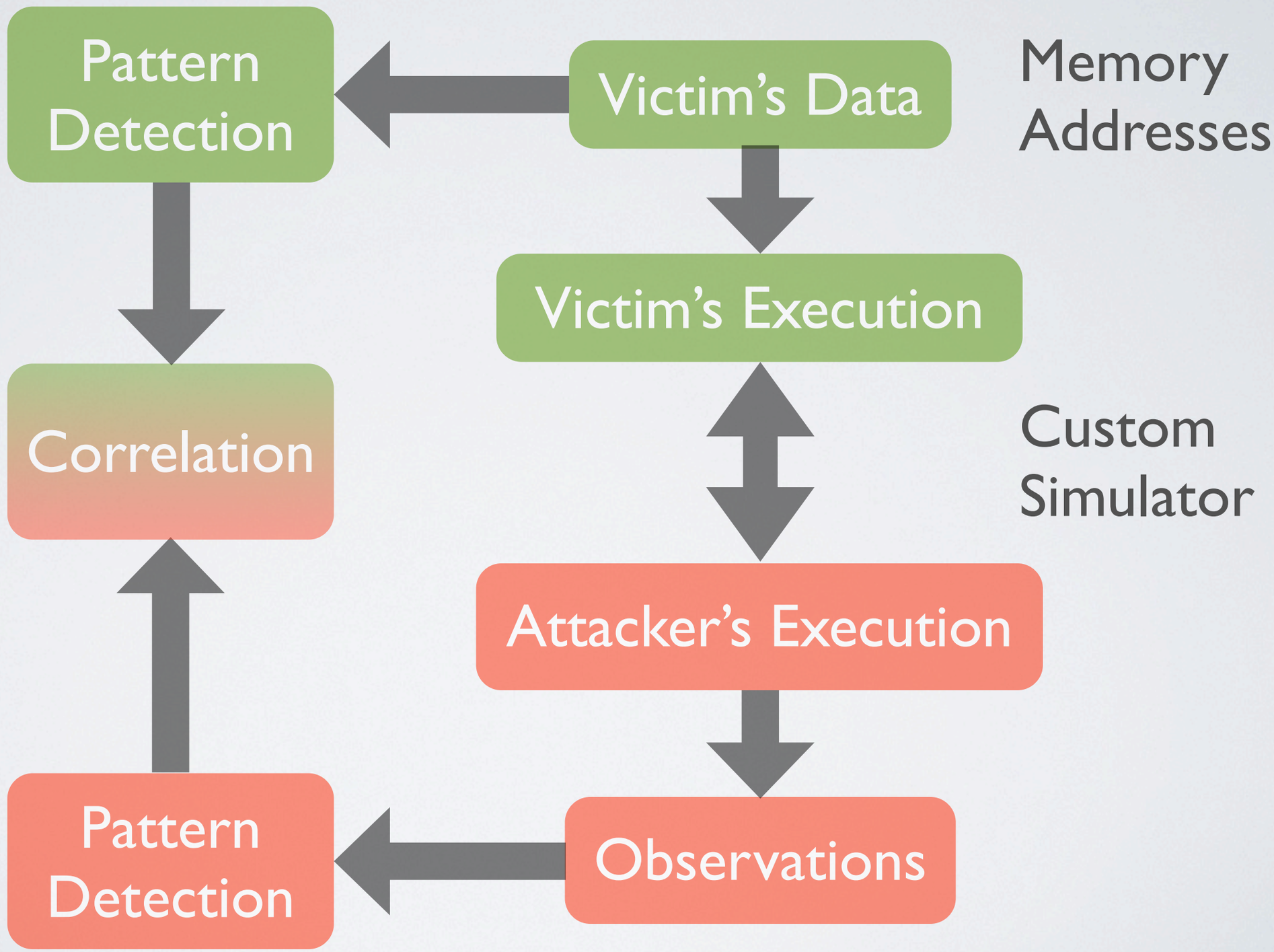
Using SVF


Pattern Detection
Victim's Data
Victim's Execution
Correlation
Attacker's Execution
Pattern Detection
Observations

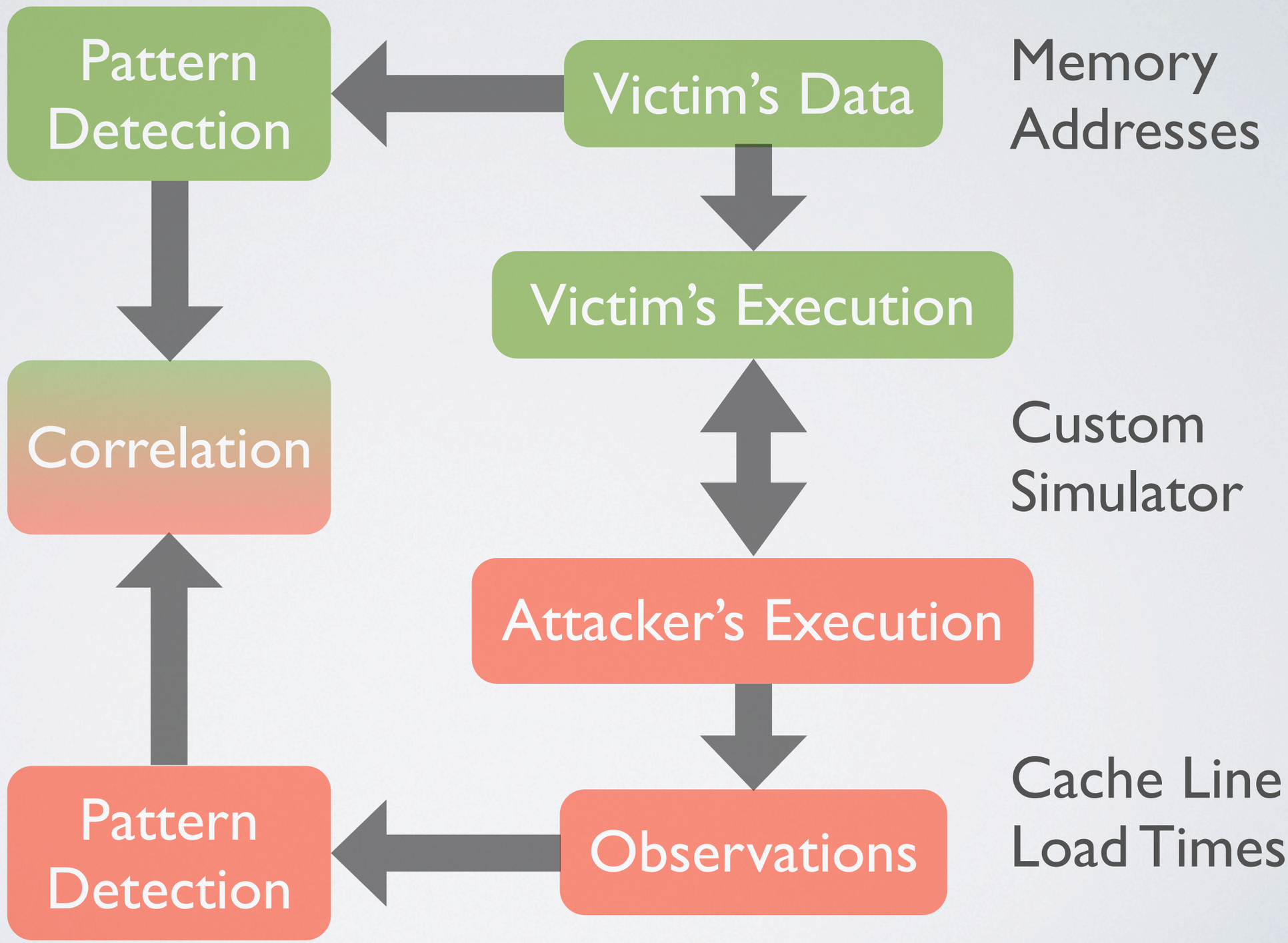
Using SVF


Pattern Detection
Victim's Data
Memory Addresses
Victim's Execution
Correlation
Attacker's Execution
Pattern Detection
Observations

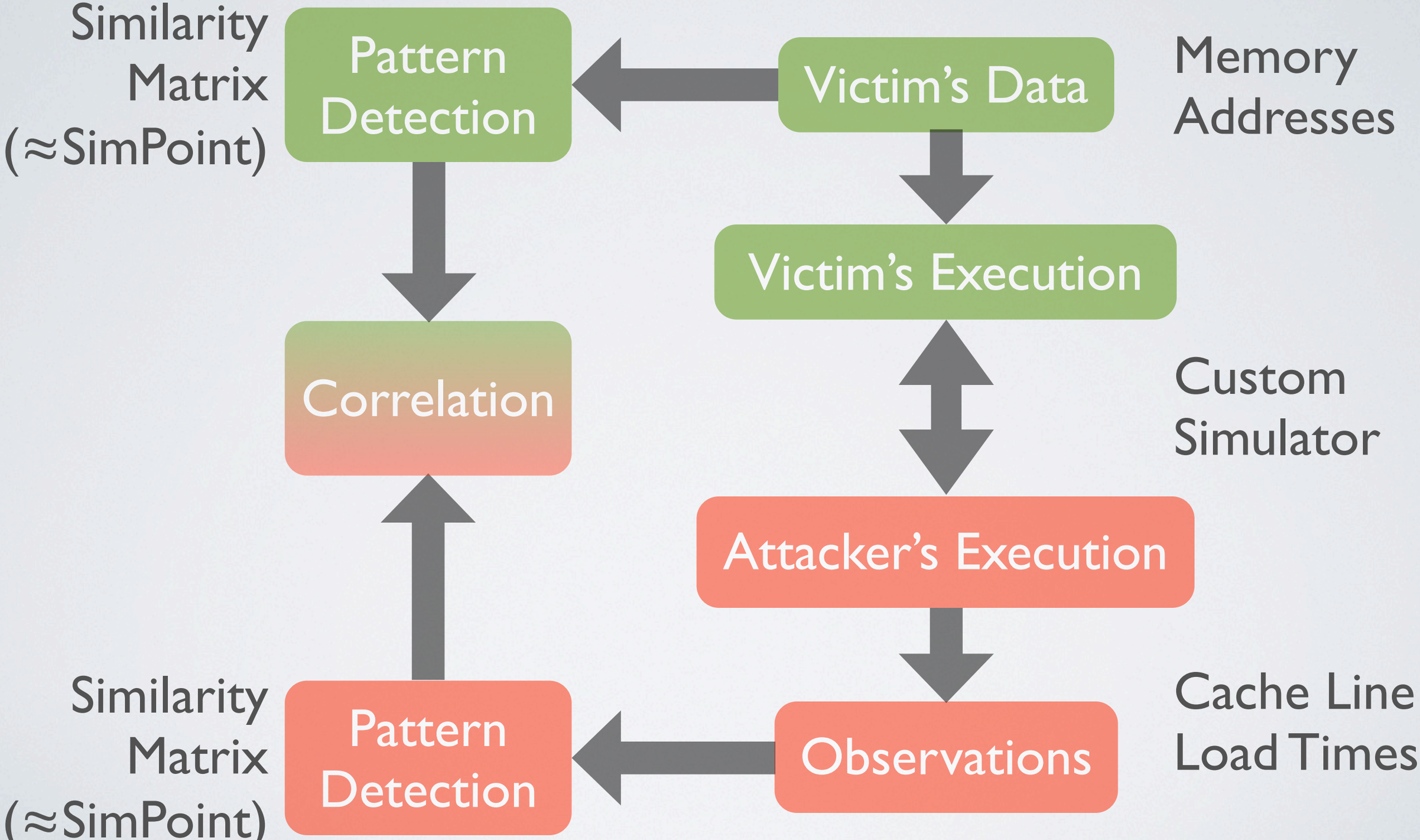
Using SVF


Pattern Detection
Victim's Data
Memory Addresses
Victim's Execution
Correlation
Custom Simulator
Attacker's Execution
Pattern Detection
Observations

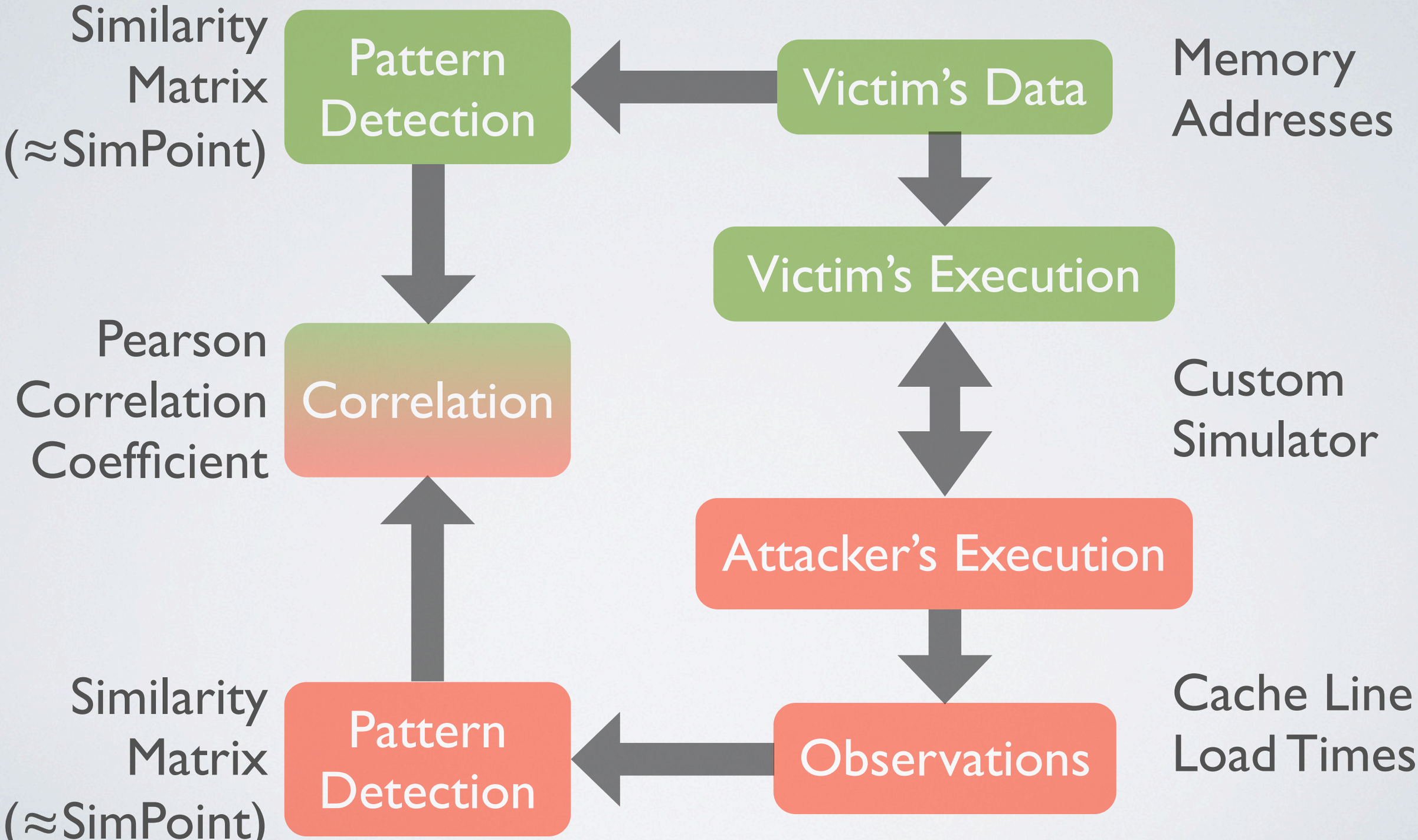
Using SVF


Pattern Detection
Victim's Data
Memory Addresses
Victim's Execution
Correlation
Custom Simulator
Attacker's Execution
Pattern Detection
Observations
Cache Line Load Times

Using SVF


Similarity Matrix (≈SimPoint)
Pattern Detection
Victim's Data
Memory Addresses
Victim's Execution
Custom Simulator
Attacker's Execution
Cache Line Load Times
Observations
Pattern Detection
Similarity Matrix (≈SimPoint)
Correlation

Using SVF


Similarity Matrix (≈SimPoint)
Pattern Detection
Victim's Data
Memory Addresses
Victim's Execution
Custom Simulator
Attacker's Execution
Observations
Cache Line Load Times
Pattern Detection
Similarity Matrix (≈SimPoint)
Correlation
Pearson Correlation Coefficient

A Large Design Space

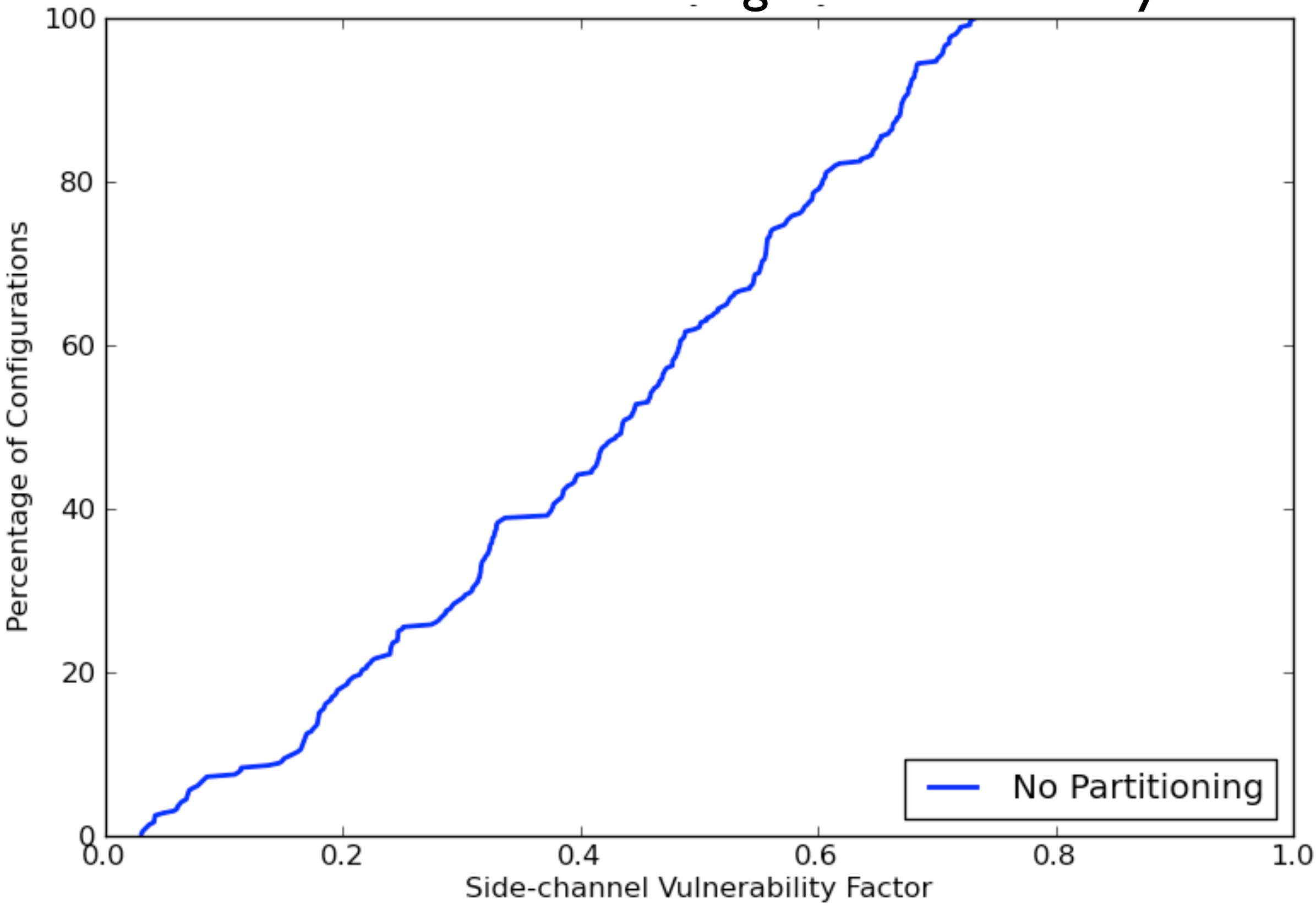
SMT x Cache Size x Line Size x Associativity x Hashing x Prefetching x Partitioning x Protection

