PowerHooK:
Enabling Software-Based Power Side Channels Against AMD SEV Technologies via Transient-Execution Replay

SCIENCE
PASSION
TECHNOLOGY

Mathias Oberhuber[1] Martin Unterguggenberger[1] Martin Wistauder[1]
Andreas Kogler[2] Rishub Nagpal[1] Stefan Mangard[1]

[1]Graz University of Technology [2]Graz University of Technology Alumni

› isec.tugraz.at

About

Transient-replay power side channels against **AMD SEV VMs**

About

Transient-replay power side channels against **AMD SEV VMs**

- Denoising software-based power side channels:
  - Malicious hypervisor uses a transient-replay gadget to amplify and denoise transient power traces
  - Enables single-run power side-channel attacks against VMs protected by AMD SEV technologies

About

Transient-replay power side channels against **AMD SEV VMs**

- Denoising software-based power side channels:
  - Malicious hypervisor uses a transient-replay gadget to amplify and denoise transient power traces
  - Enables single-run power side-channel attacks against VMs protected by AMD SEV technologies
- Systematic leakage analysis:
  - Comparing architectural, speculative, and transient power leakage across VM boundaries

About

Transient-replay power side channels against **AMD SEV VMs**

- Denoising software-based power side channels:
  - Malicious hypervisor uses a transient-replay gadget to amplify and denoise transient power traces
  - Enables single-run power side-channel attacks against VMs protected by AMD SEV technologies
- Systematic leakage analysis:
  - Comparing architectural, speculative, and transient power leakage across VM boundaries
- Leakage Characterization:
  - Synthetic first-round AES-NI CPA attack benchmark across AMD-V, SEV, SEV-ES, SEV-SNP.

About

Transient-replay power side channels against **AMD SEV VMs**

- Denoising software-based power side channels:
  - Malicious hypervisor uses a transient-replay gadget to amplify and denoise transient power traces
  - Enables single-run power side-channel attacks against VMs protected by AMD SEV technologies
- Systematic leakage analysis:
  - Comparing architectural, speculative, and transient power leakage across VM boundaries
- Leakage Characterization:
  - Synthetic first-round AES-NI CPA attack benchmark across AMD-V, SEV, SEV-ES, SEV-SNP.
- Real-world AES-NI key-byte recovery:
  - OpenSSL AES key-byte recovery from a single SEV-ES VM invocation of AES-NI accelerated CBC

Motivation & Threat Model

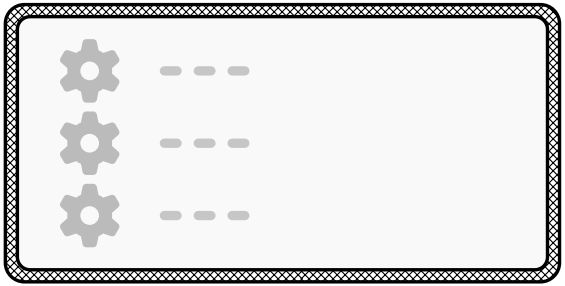
Motivation & Threat Model

Malicious Hypervisor

Confidential VM

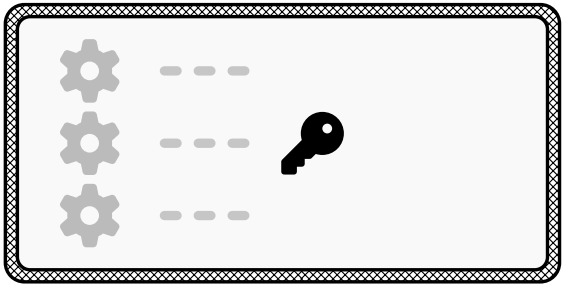
Motivation & Threat Model

Malicious Hypervisor



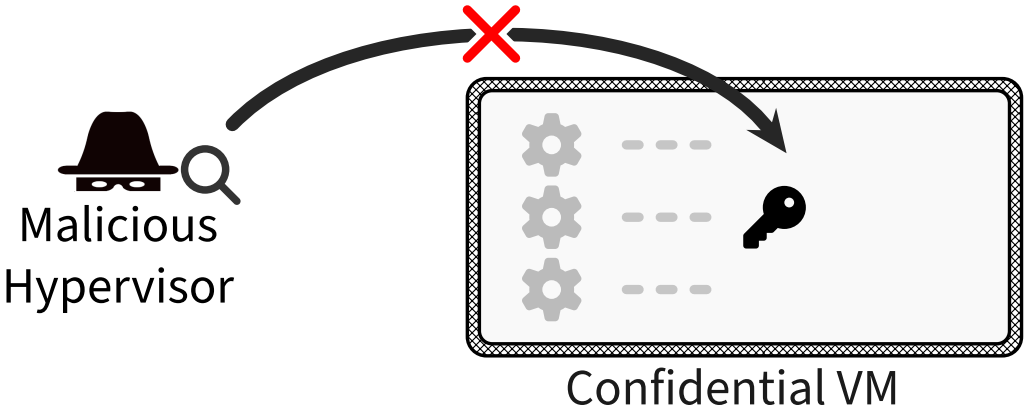
Confidential VM

Malicious Hypervisor