=

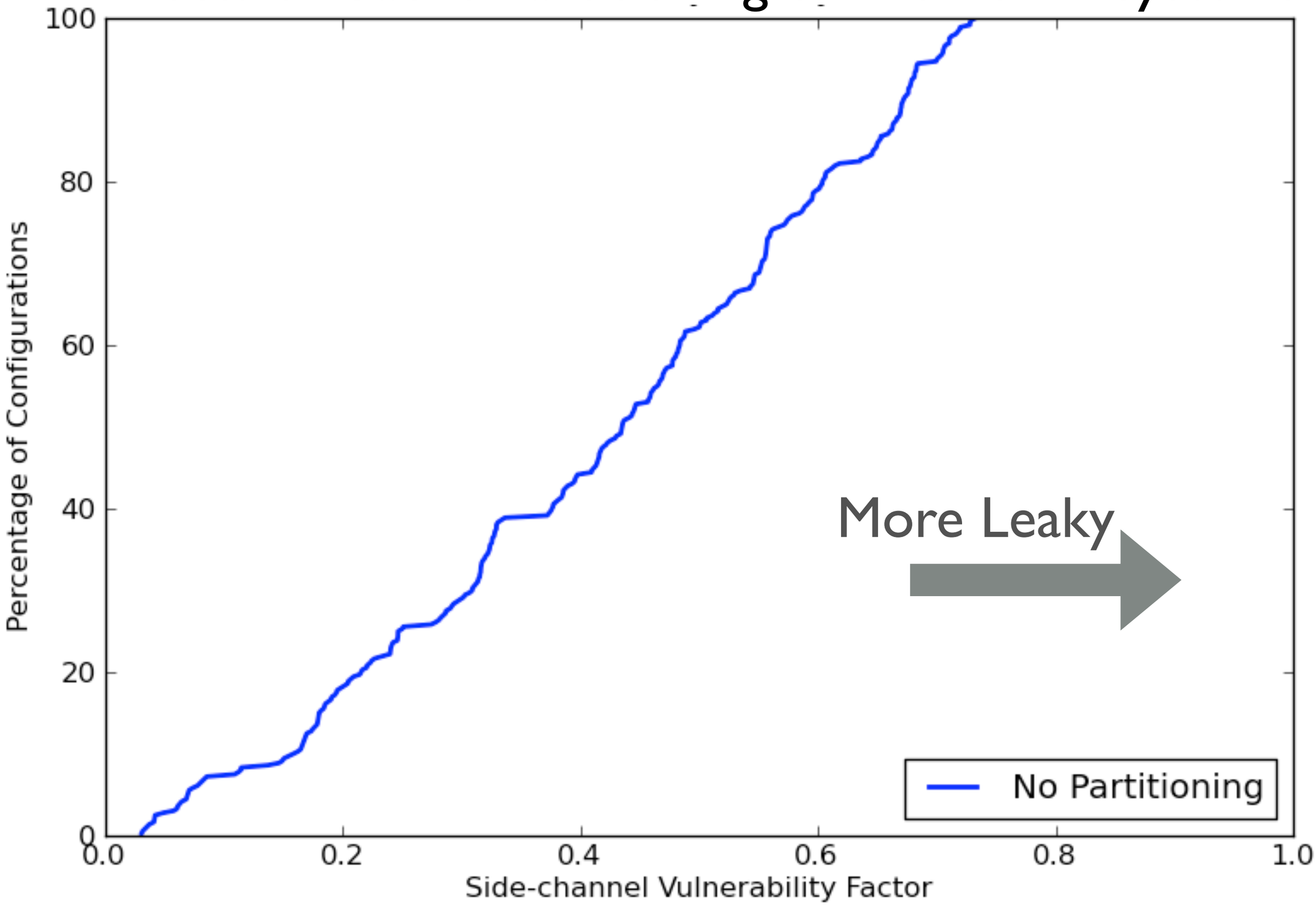
34,020 Simulations

- We examine PRS with our policies, not RPCache
  - Refer to: Z. Wang and R. B. Lee. Covert and side channels due to processor architecture. ACSAC '06
- Results are specific to our simulator
  - While SVF can be a comparative tool, this is not a comparative study

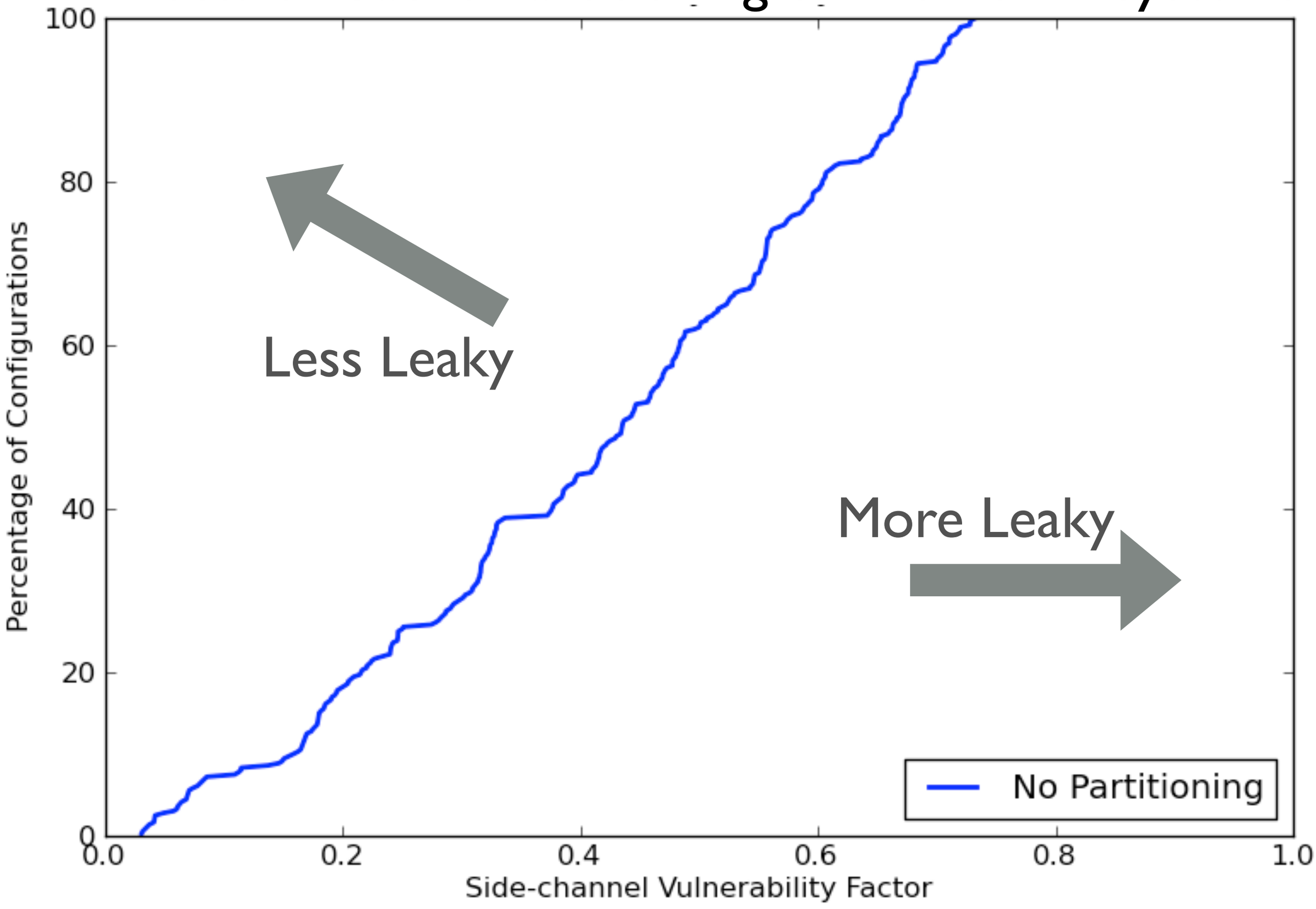
Effects of Cache Partitioning on Non-SMT Systems



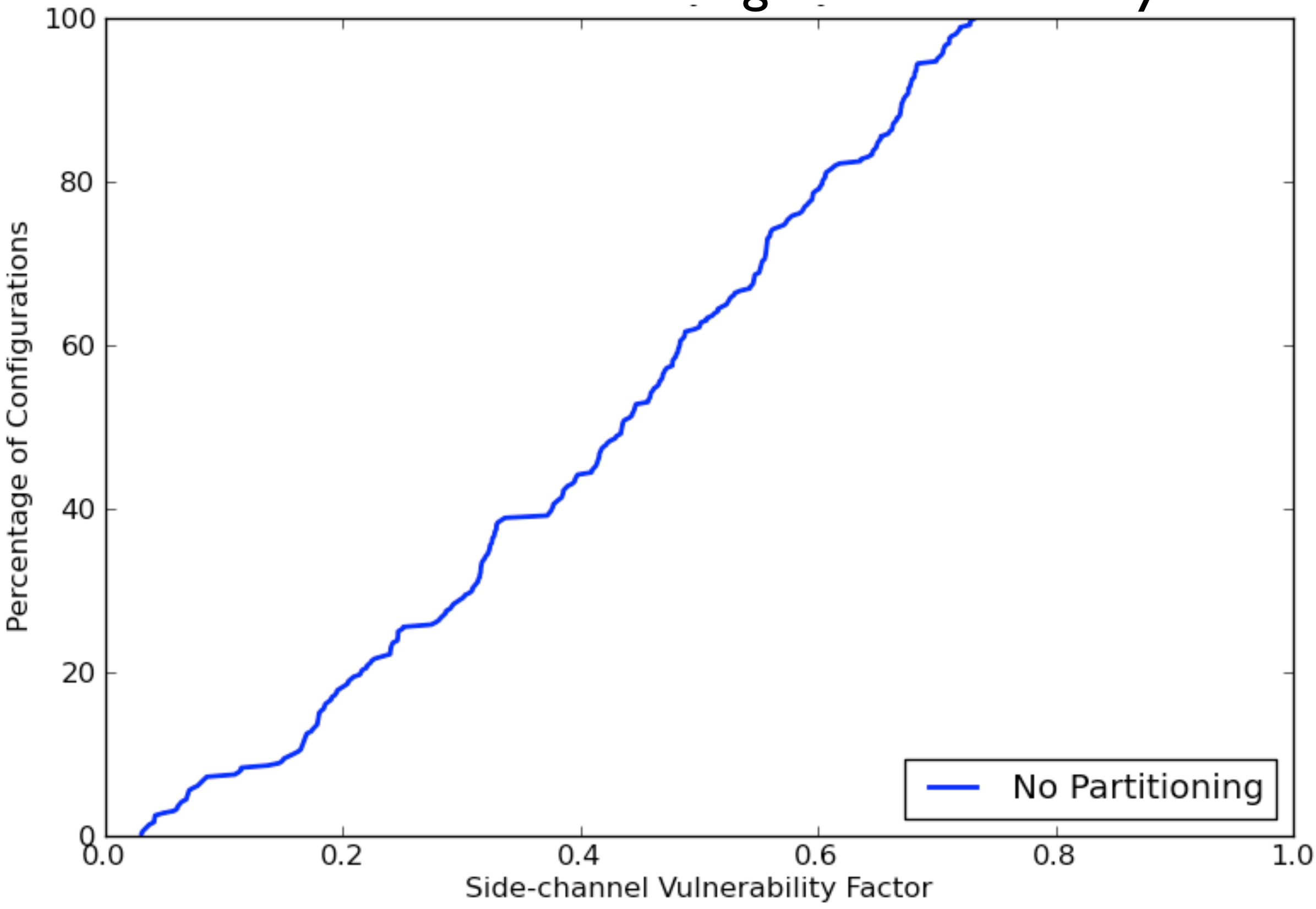
Effects of Cache Partitioning on Non-SMT Systems



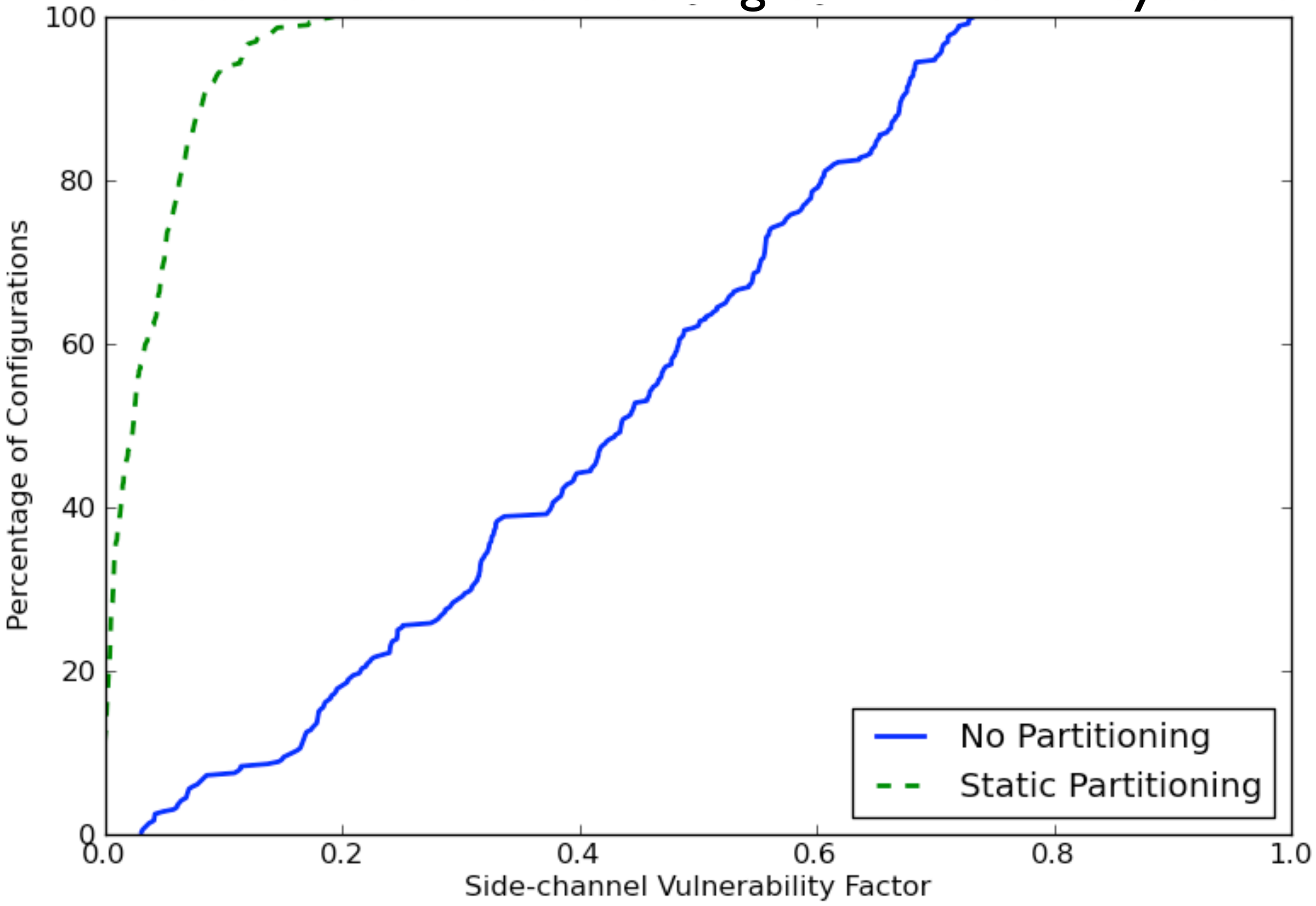
Effects of Cache Partitioning on Non-SMT Systems



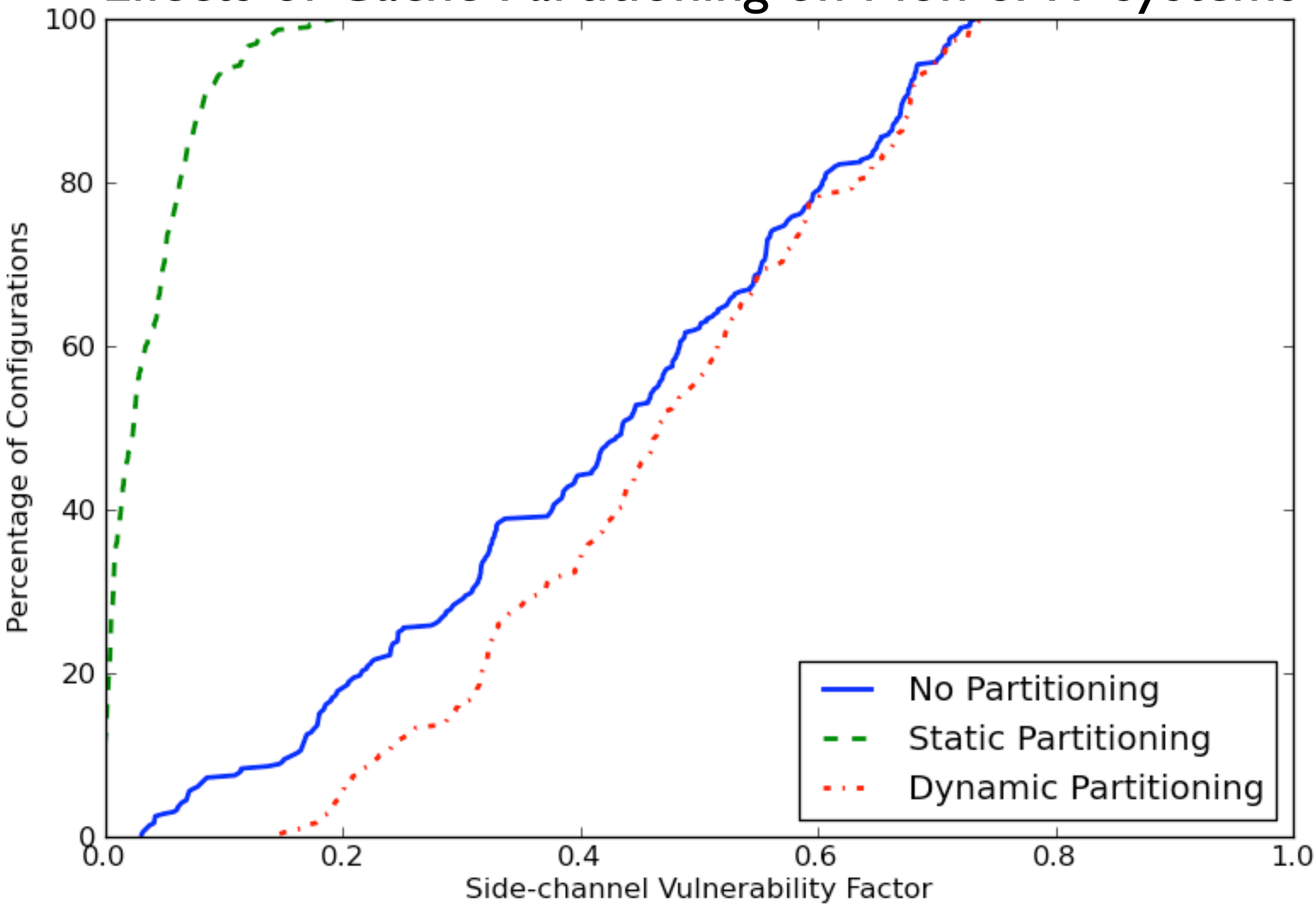
Effects of Cache Partitioning on Non-SMT Systems



Effects of Cache Partitioning on Non-SMT Systems

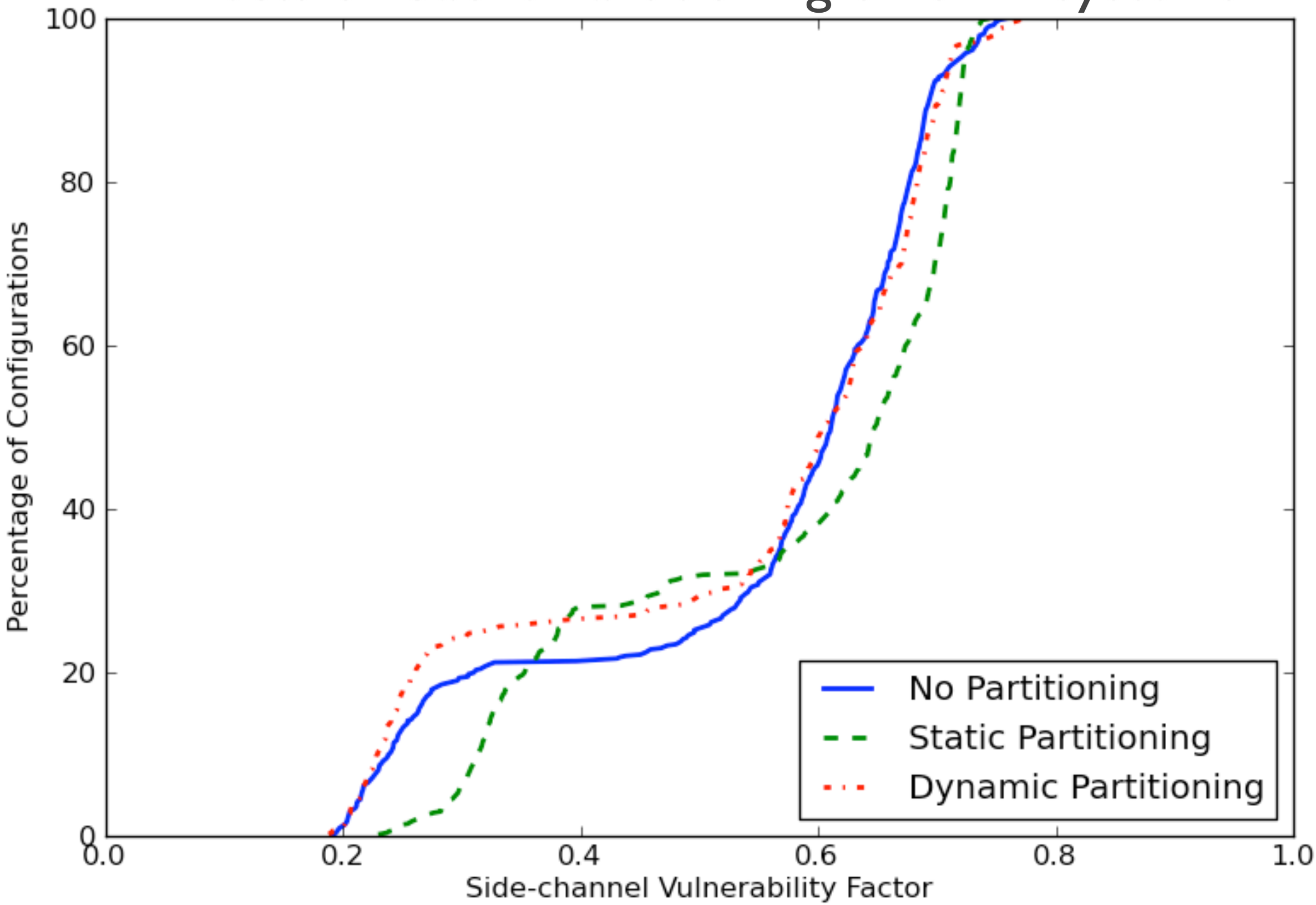


Effects of Cache Partitioning on Non-SMT Systems



Effects of Cache Partitioning on SMT Systems

Effects of Cache Partitioning on SMT Systems



Related Work

- Physically Observable Cryptography [Micali & Reyzin 2004]
- Predictive Cache Leakage Model [Dominister et al. 2010]
- SVF is practical and generally applicable

Conclusions

Conclusions

- SVF: Measures information leakage
  - General, practical, quantitative

Conclusions

- SVF: Measures information leakage
  - General, practical, quantitative

- Key Insight
  - Attackers correlate measured patterns to victim's secrets

Impact & Future Work

Impact & Future Work

- Uses / impact
  - Early design-phase security analysis
  - Performance-security tradeoffs

Impact & Future Work

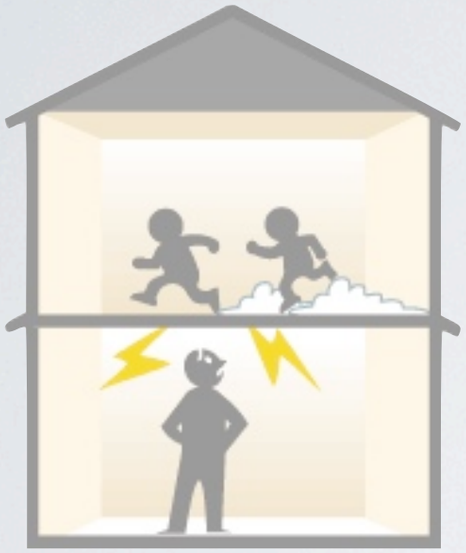
- Uses / impact
  - Early design-phase security analysis
  - Performance-security tradeoffs
- Future Work
  - Further applications of SVF and improvements
  - Implementing SVF on real systems
  - Automatic identification of side-channels

Backup Slides

Man down! Need backup!