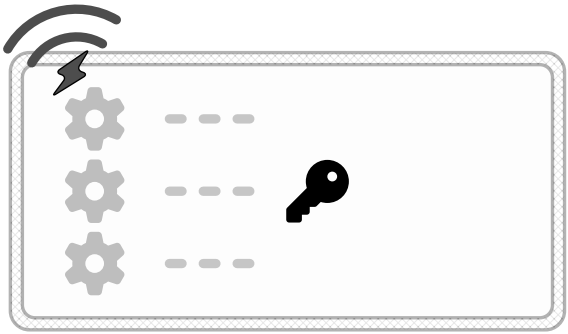


Confidential VM

Motivation & Threat Model

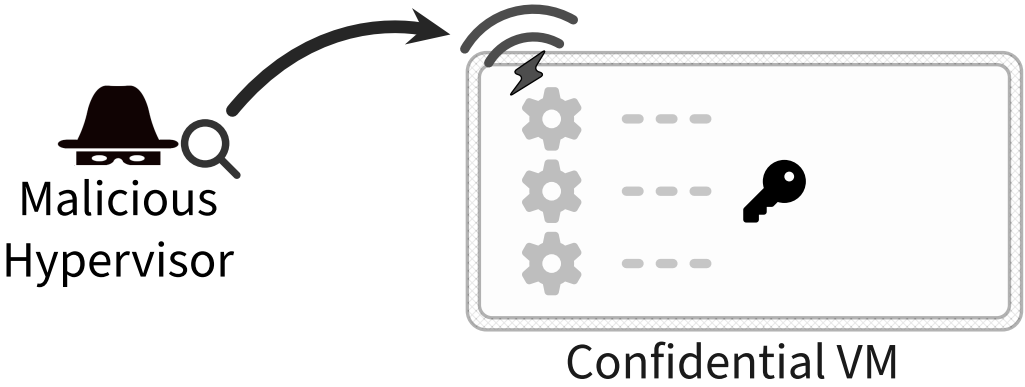


Malicious Hypervisor

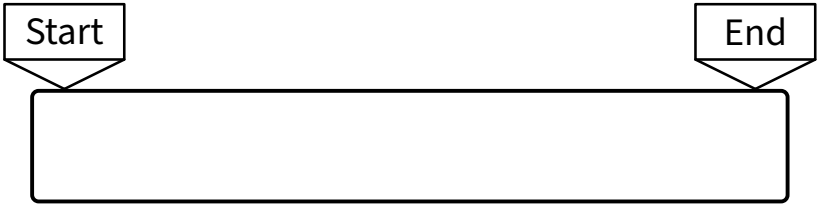


Confidential VM

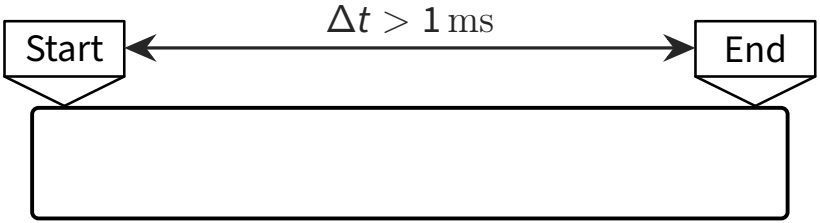
Motivation & Threat Model



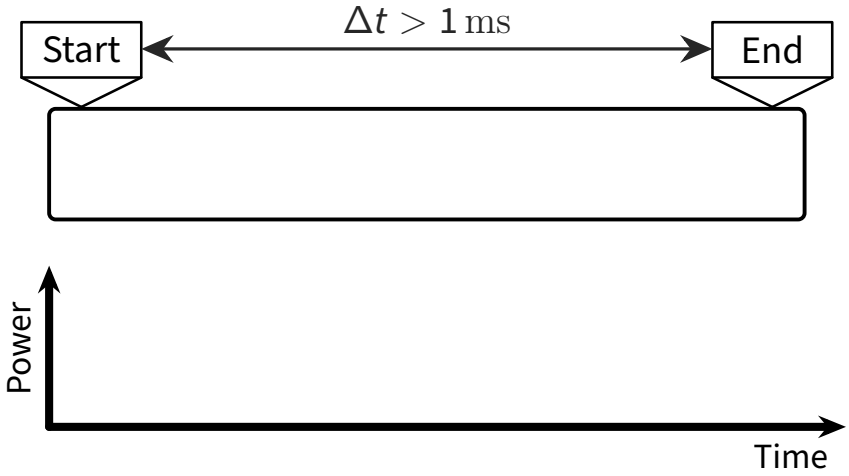
Motivation: Measuring Power in Software



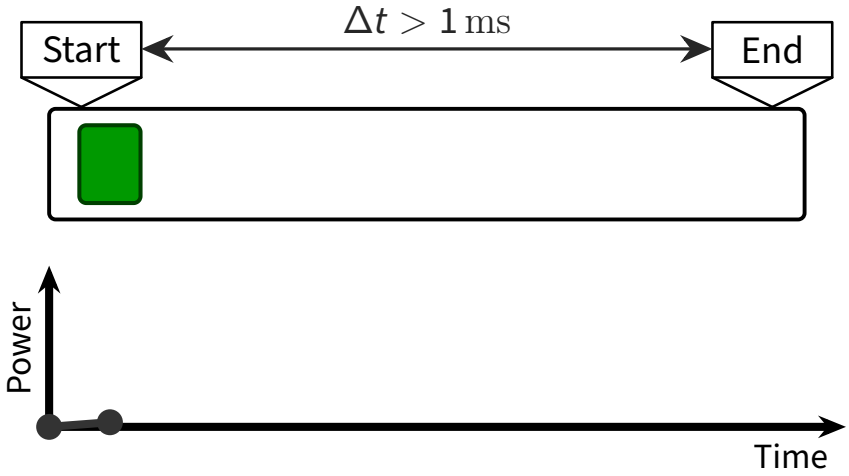
Motivation: Measuring Power in Software



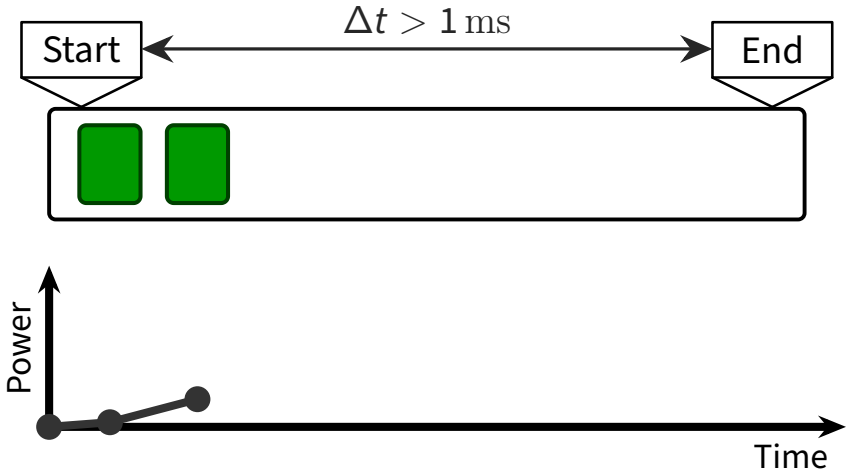
Motivation: Measuring Power in Software



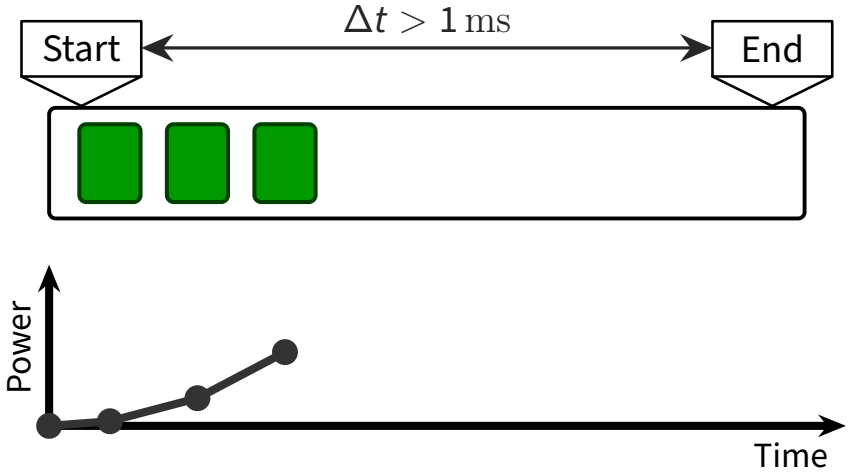