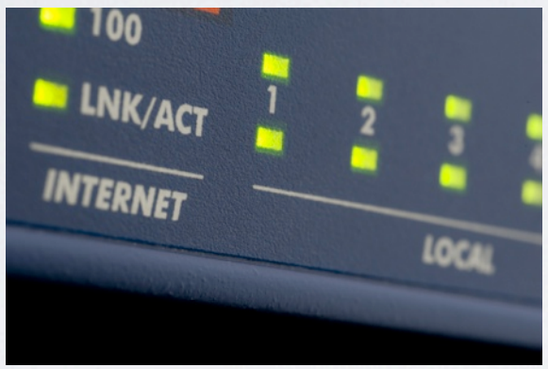
Types of Side Channels

Physical Side Channels



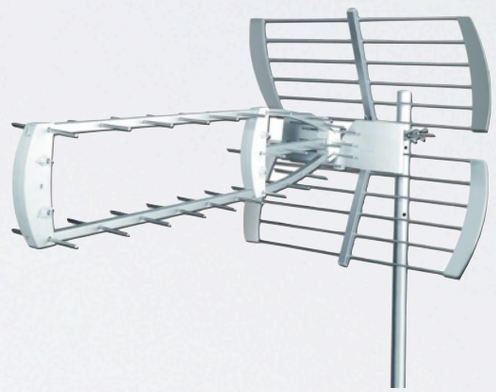
Acoustic

[Asonov et al. 2004]
[Backes et al. 2010]



Optical

[Ferrigno et al. 2008]



Electromagnetic

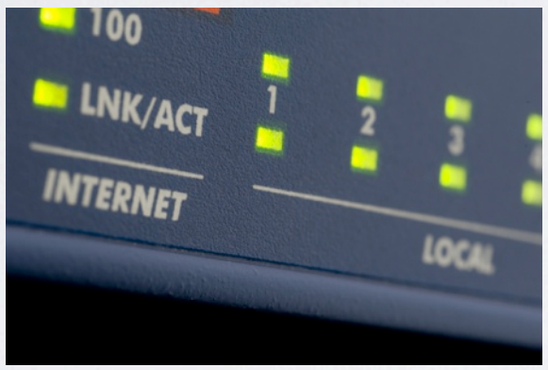
[Van Eck et al. 1985]

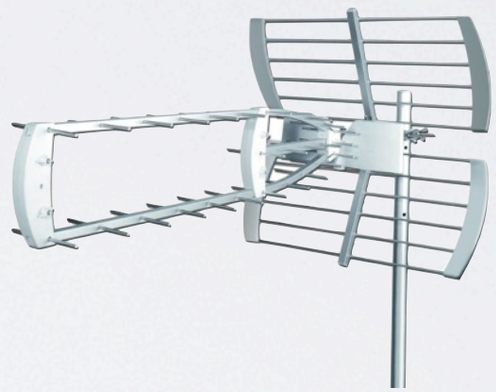
Power

[Messerges et al. 1999]

Types of Side Channels

Physical Side Channels





Acoustic

[Asonov et al. 2004]
[Backes et al. 2010]

Optical

[Ferrigno et al. 2008]

Electromagnetic

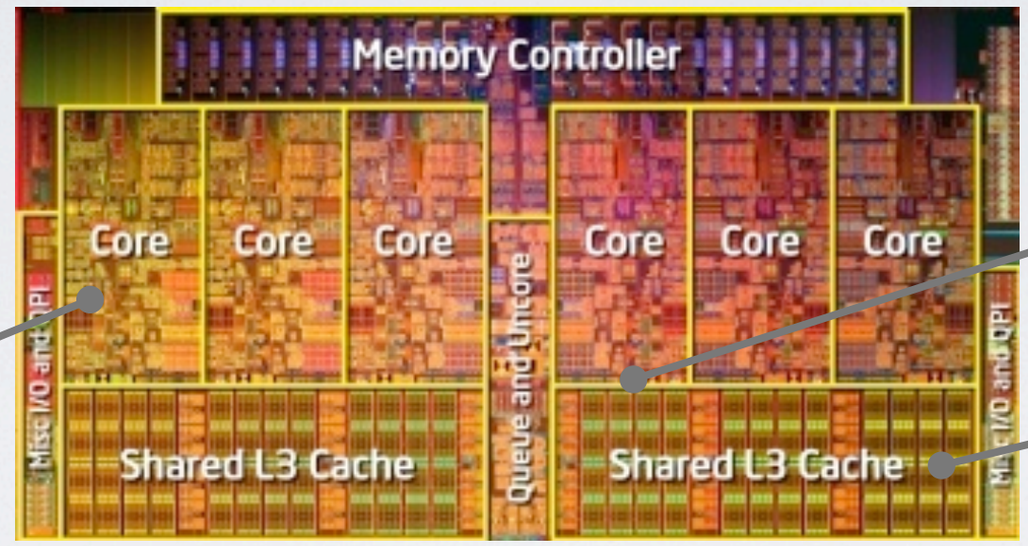
[Van Eck et al. 1985]

Power

[Messerges et al. 1999]