Motivation: Measuring Power in Software



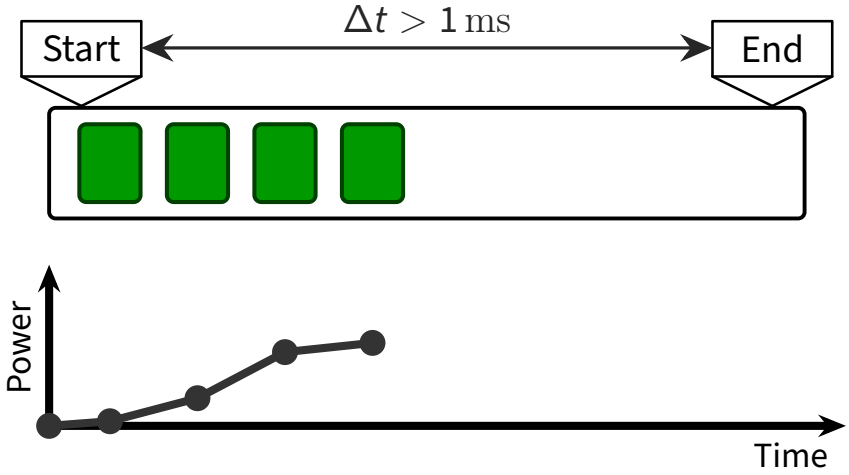
Motivation: Measuring Power in Software



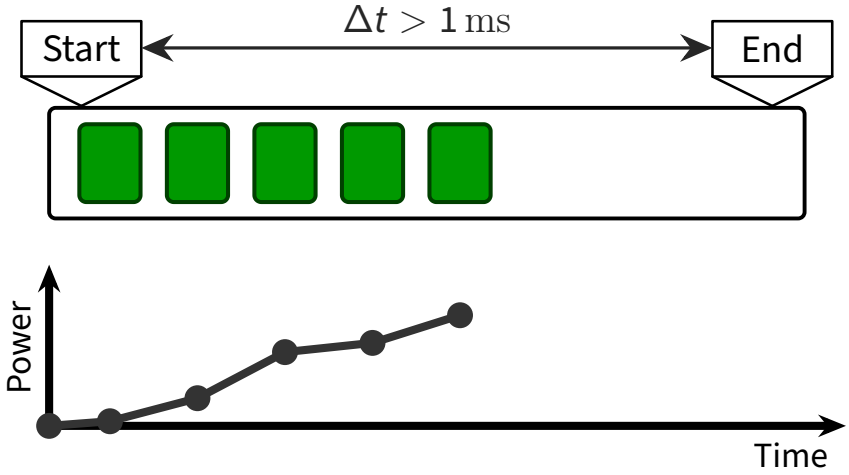
Motivation: Measuring Power in Software



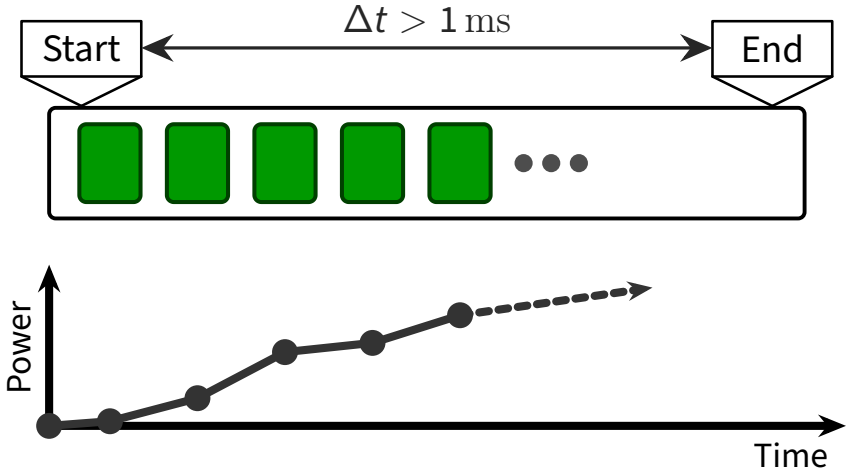
Motivation: Measuring Power in Software



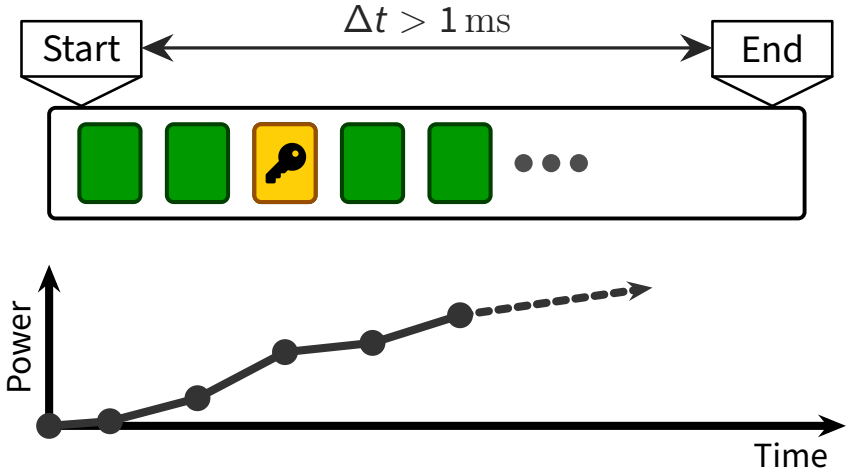
Motivation: Measuring Power in Software



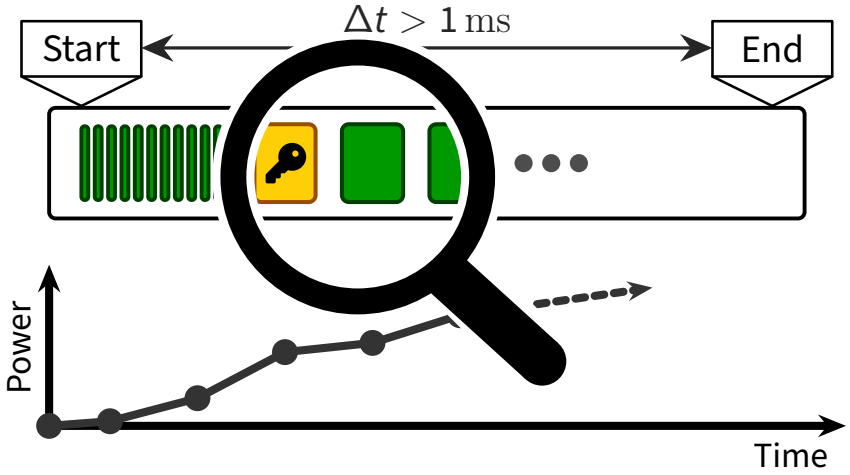
Motivation: Measuring Power in Software



Motivation: Measuring Power in Software

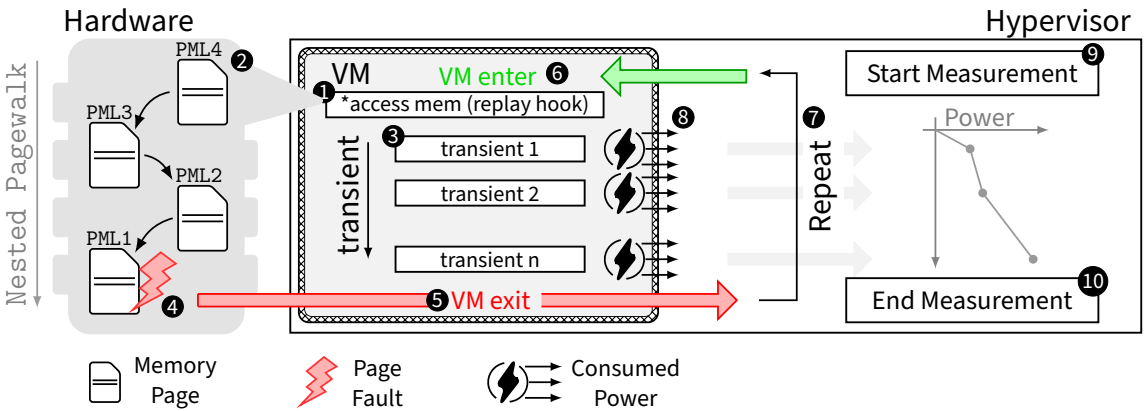


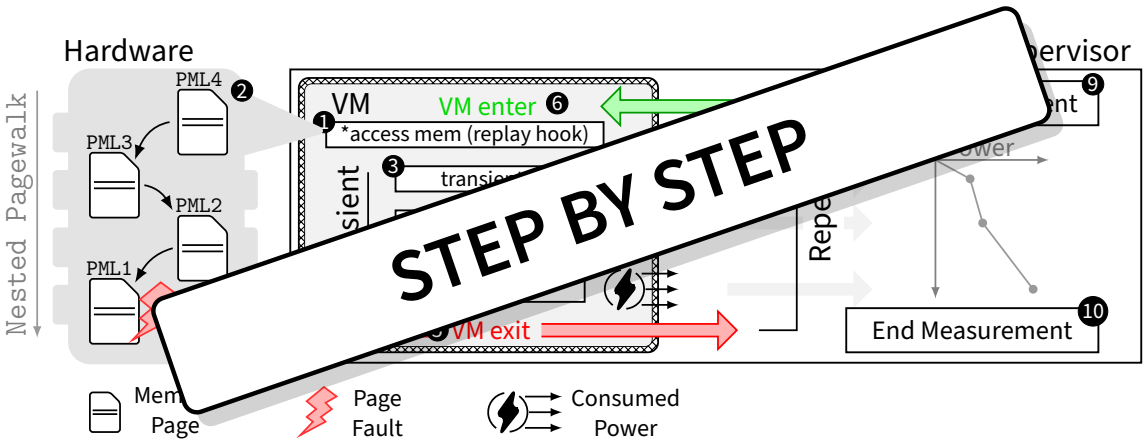