Types of Side Channels

Contention Side Channels



Pipeline

NOC

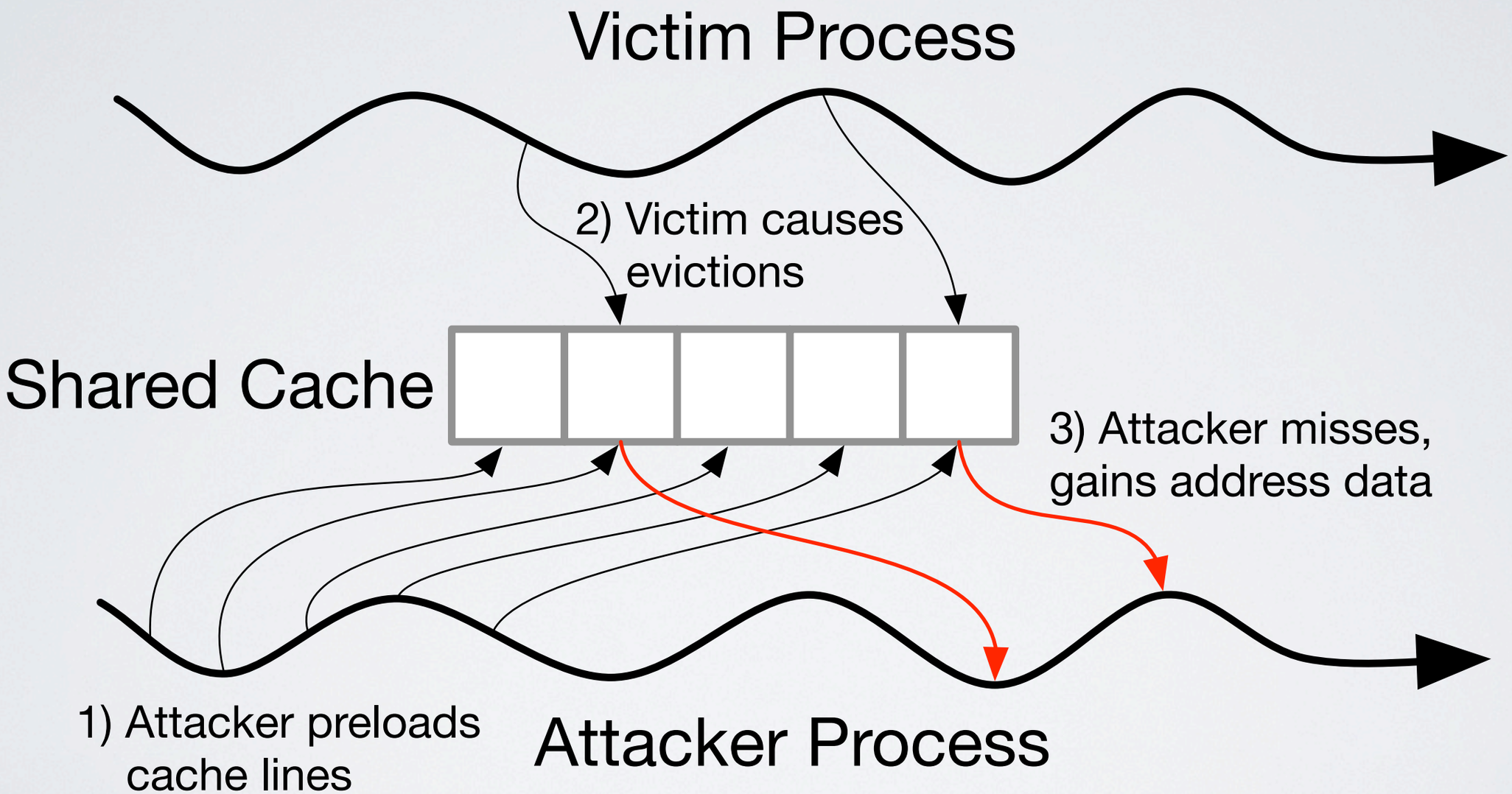
Cache

Processor

Disk

Network

Cache Side Channels



Cache Side Channels

Image Credit: C. Percival 2005

Cache Side Channels

1) Measure usage over time

Image Credit: C. Percival 2005

Cache Side Channels

1) Measure usage over time

2) Look for patterns

Image Credit: C. Percival 2005

Cache Side Channels

1) Measure usage over time

2) Look for patterns

Image Credit: C. Percival 2005

Cache Side Channels

1) Measure usage over time

2) Look for patterns

3) Find correlation to victim

Image Credit: C. Percival 2005

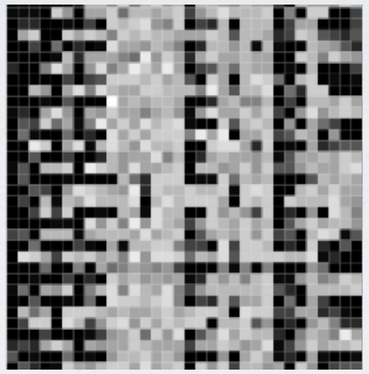
Measuring Side Channels

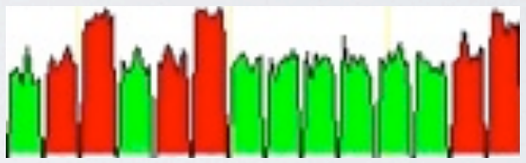
Measure

Analyze

Correlate

Measuring Side Channels



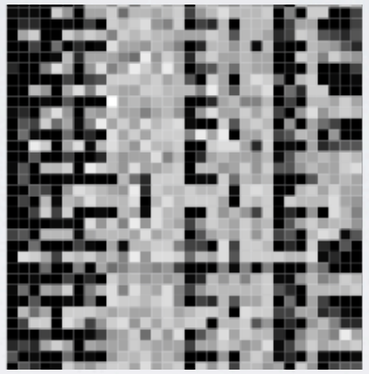


Measure

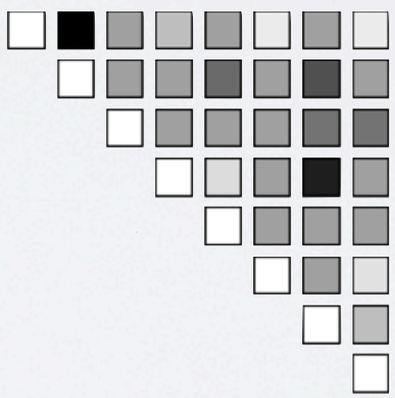
Analyze

Correlate

Measuring Side Channels



Measure

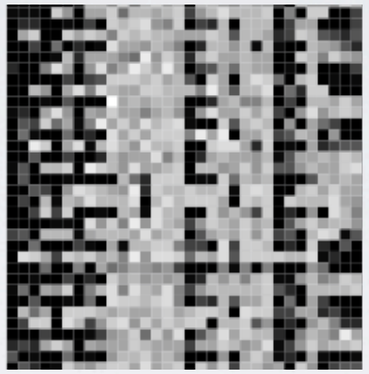


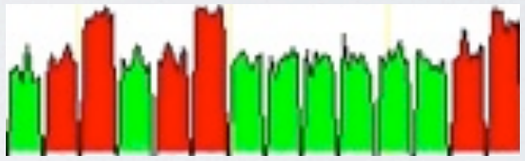
Analyze

Correlate

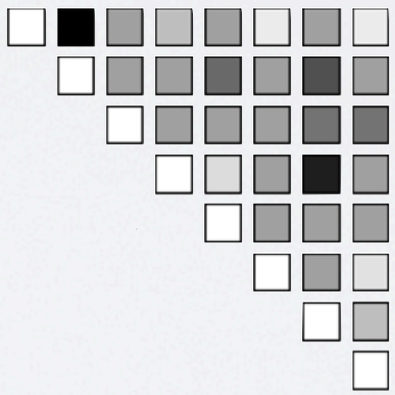
Measuring Side Channels

Side Channel Trace





Measure



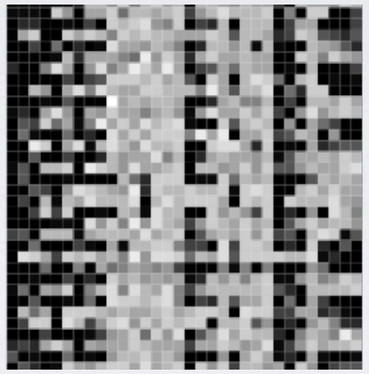
Analyze

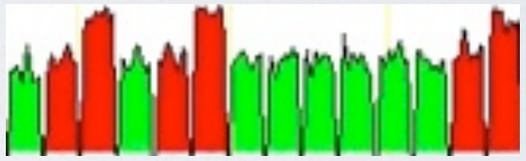
Correlate

Measuring Side Channels

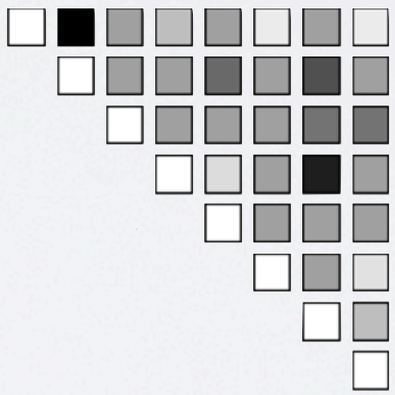
Oracle Trace

Side Channel Trace





Measure

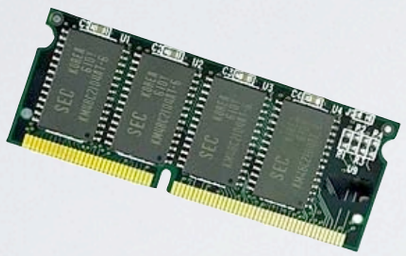


Analyze

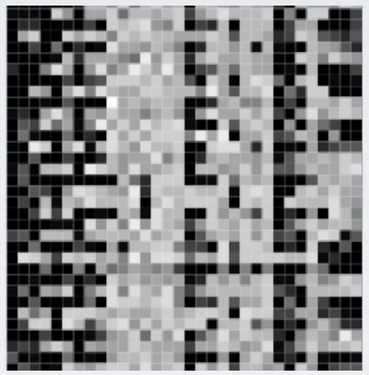
Correlate

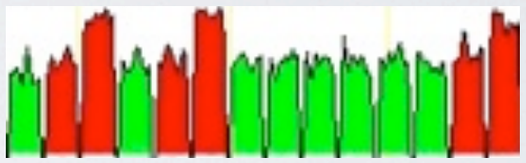
Measuring Side Channels

Oracle Trace

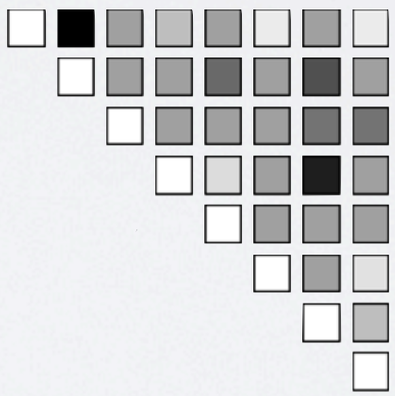


Side Channel Trace





Measure

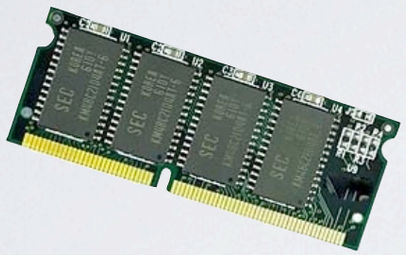


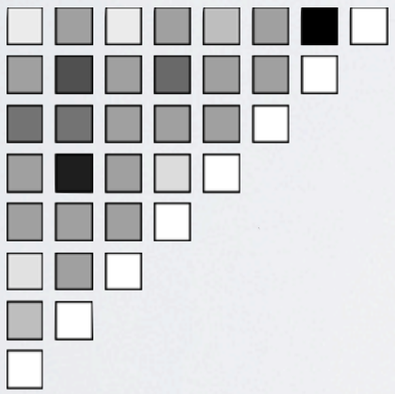
Analyze

Correlate

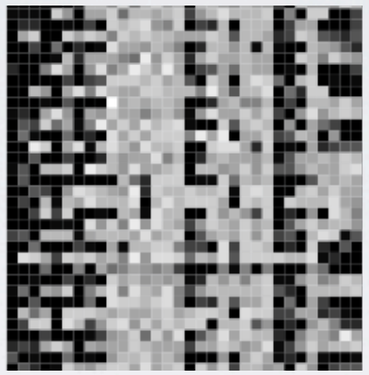
Measuring Side Channels

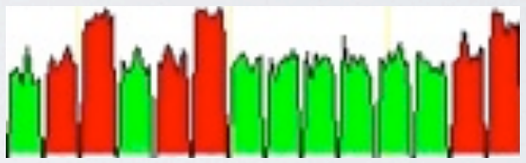
Oracle Trace

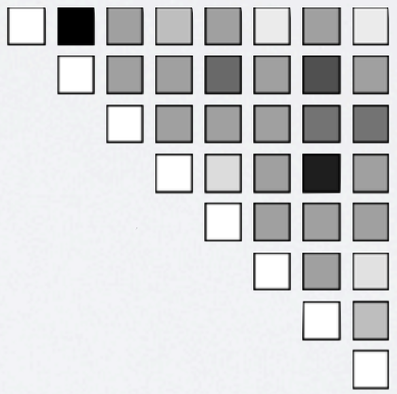




Side Channel Trace







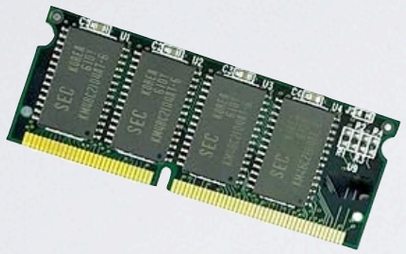
Measure

Analyze

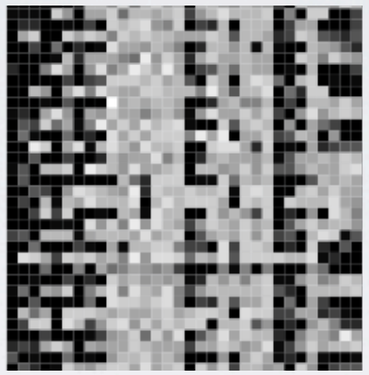
Correlate

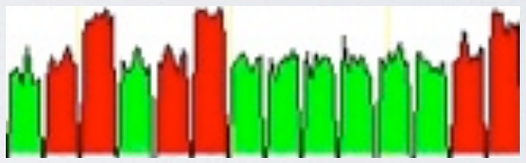
Measuring Side Channels

Oracle Trace

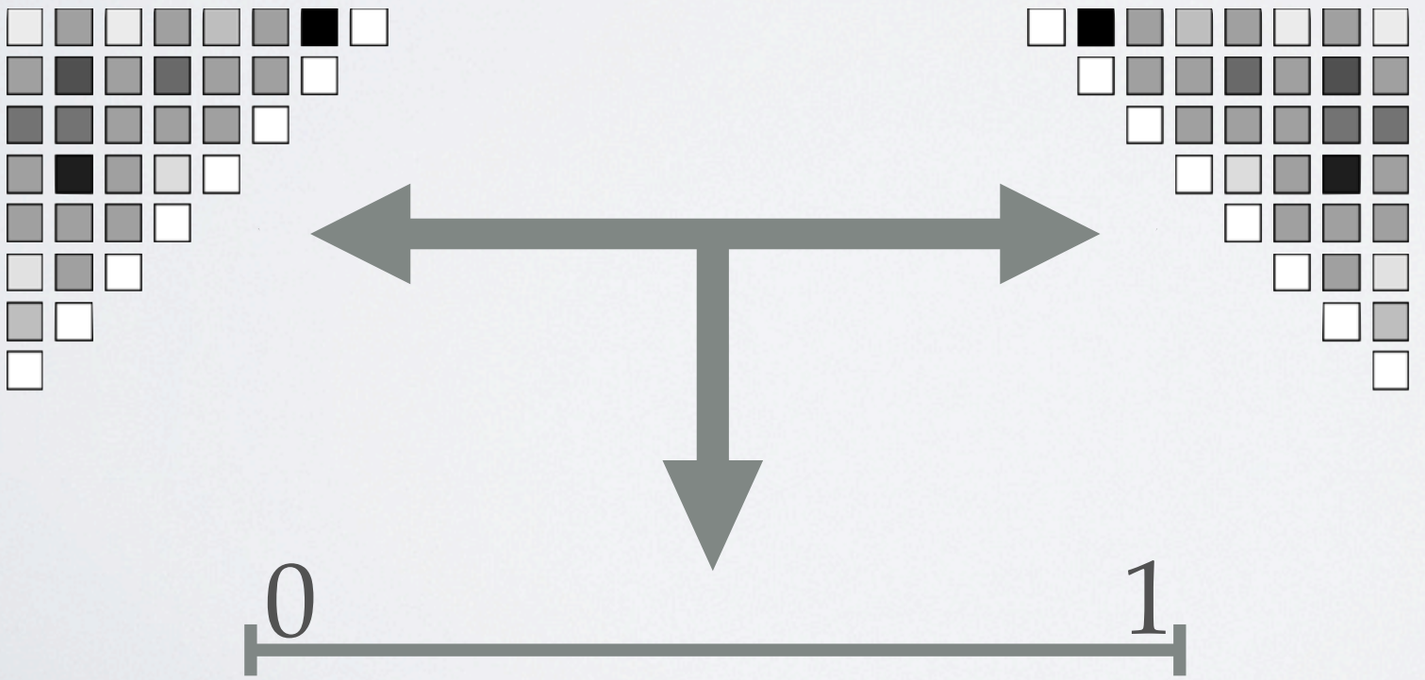


Side Channel Trace





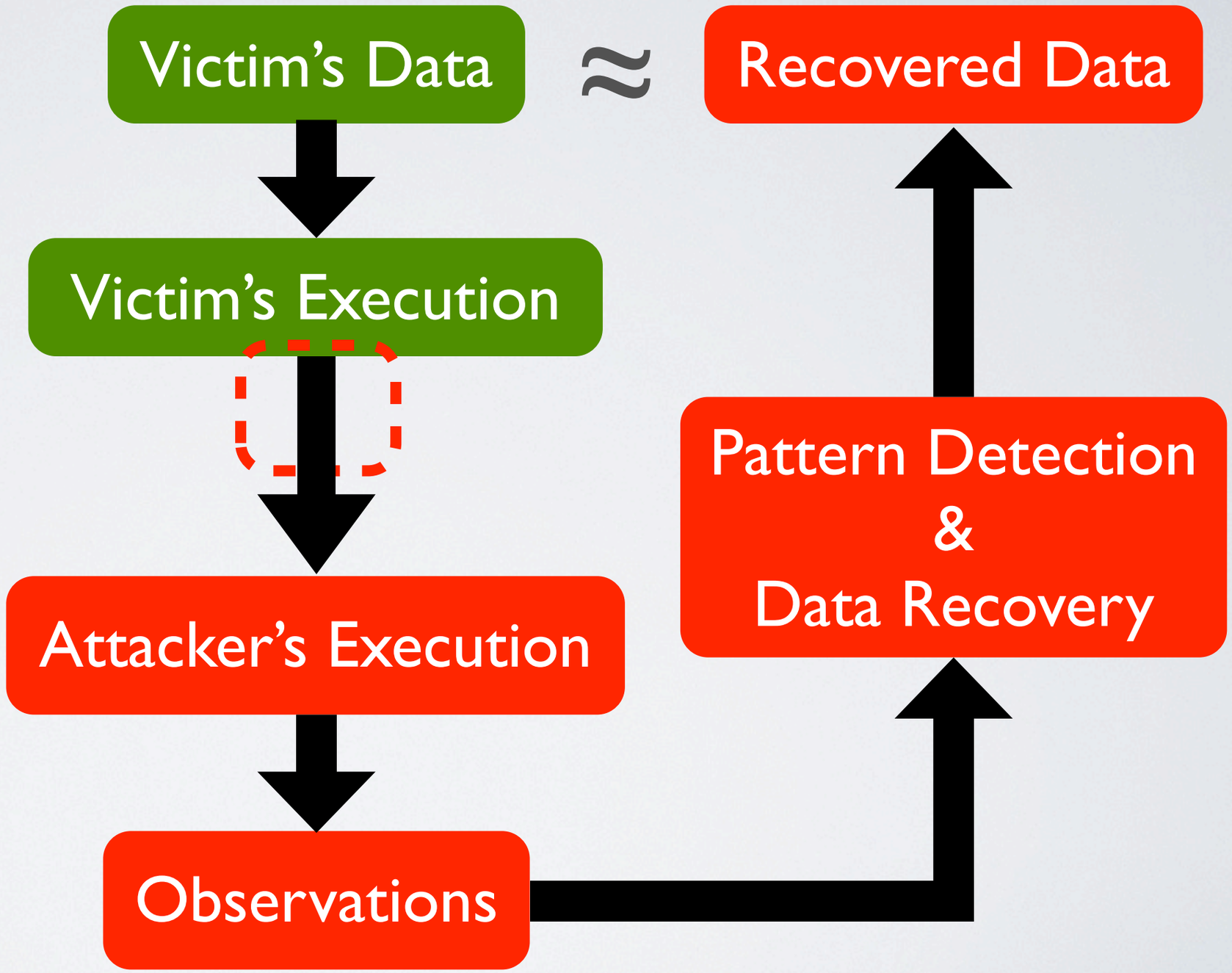
Measure



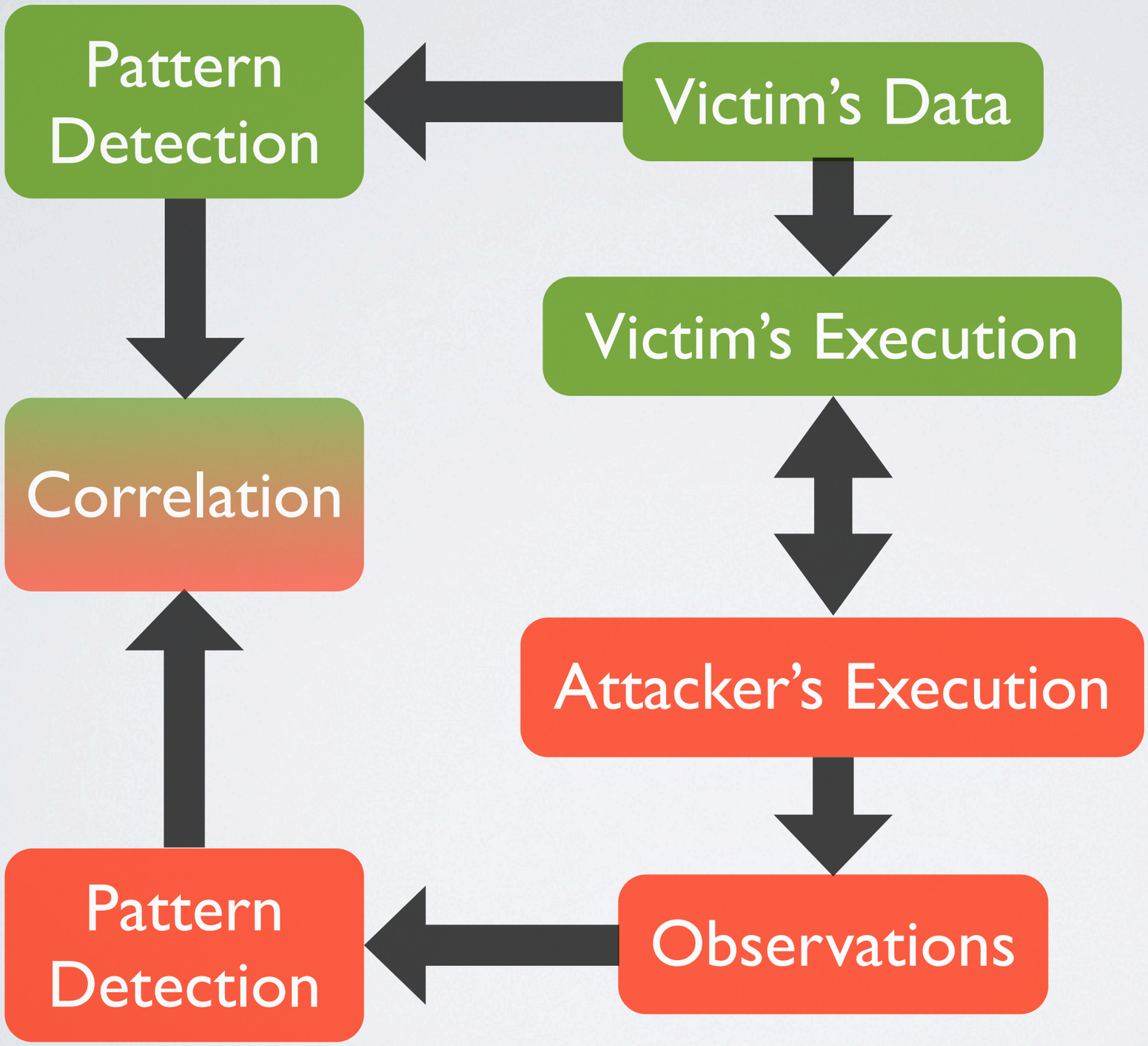
Analyze

Correlate

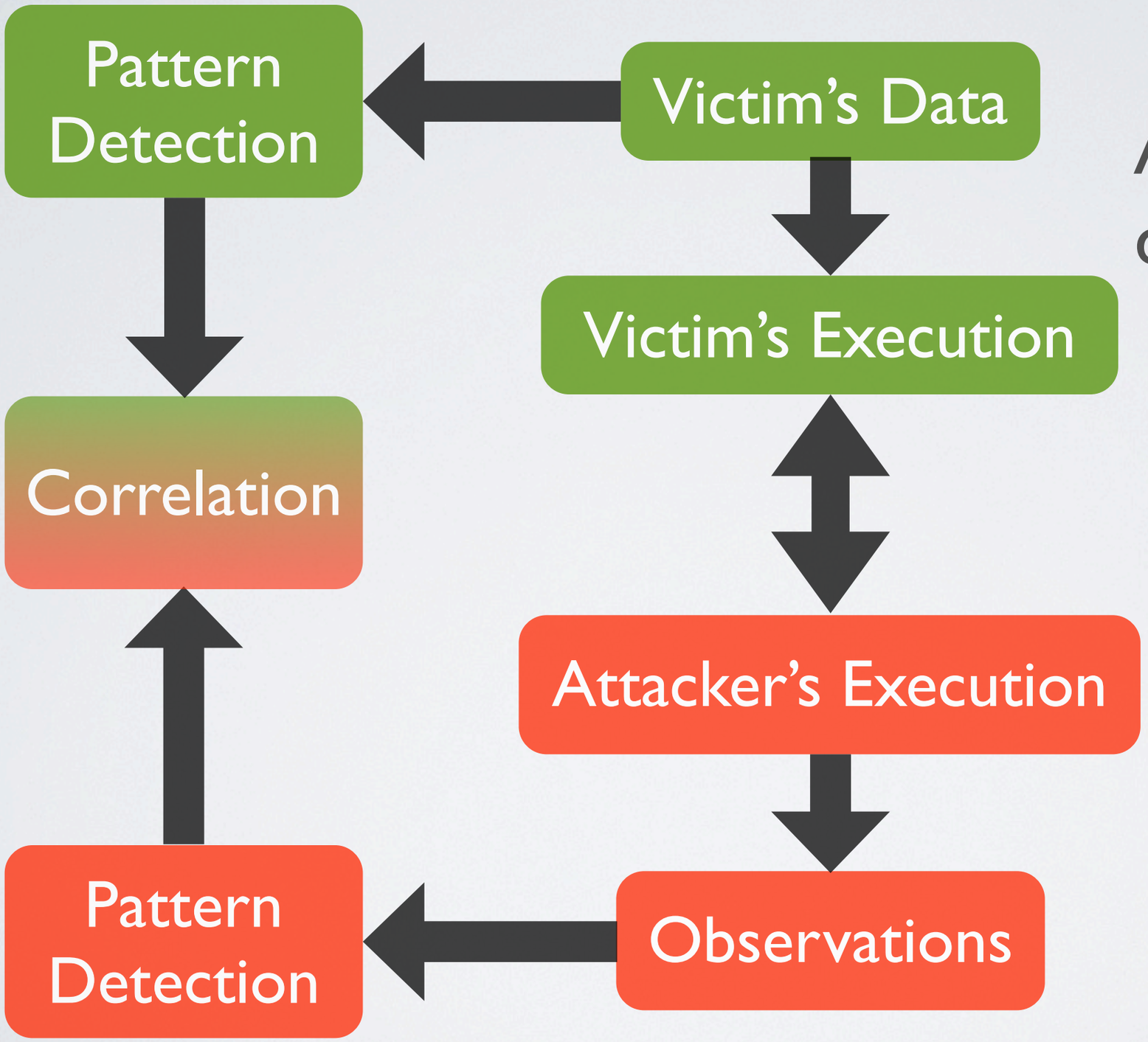
Generalizing Attacks



Limitations

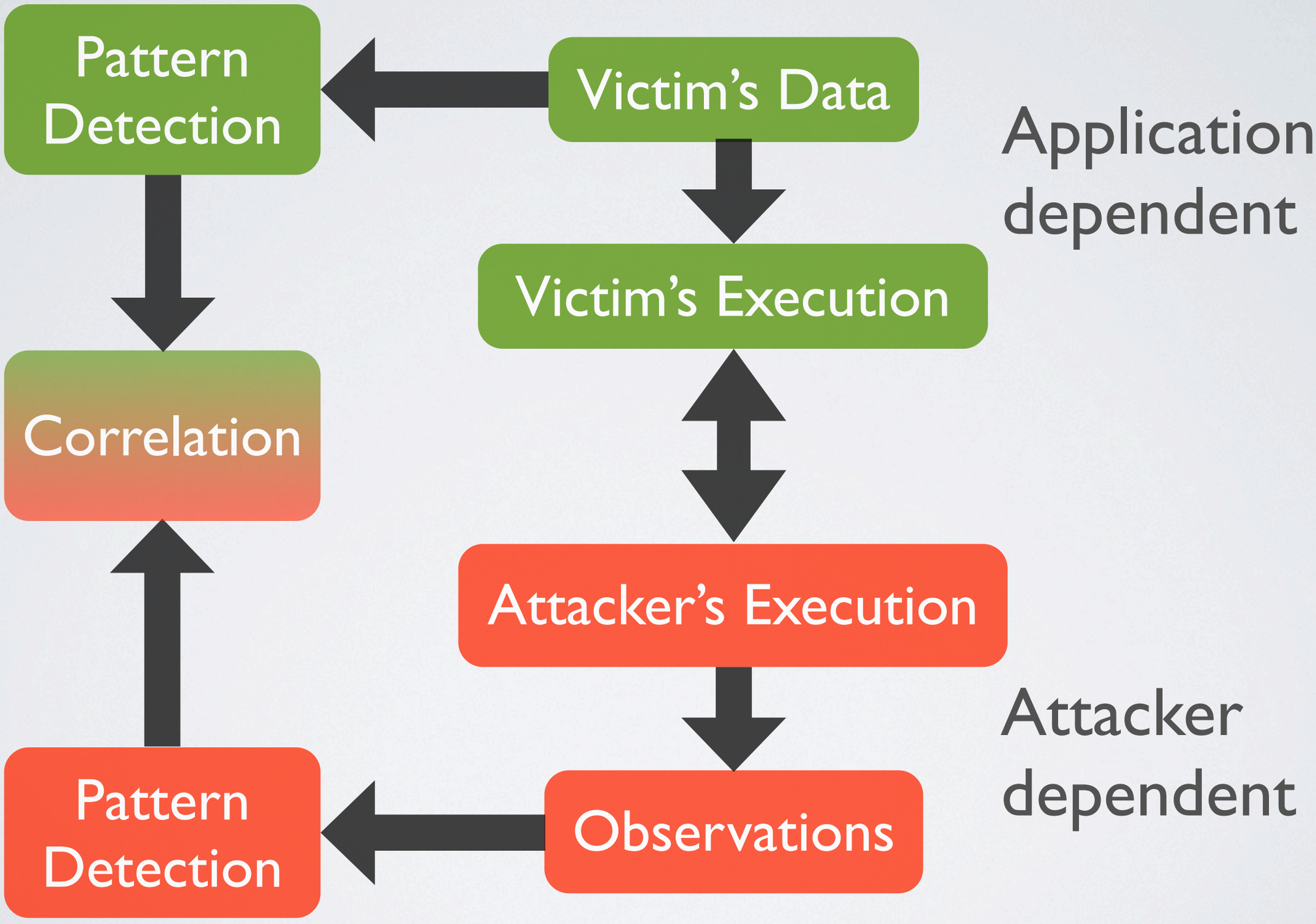


Limitations



Application dependent

Limitations

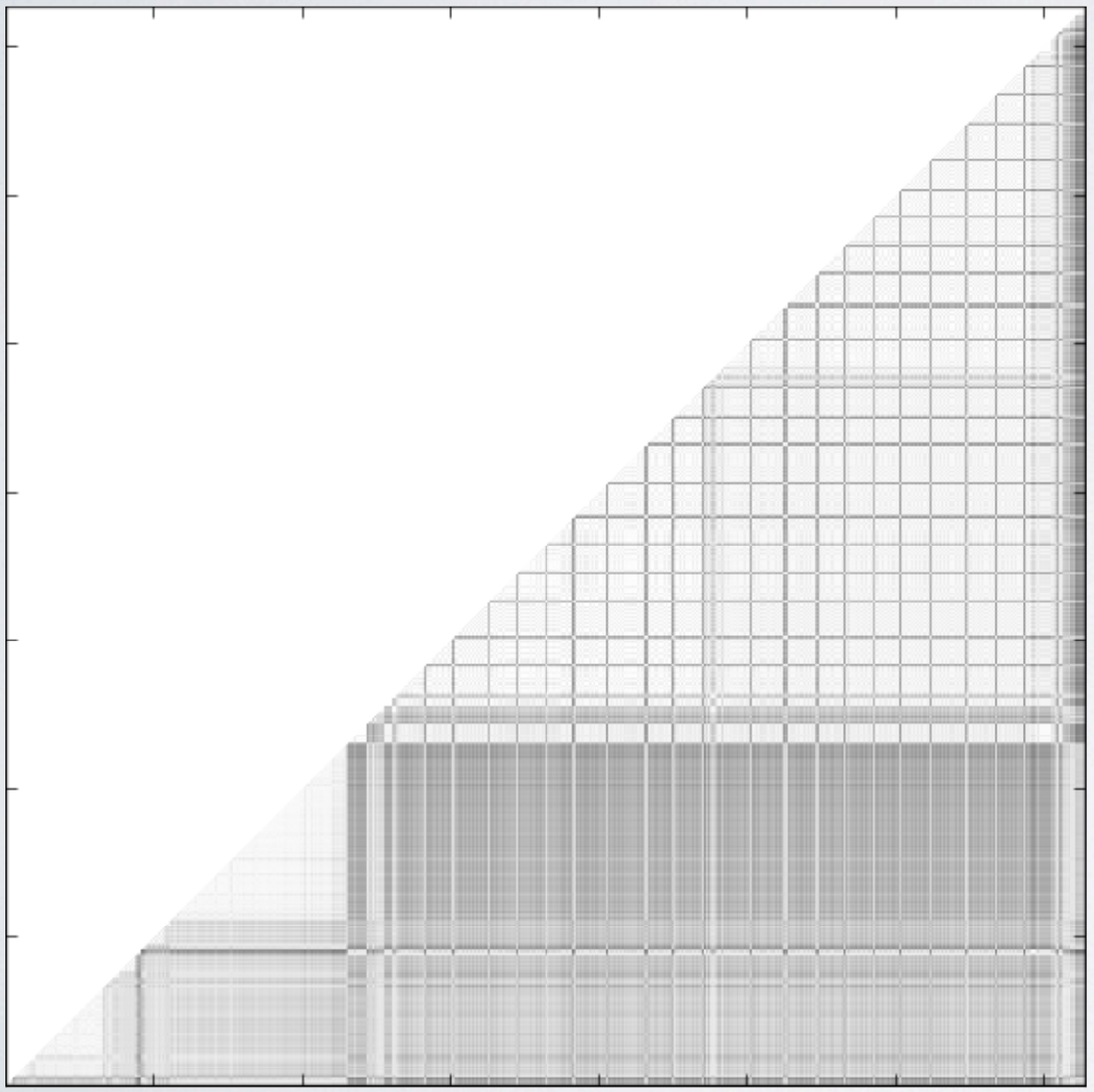


Application dependent

Attacker dependent

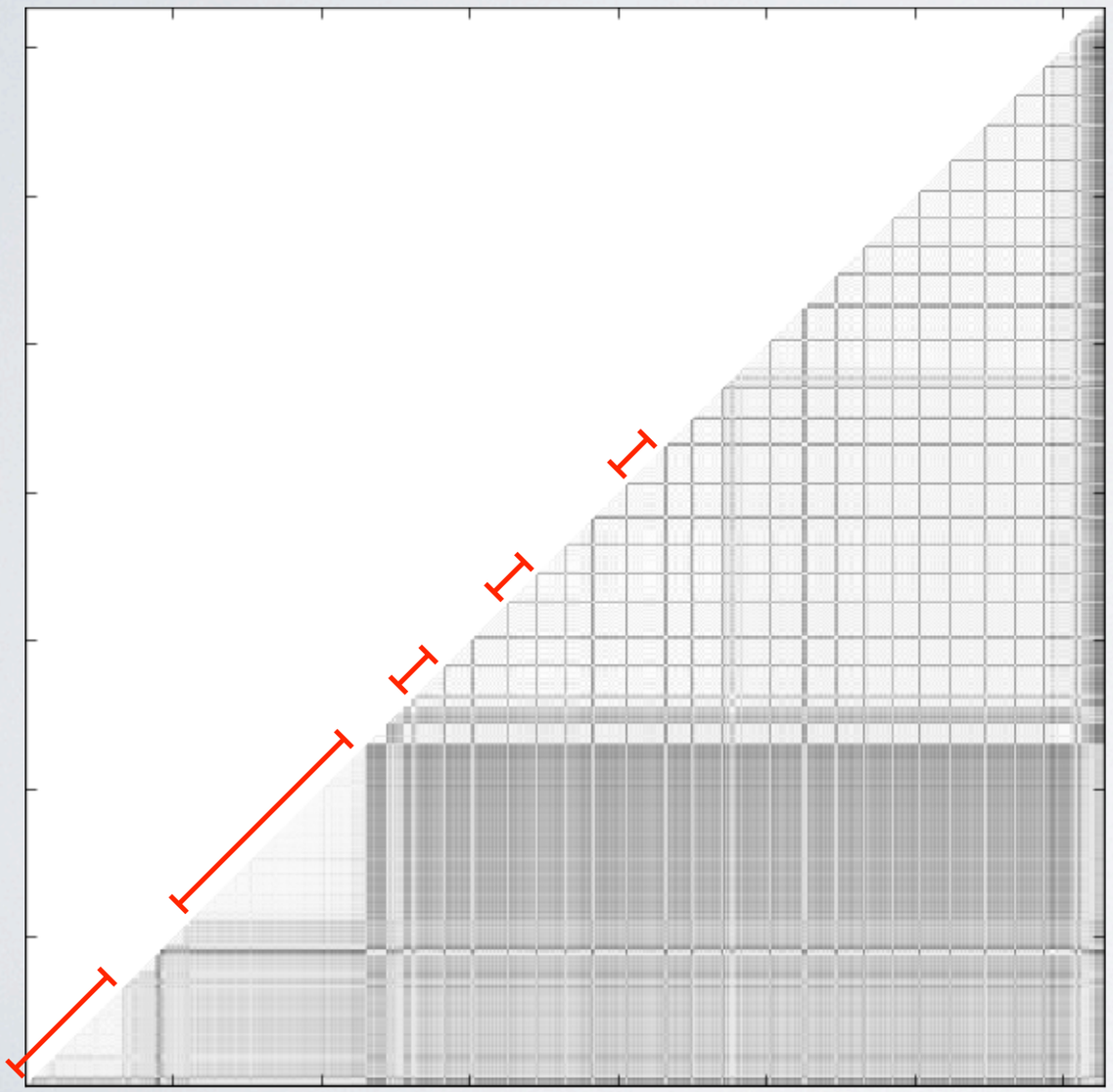
Leaky Example Matrices (0.77)

Oracle



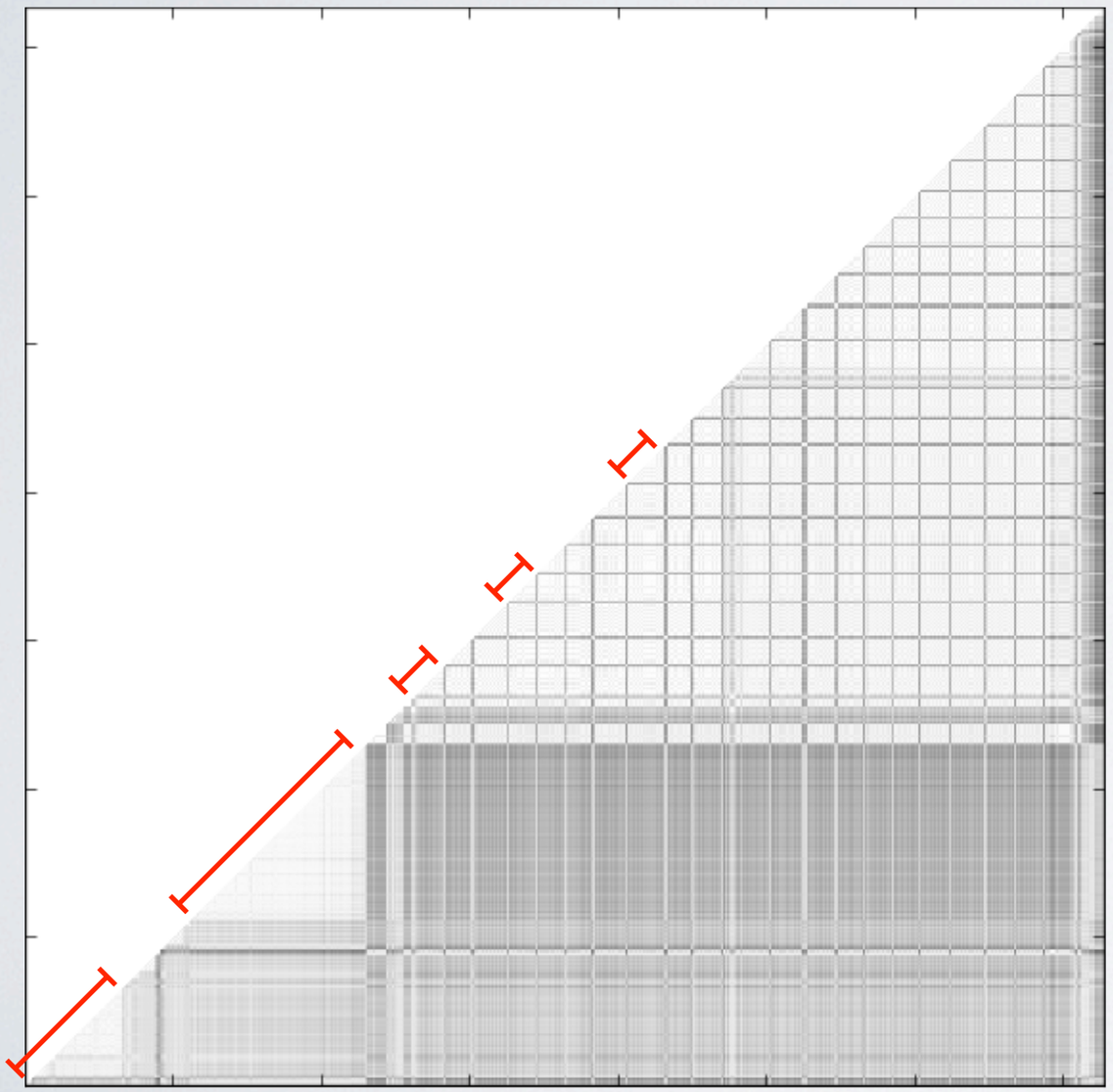
Leaky Example Matrices (0.77)

Oracle

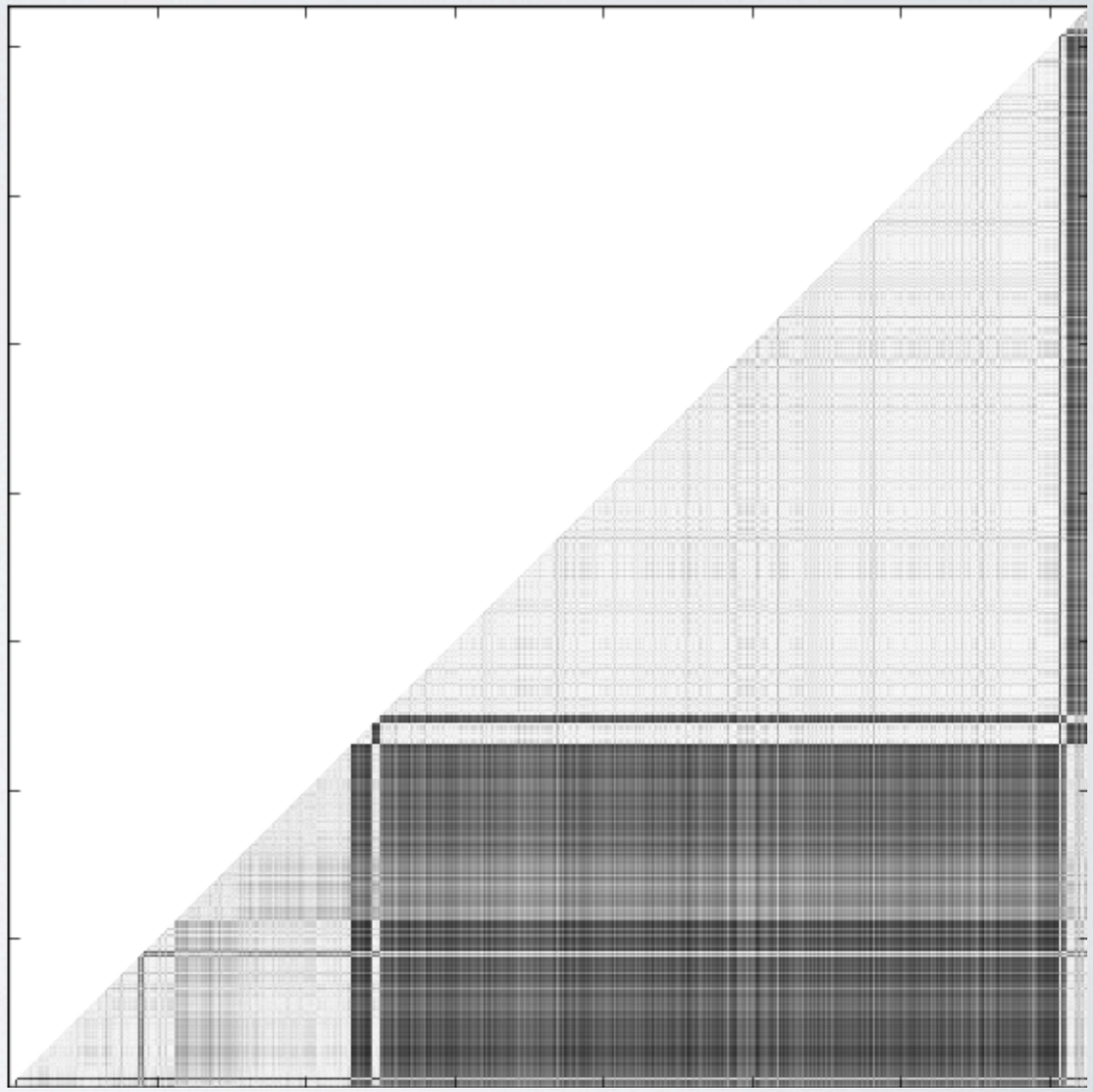


Leaky Example Matrices (0.77)

Oracle

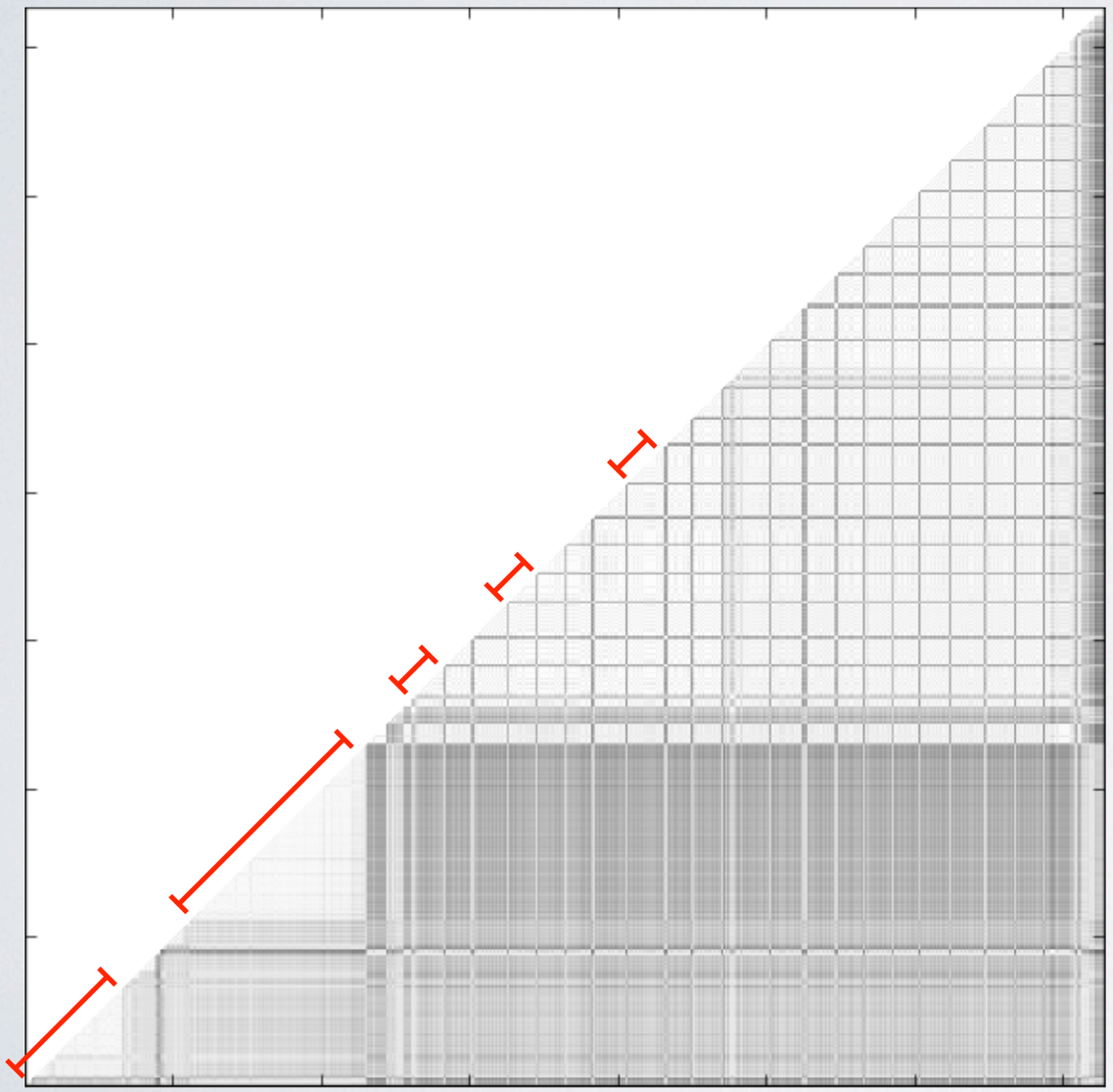


Side Channel

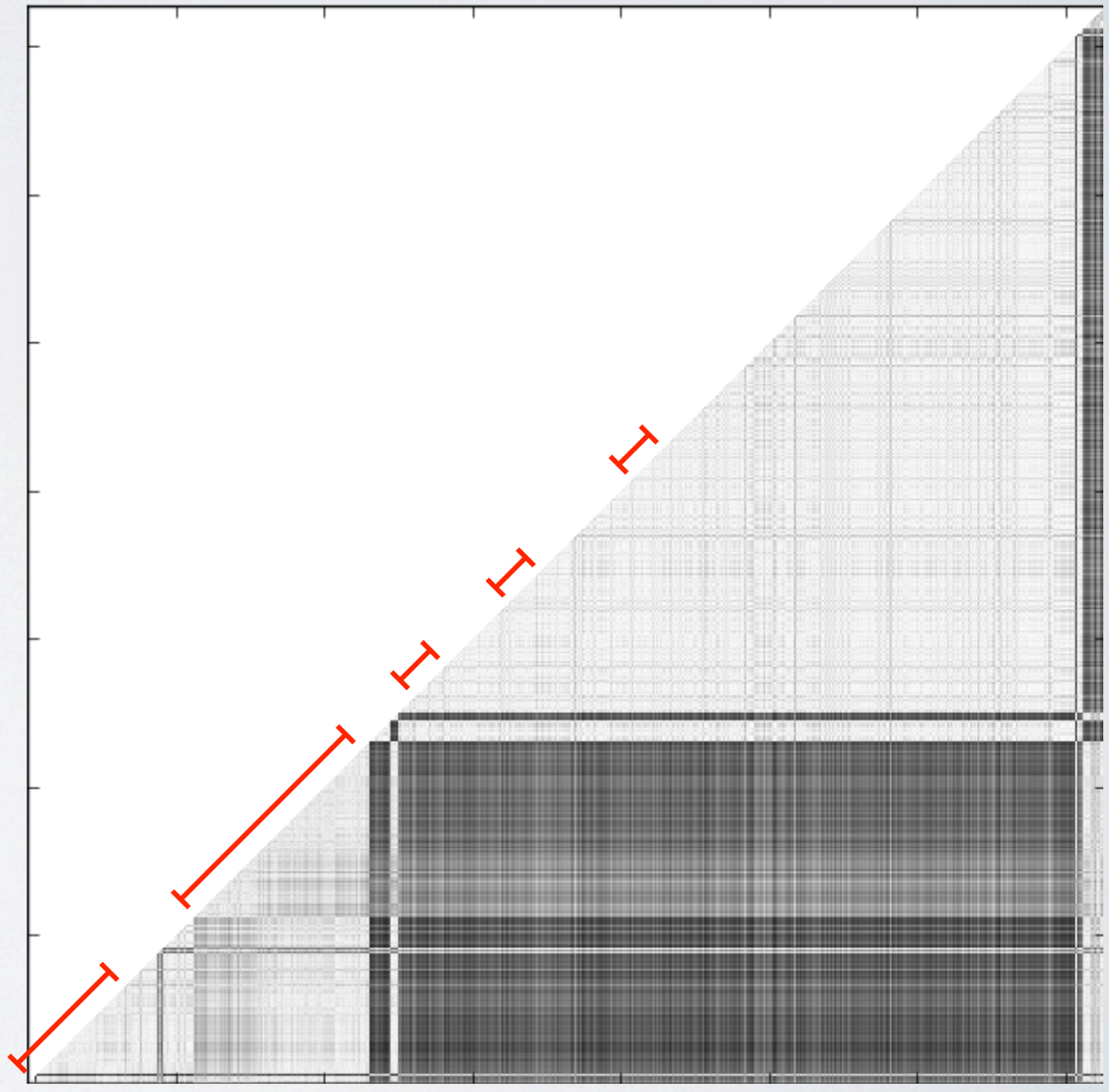


Leaky Example Matrices (0.77)