Motivation: Measuring Power in Software



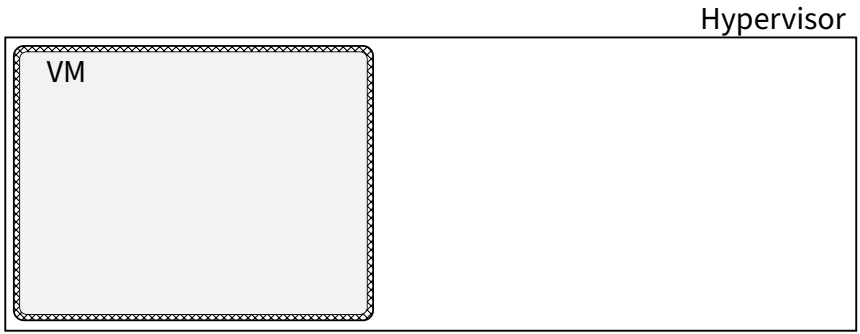
PowerHooK: Overview

PowerHooK Overview

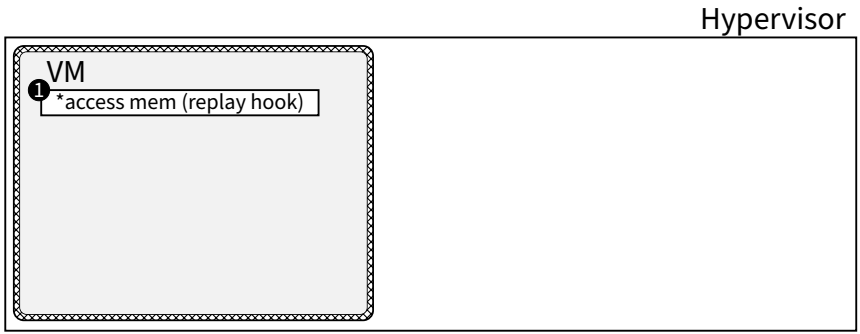



Hardware
Nested Pagewalk
PML4
PML3
PML2
PML1
VM
*access mem (replay hook)
VM enter
VM exit
End Measurement
Page Fault
Consumed Power
STEP BY STEP