Oracle

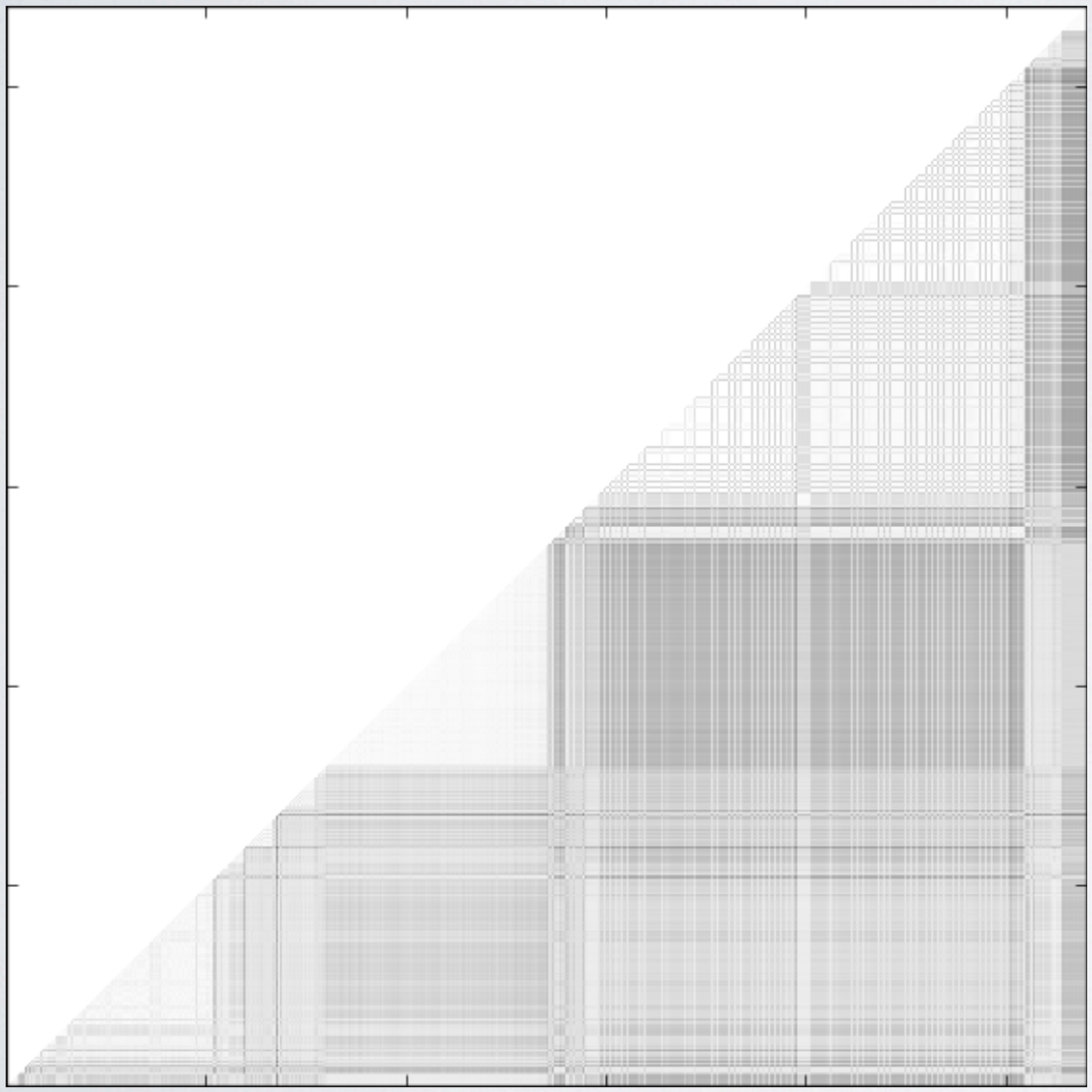


Side Channel

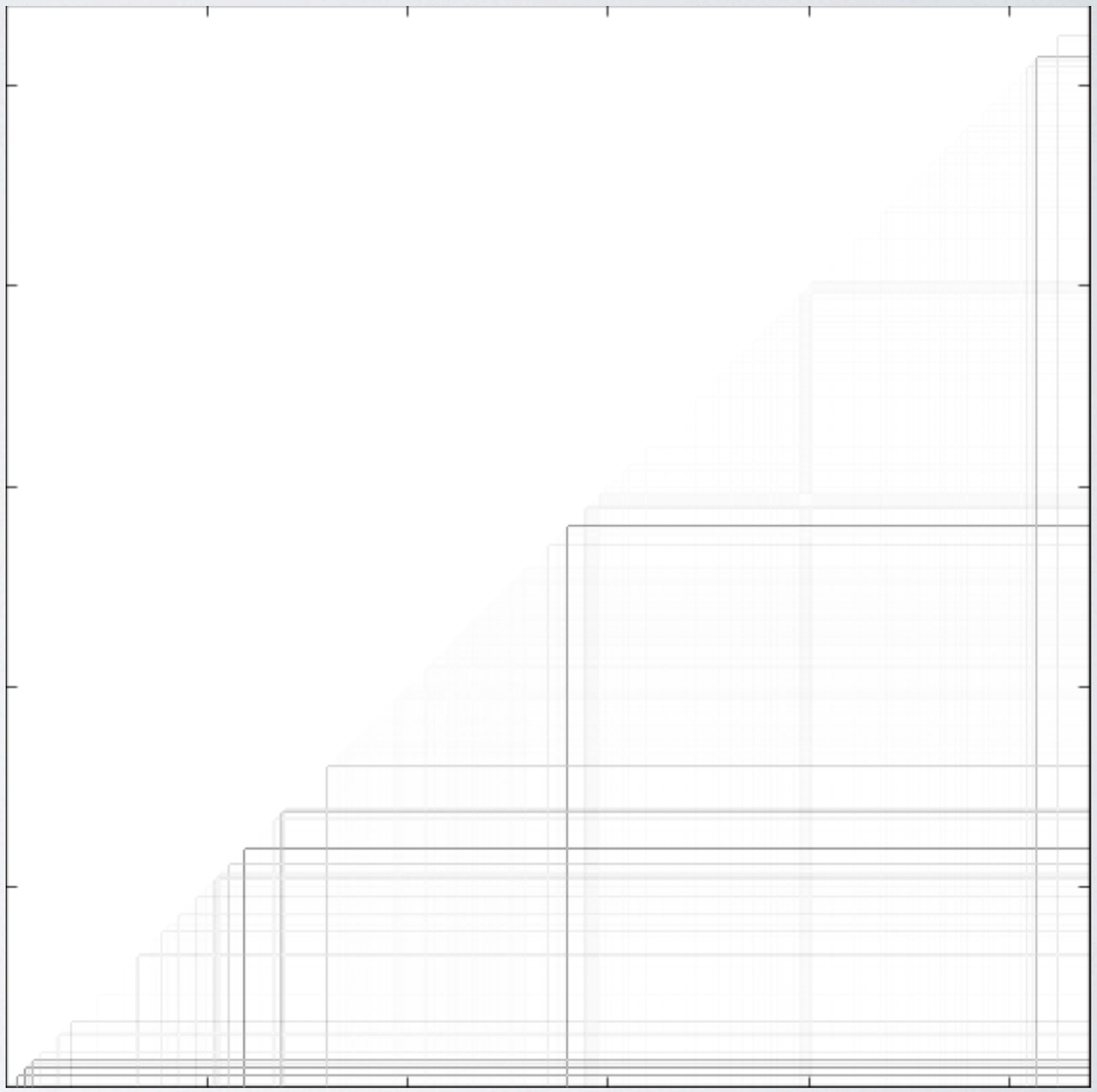


Secure Example Matrices (0.098)

Oracle



Side Channel



Errata / Clarification

- We examine PRS with our policies, not RPCache
- This citation is wrong:
  - [16] Z. Wang and R. B. Lee. New cache designs for thwarting software cache-based side channel attacks. ISCA '07
- It should be:
  - [16] Z. Wang and R. B. Lee. Covert and side channels due to processor architecture. ACSAC '06

Methodology

- Victim: OpenSSL 0.9.8k -- RSA Signing
  - Trace: memory location accesses
    - Indicates working set in memory
- Attackers
  - Cache Scanning Types
    - In order
    - Random
    - Random subset
- Prefetcher
  - Has no effect on attacker, only victim
  - Operates on attacker and victim
- Trace: latency to access each cache set

Simulation Parameters

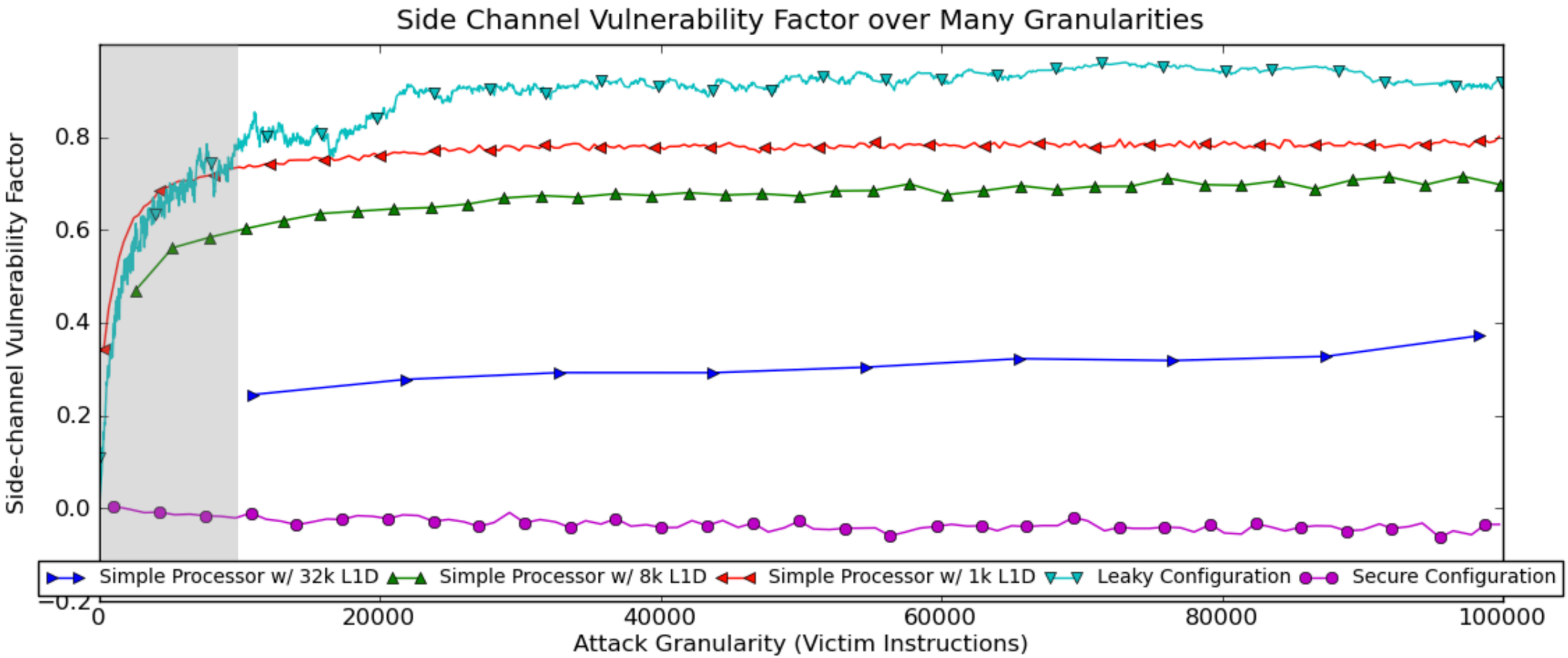
- SMT On/Off
- Cache sharing
  - L1 vs. L2
- Cache size
  - 1k, 8k, 32k L1
  - 8x L2, 256x L3
- Line size
  - 8B, 64B
- Set associativity
  - 1, 4, and 8 way
- Hashing

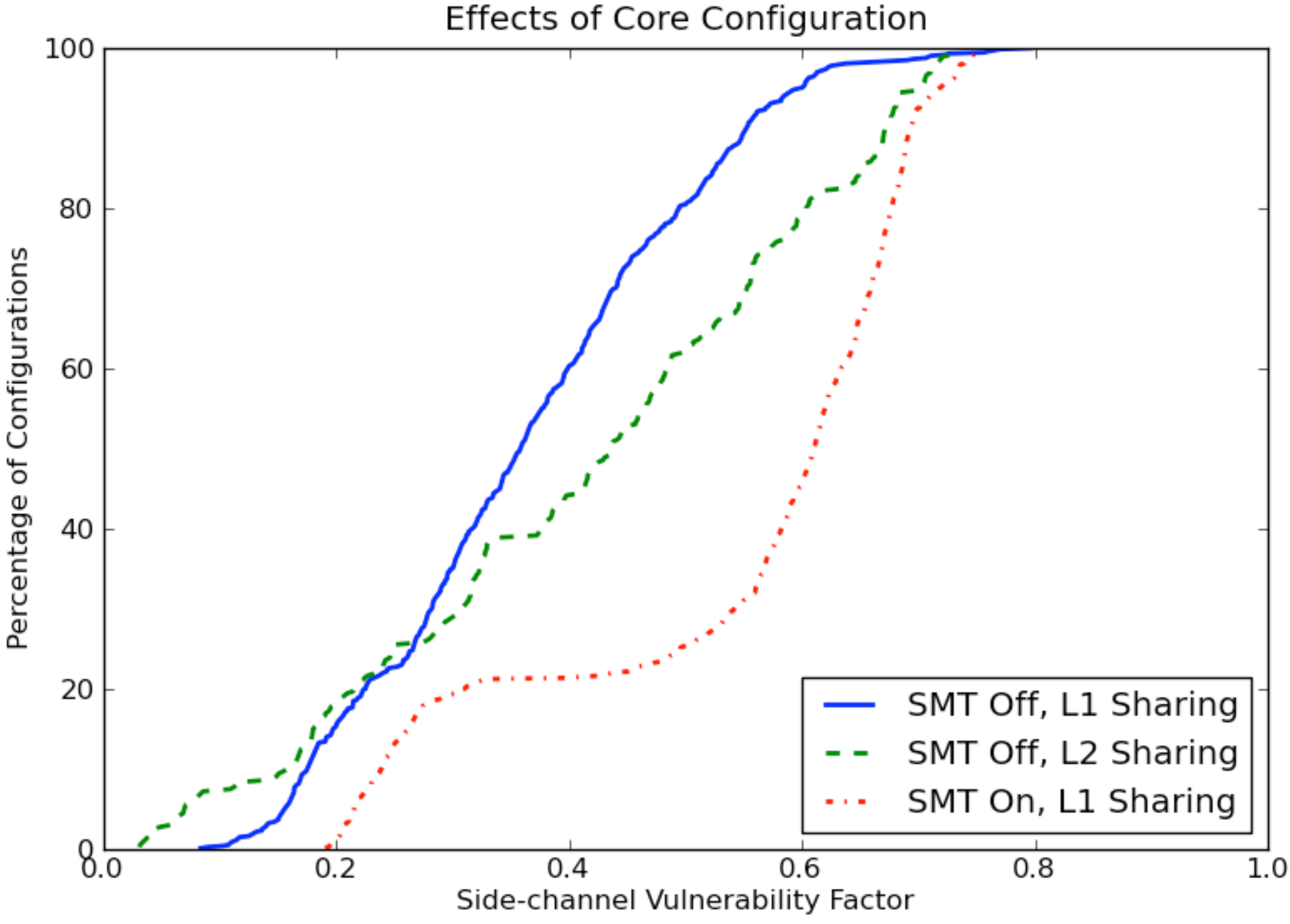
  Low bits, XOR, PRS
- Prefetching

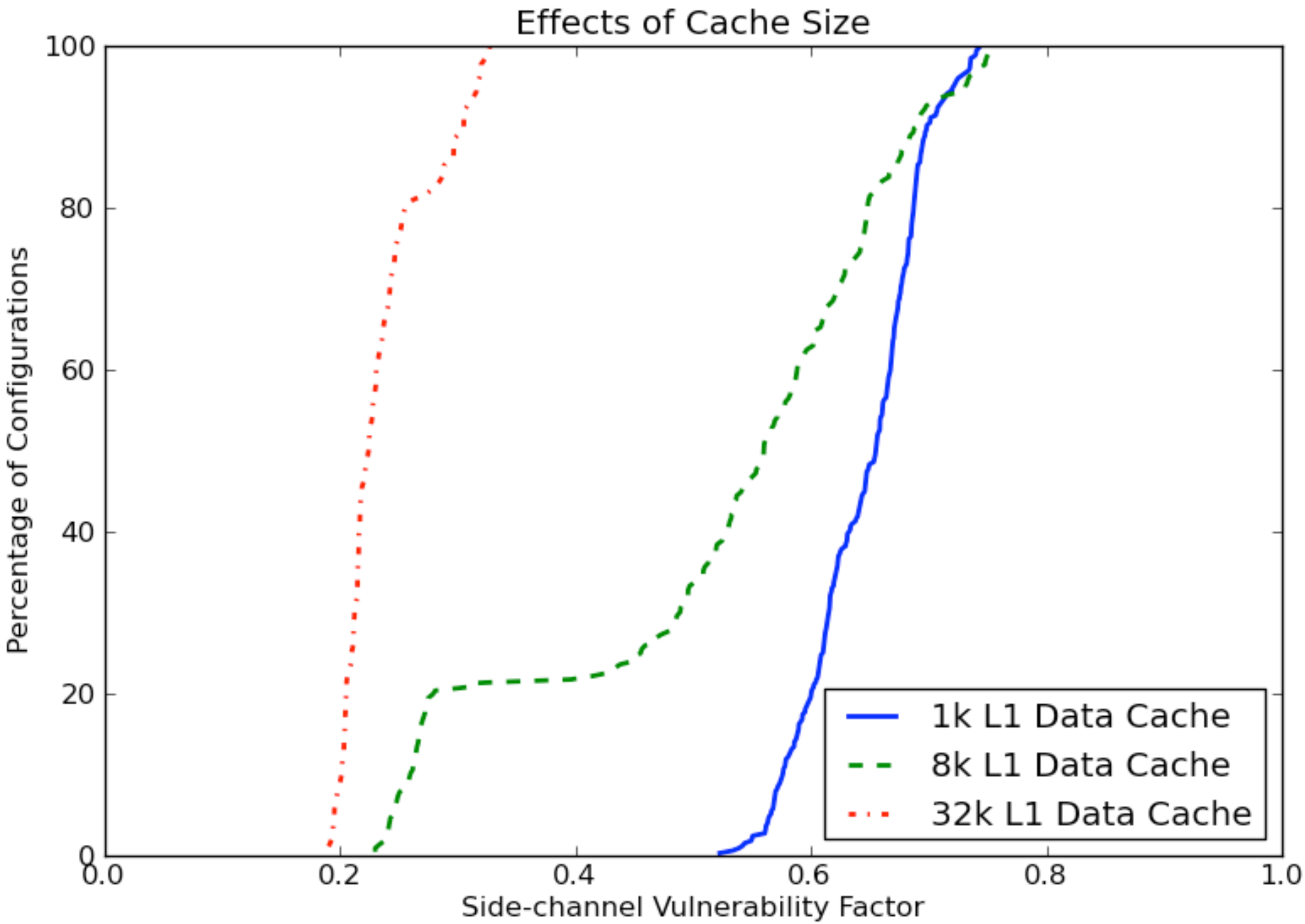
  None, Next line, Arithmetic, GHB/PCCS, GHB/PCDC
- Cache Partitioning

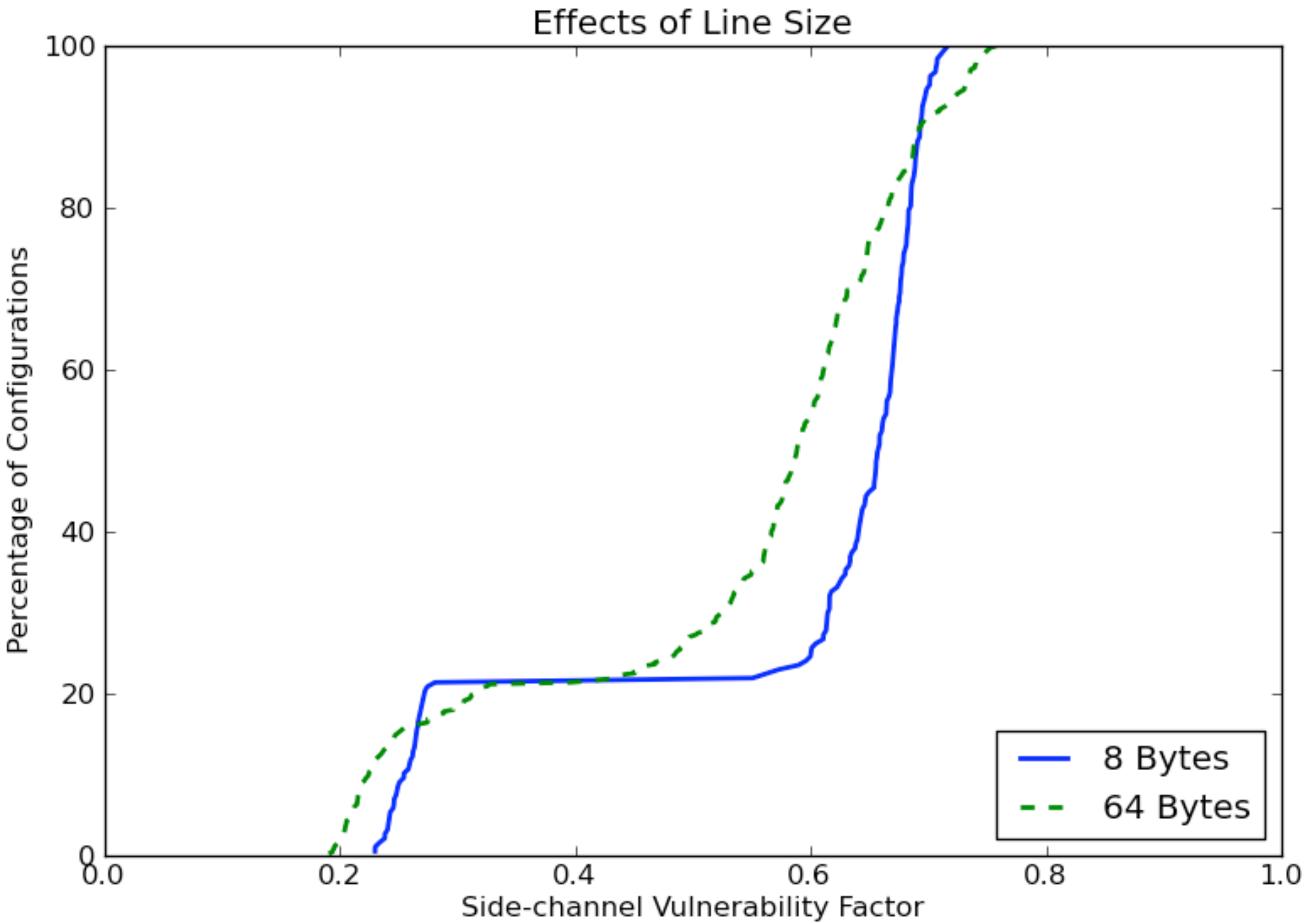
  None, Split, Dynamic
- Random Eviction

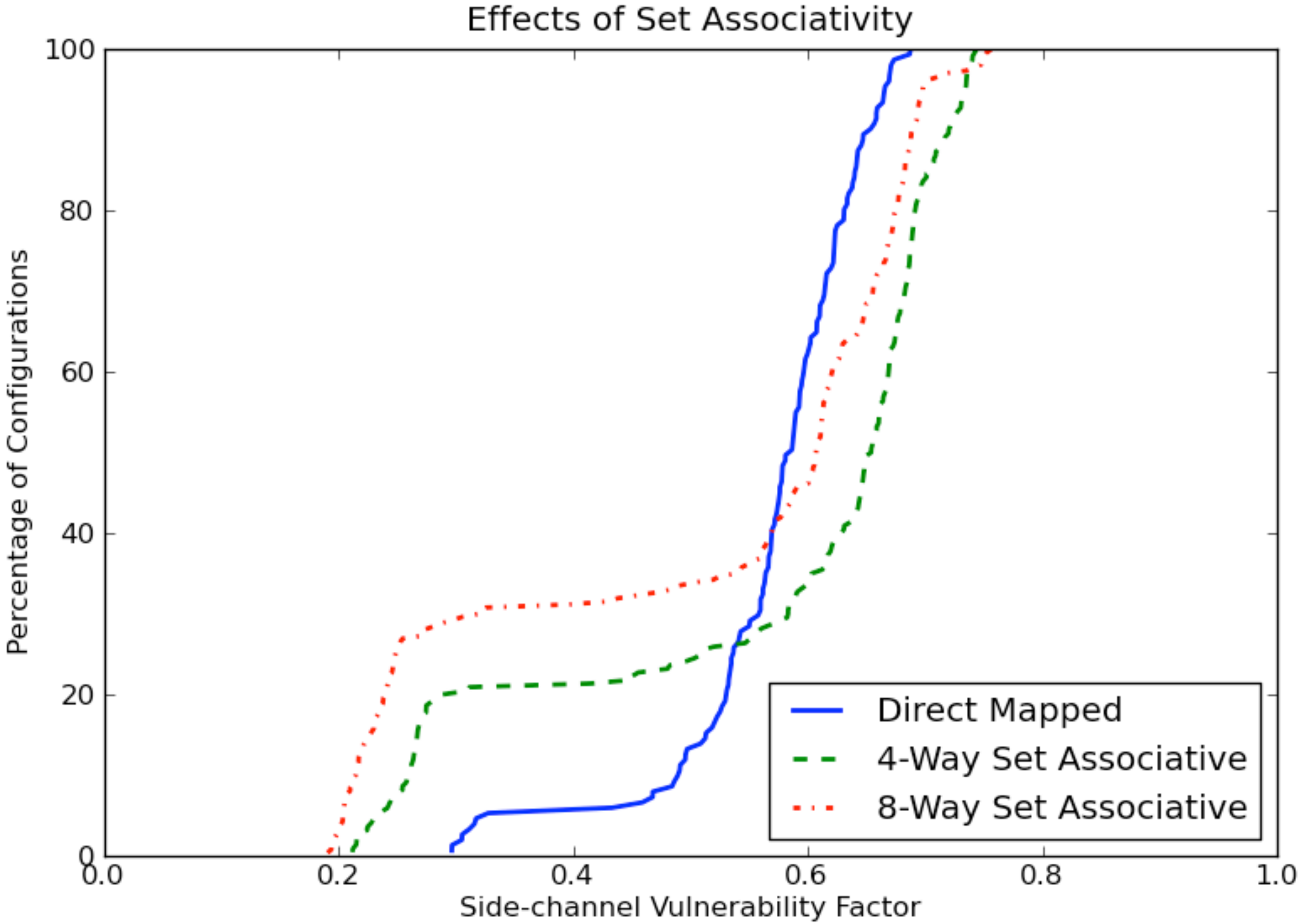
Example Results

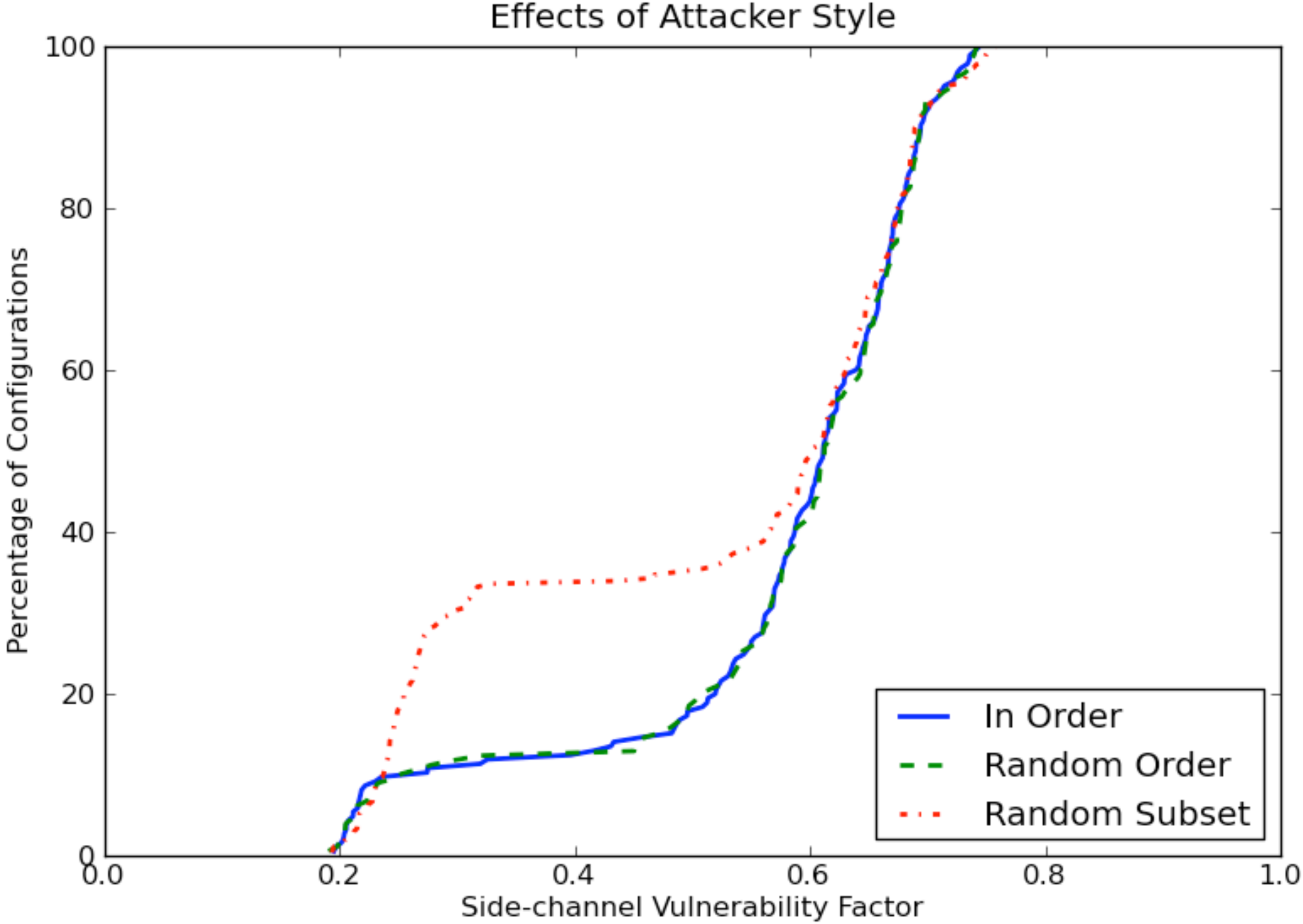


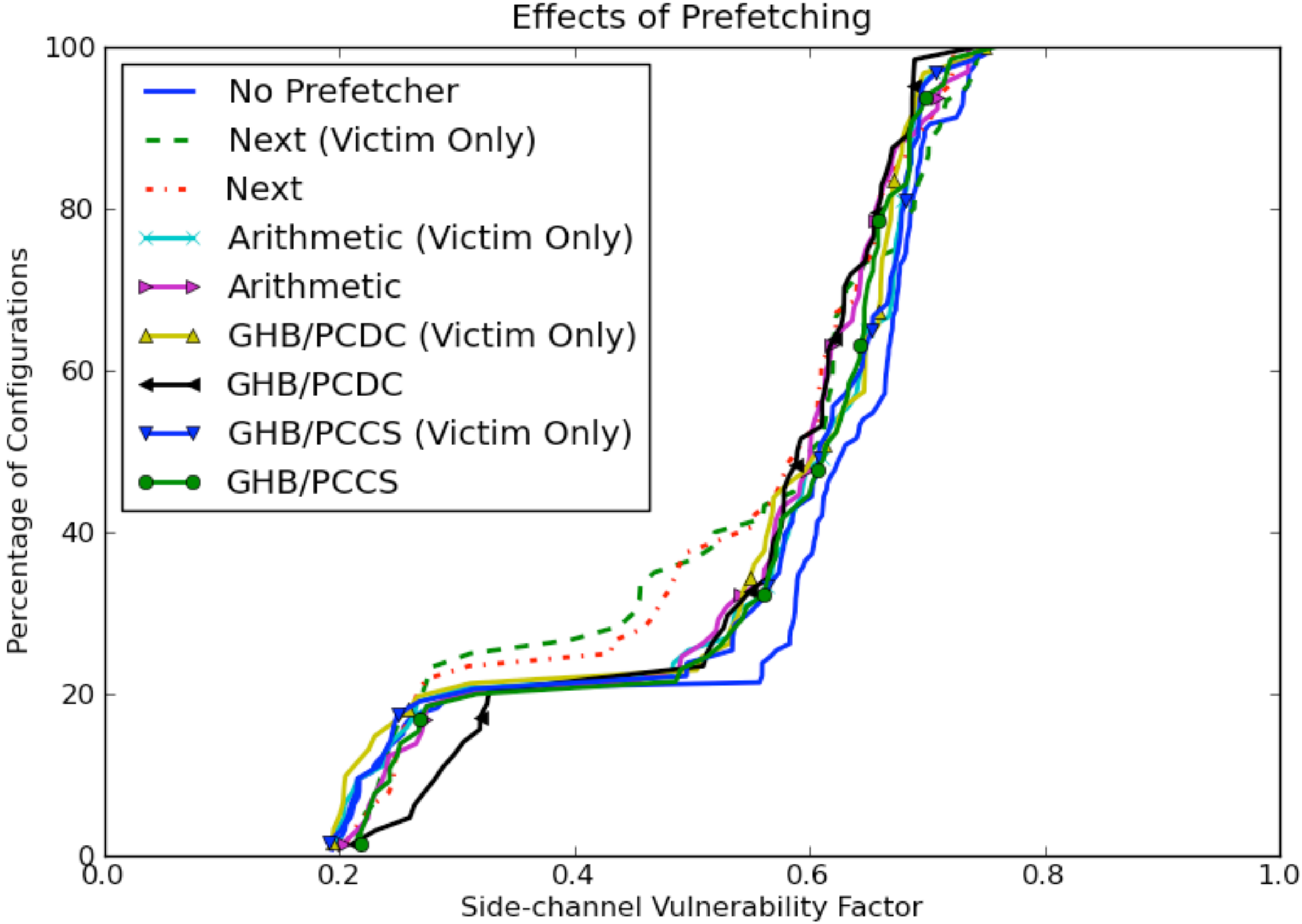

Effects of Core Configuration
Percentage of Configurations
Side-channel Vulnerability Factor
0
20
40
60
80
100
0.0
0.2
0.4
0.6
0.8
1.0
SMT Off, L1 Sharing
SMT Off, L2 Sharing
SMT On, L1 Sharing

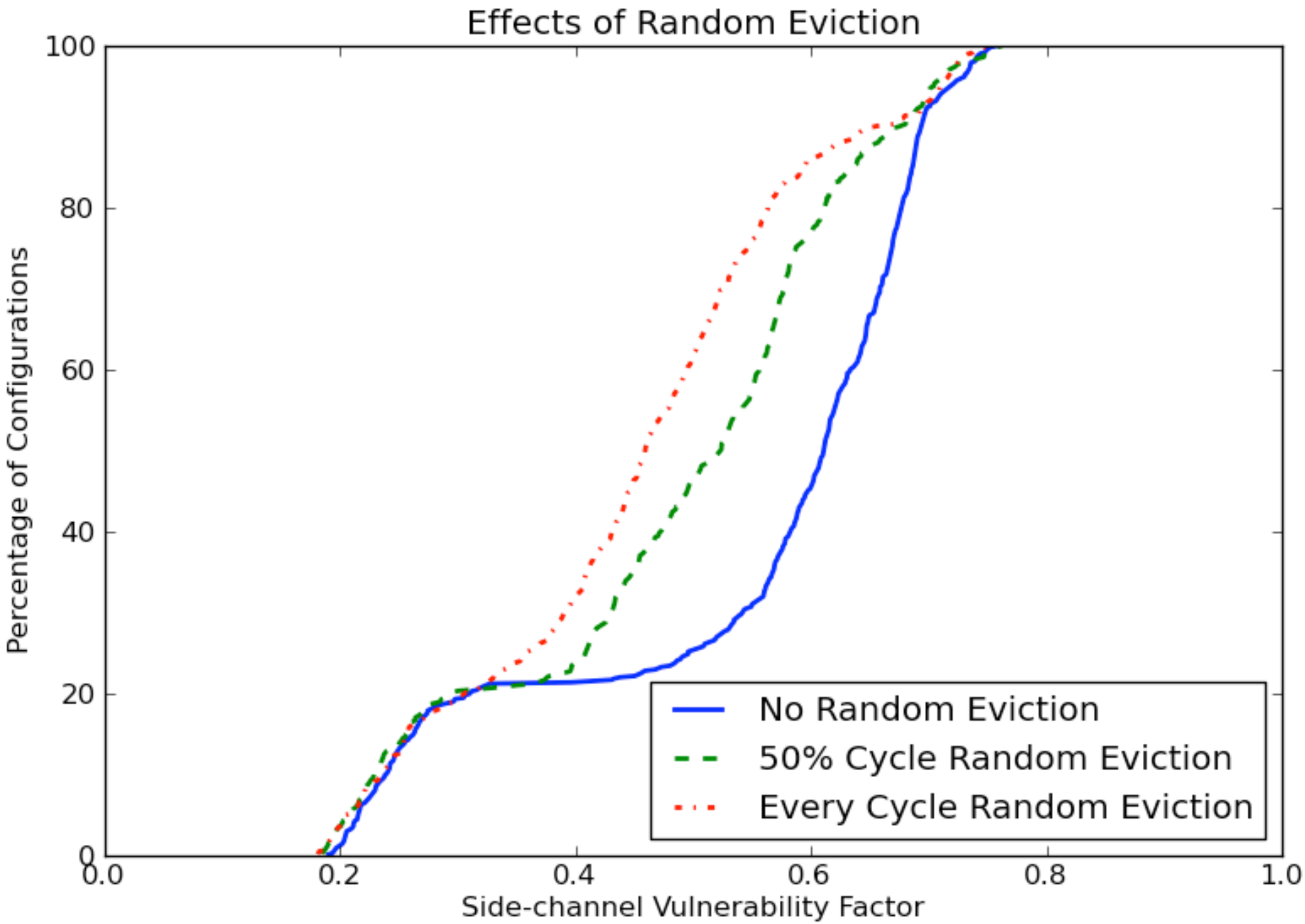

Effects of Cache Size
Percentage of Configurations
Side-channel Vulnerability Factor
0
20
40
60
80
100
0.0
0.2
0.4
0.6
0.8
1.0
1k L1 Data Cache
8k L1 Data Cache
32k L1 Data Cache

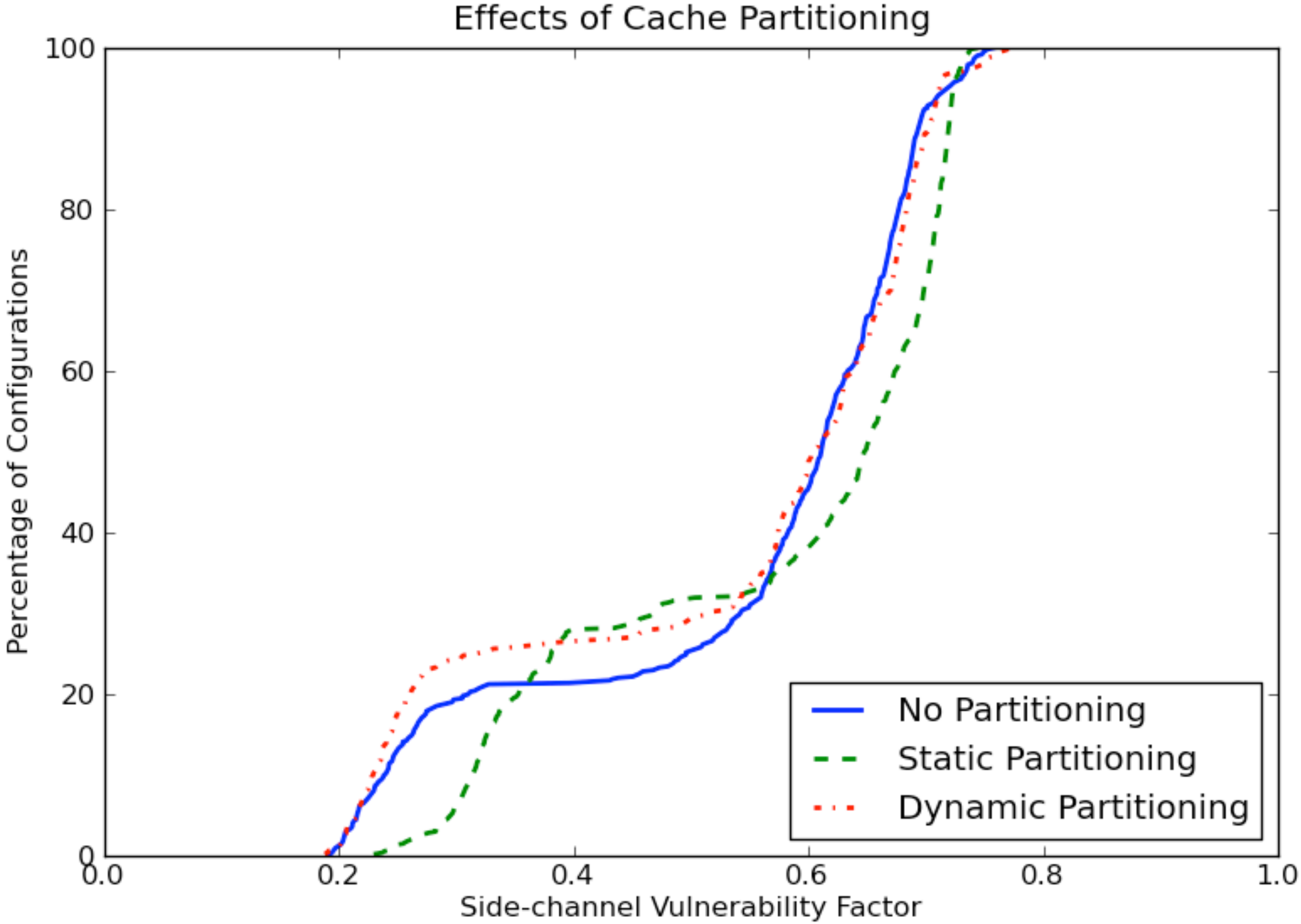

Effects of Line Size
Percentage of Configurations
Side-channel Vulnerability Factor
0
20
40
60
80
100
0.0
0.2
0.4
0.6
0.8
1.0
8 Bytes
64 Bytes

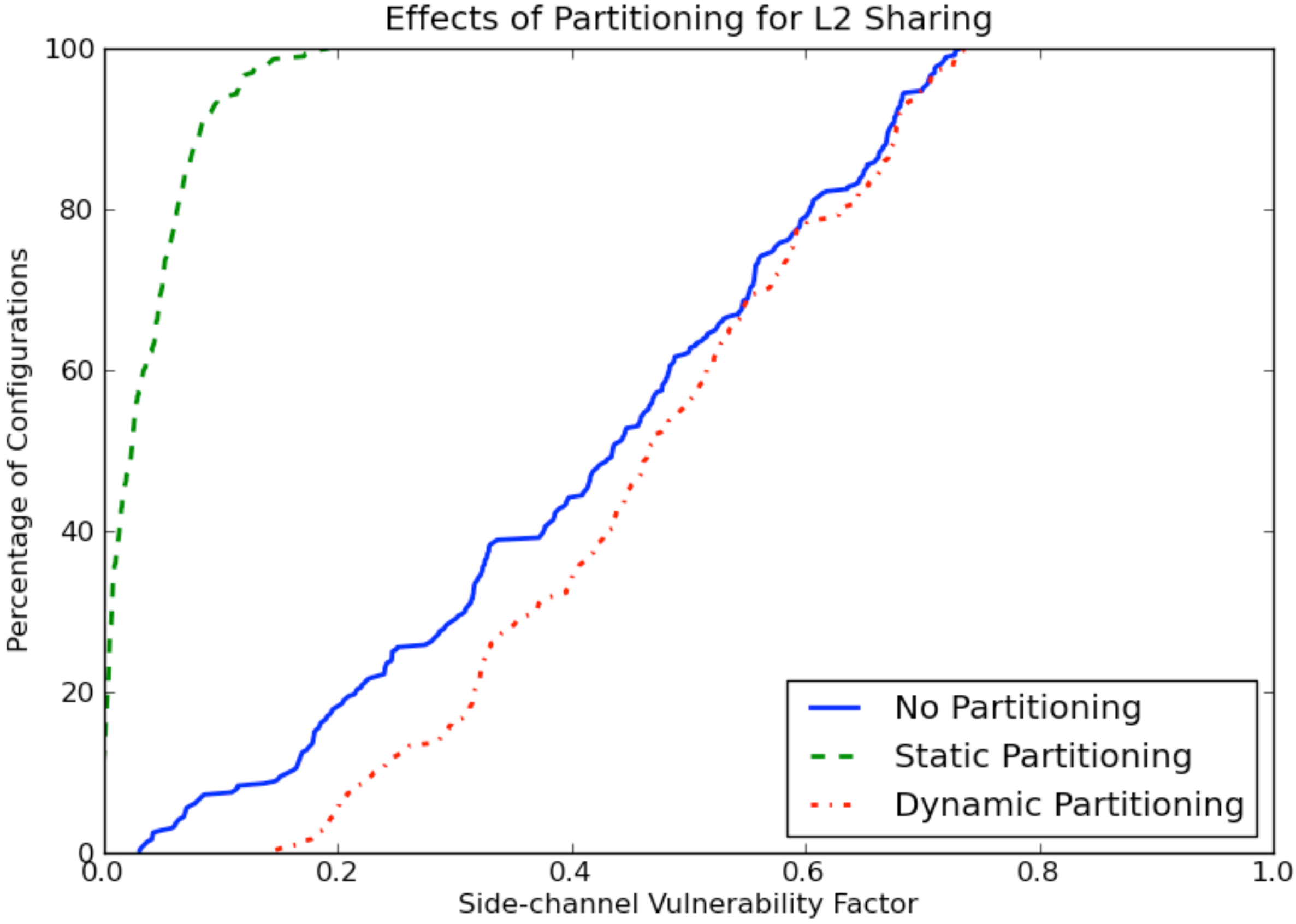

Effects of Set Associativity
Percentage of Configurations
Side-channel Vulnerability Factor
0
20
40
60
80
100
0.0
0.2
0.4
0.6
0.8
1.0
Direct Mapped
4-Way Set Associative
8-Way Set Associative

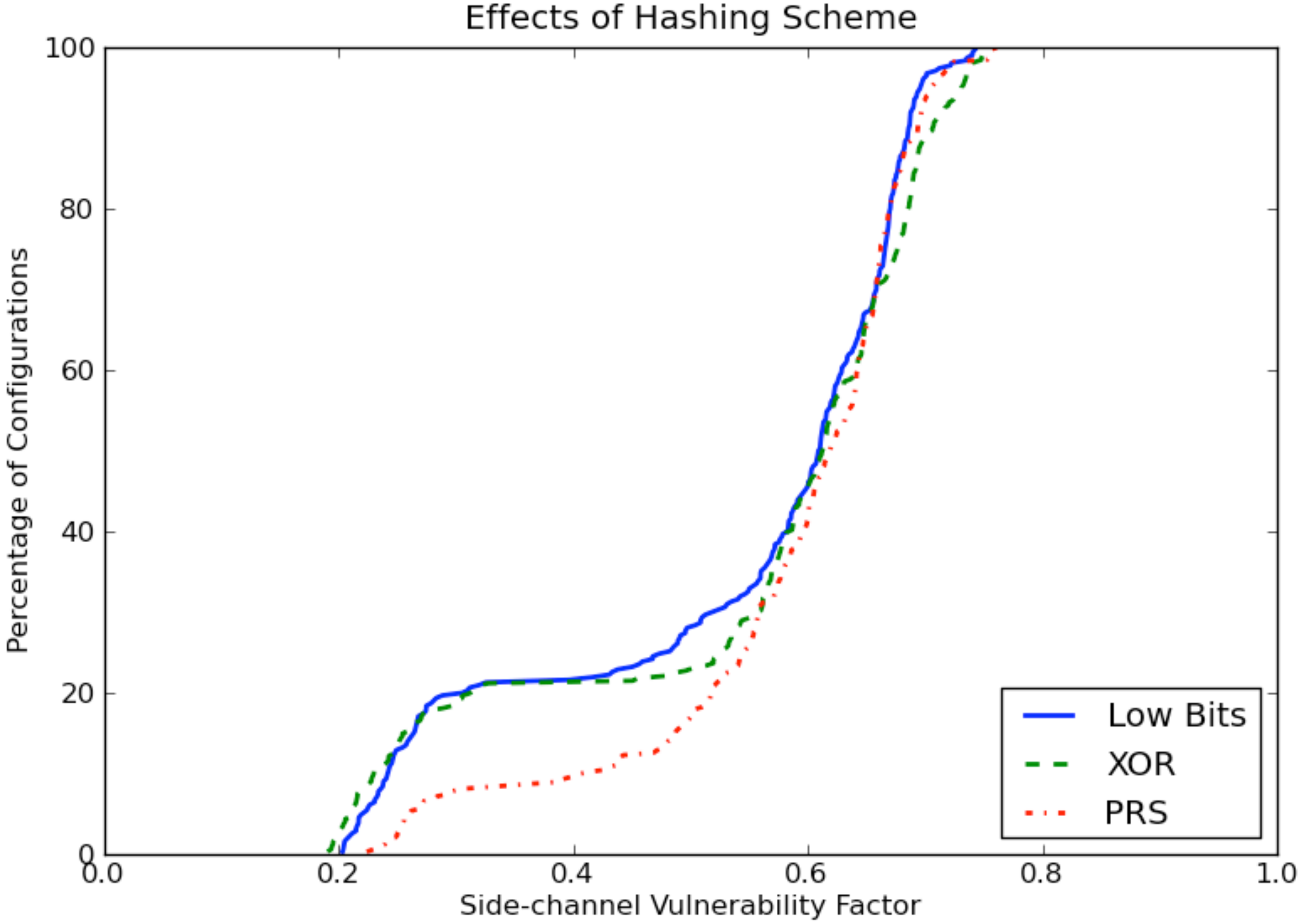

Effects of Attacker Style
Percentage of Configurations
Side-channel Vulnerability Factor
0
20
40
60
80
100
0.0
0.2
0.4
0.6
0.8
1.0
In Order
Random Order
Random Subset

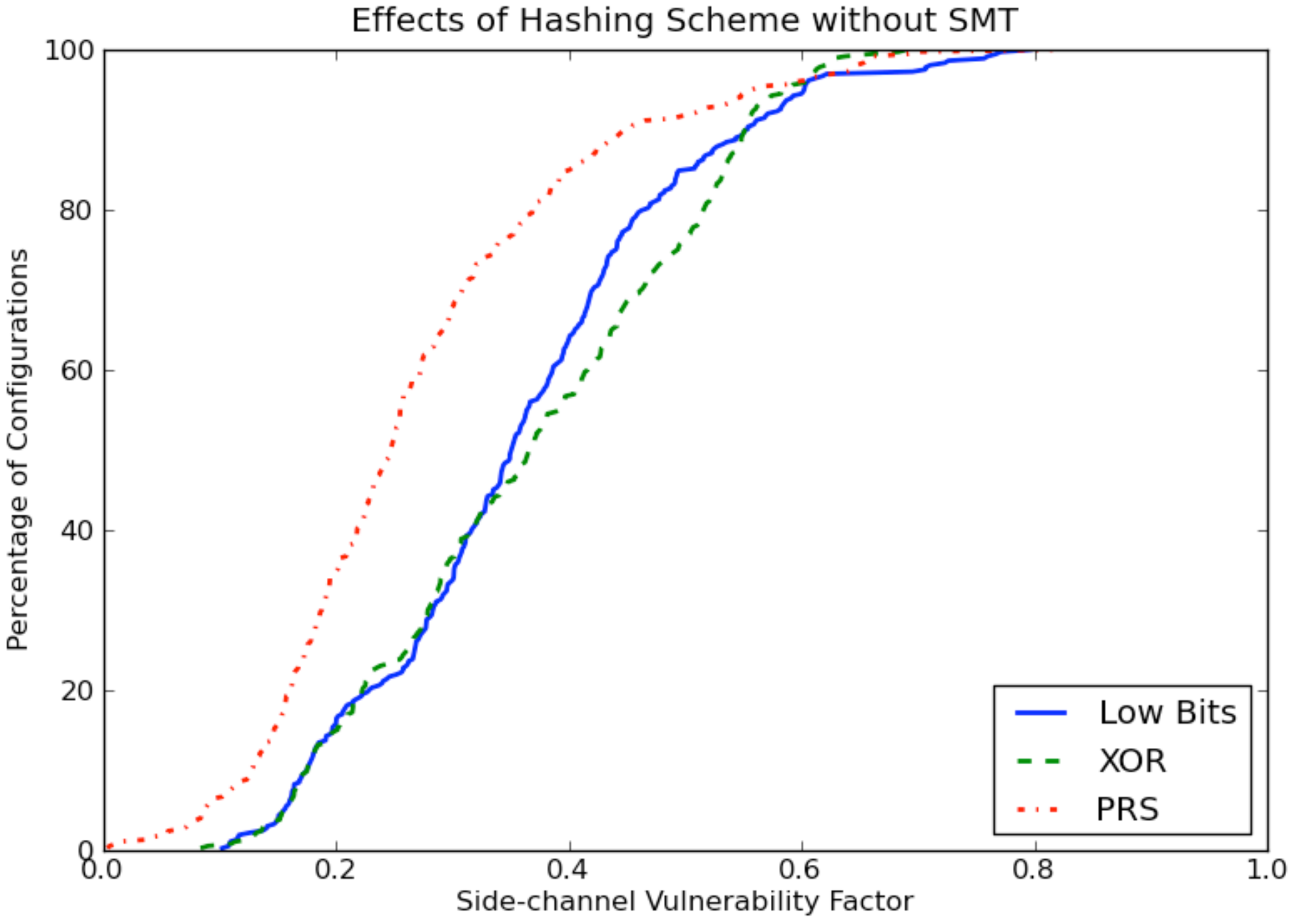

Effects of Prefetching
No Prefetcher
Next (Victim Only)
Next
Arithmetic (Victim Only)
Arithmetic
GHB/PCDC (Victim Only)
GHB/PCDC
GHB/PCCS (Victim Only)
GHB/PCCS
Percentage of Configurations
Side-channel Vulnerability Factor
0
20
40
60
80
100
0.0
0.2
0.4
0.6
0.8
1.0

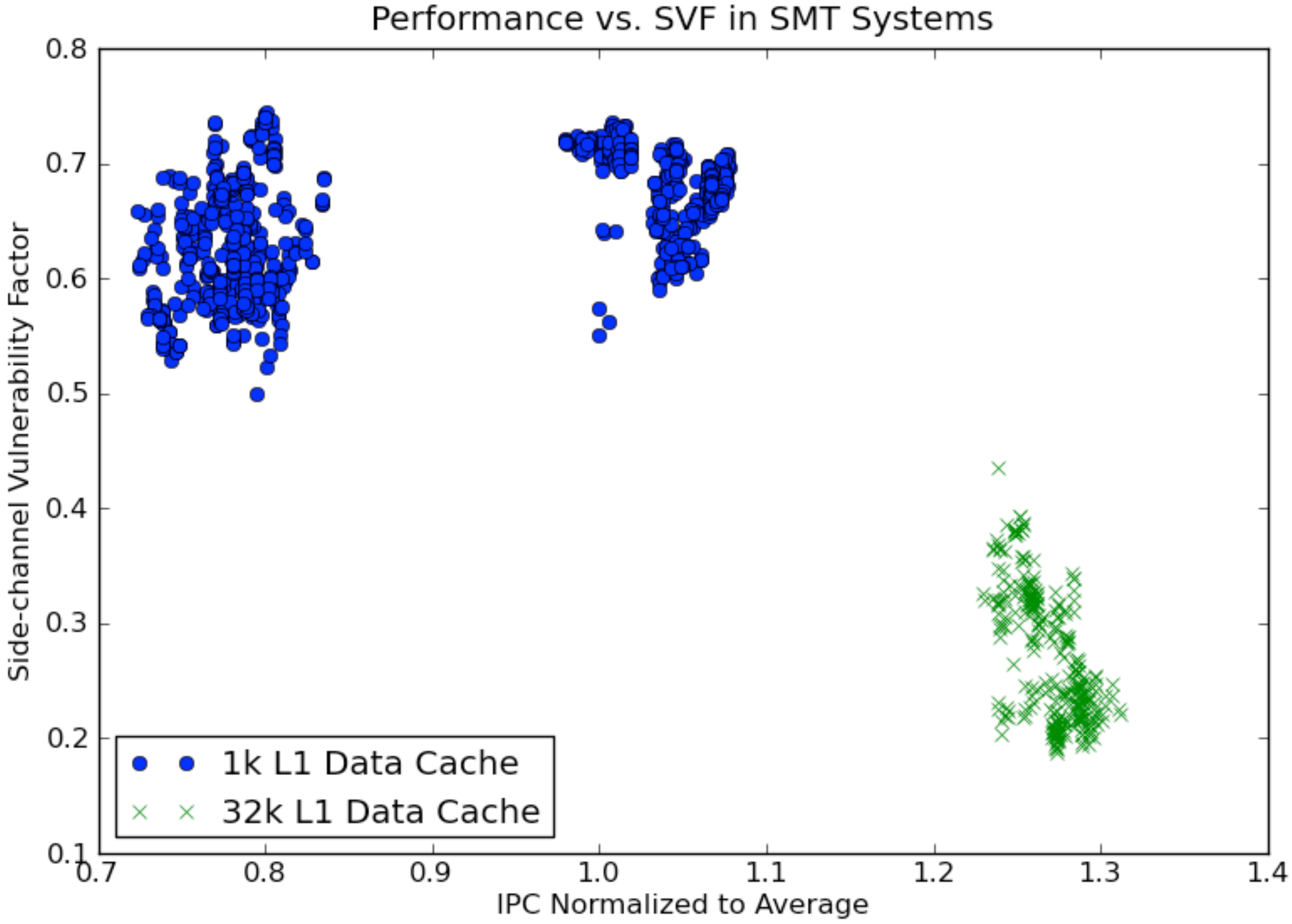

Effects of Random Eviction
Percentage of Configurations
Side-channel Vulnerability Factor
0
20
40
60
80
100
0.0
0.2
0.4
0.6
0.8
1.0
No Random Eviction
50% Cycle Random Eviction
Every Cycle Random Eviction

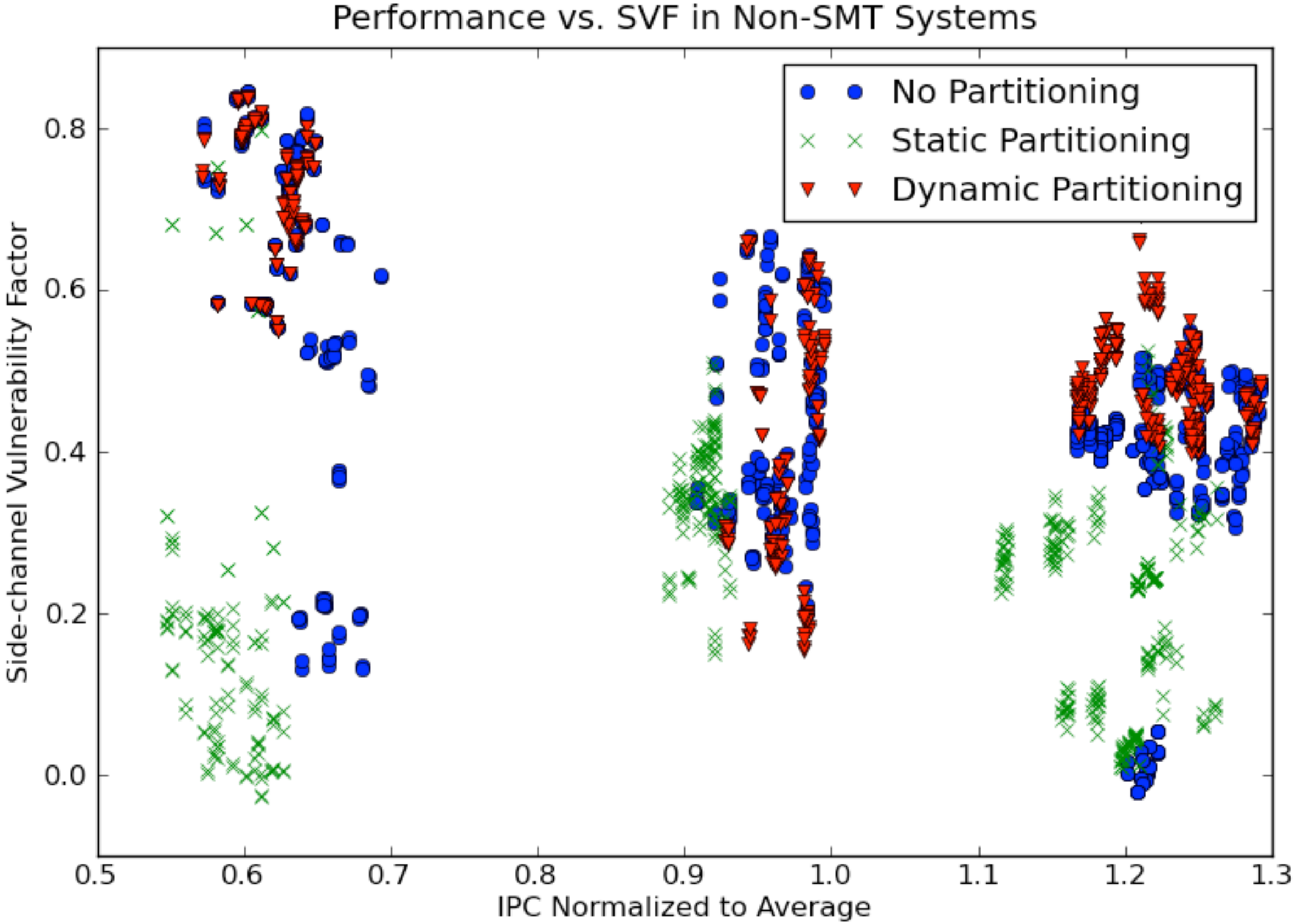

Effects of Cache Partitioning
Percentage of Configurations
Side-channel Vulnerability Factor
0
20
40
60
80
100
0.0
0.2
0.4
0.6
0.8
1.0
No Partitioning
Static Partitioning
Dynamic Partitioning


Effects of Partitioning for L2 Sharing
Percentage of Configurations
Side-channel Vulnerability Factor
0
20
40
60
80
100
0.0
0.2
0.4
0.6
0.8
1.0
No Partitioning
Static Partitioning
Dynamic Partitioning


Effects of Hashing Scheme
Percentage of Configurations
Side-channel Vulnerability Factor
0
20
40
60
80
100
0.0
0.2
0.4
0.6
0.8
1.0
Low Bits
XOR
PRS


Effects of Hashing Scheme without SMT
Percentage of Configurations
Side-channel Vulnerability Factor
0
20
40
60
80
100
0.0
0.2
0.4
0.6
0.8
1.0
Low Bits
XOR
PRS


Performance vs. SVF in SMT Systems
Side-channel Vulnerability Factor
IPC Normalized to Average
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.7
0.8
0.9
1.0
1.1
1.2
1.3
1.4
1k L1 Data Cache
32k L1 Data Cache


Performance vs. SVF in Non-SMT Systems
No Partitioning
Static Partitioning
Dynamic Partitioning
Side-channel Vulnerability Factor
0.0
0.2
0.4
0.6
0.8
0.5
0.6
0.7
0.8
0.9
1.0
1.1
1.2
1.3
IPC Normalized to Average