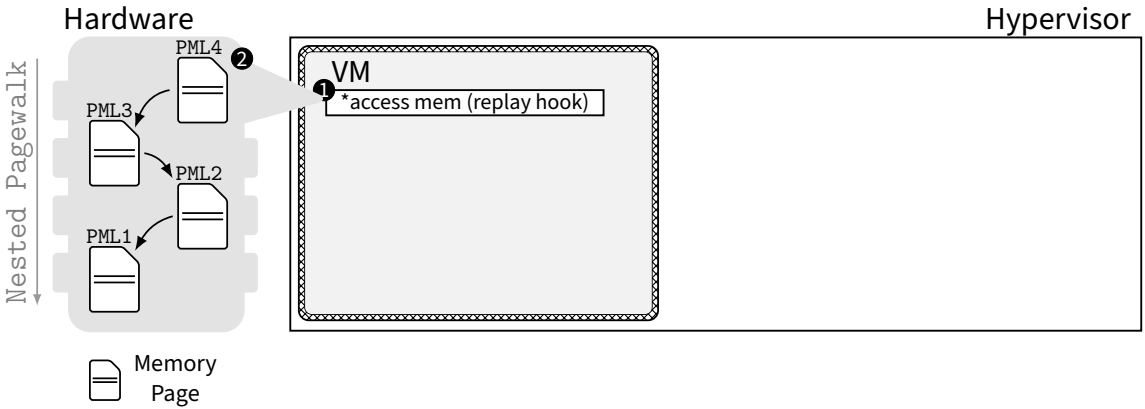
PowerHooK Overview



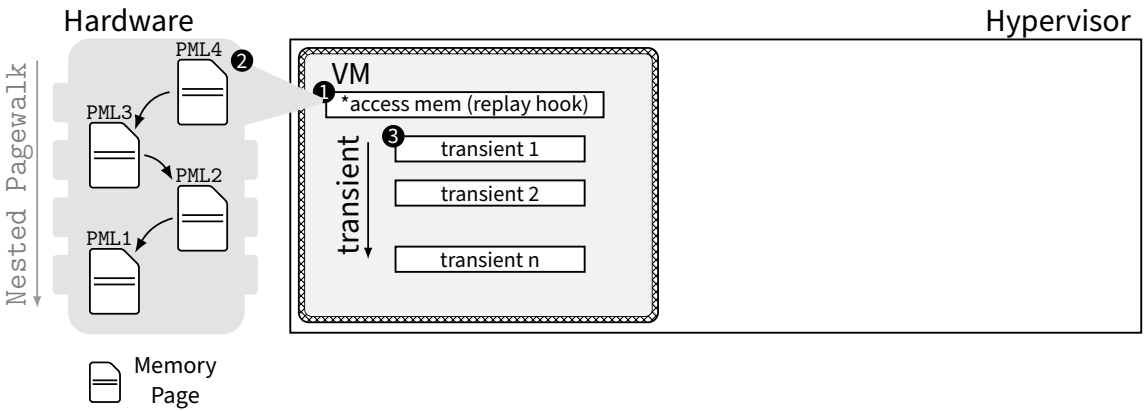
PowerHooK Overview



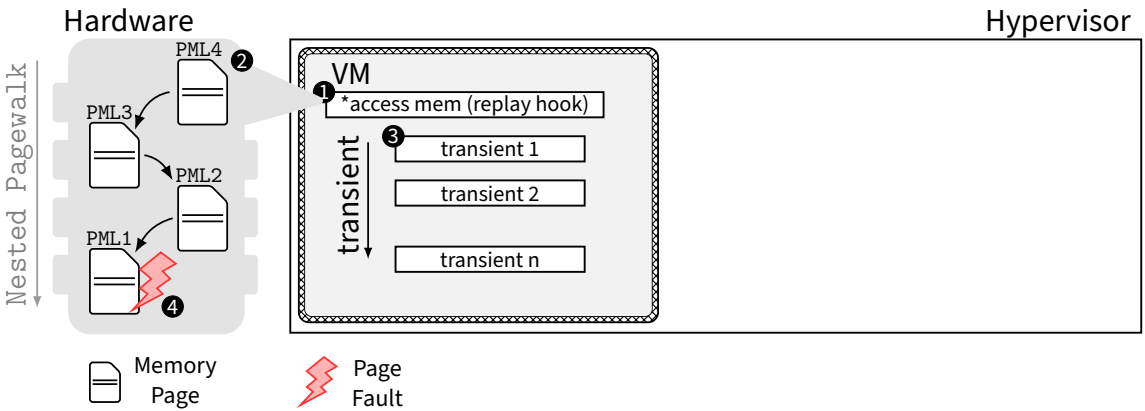
PowerHooK Overview



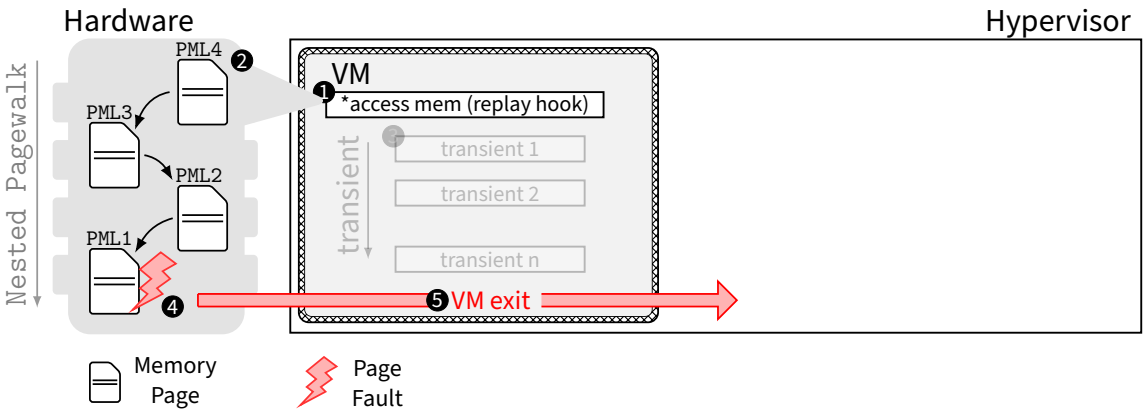
PowerHooK Overview



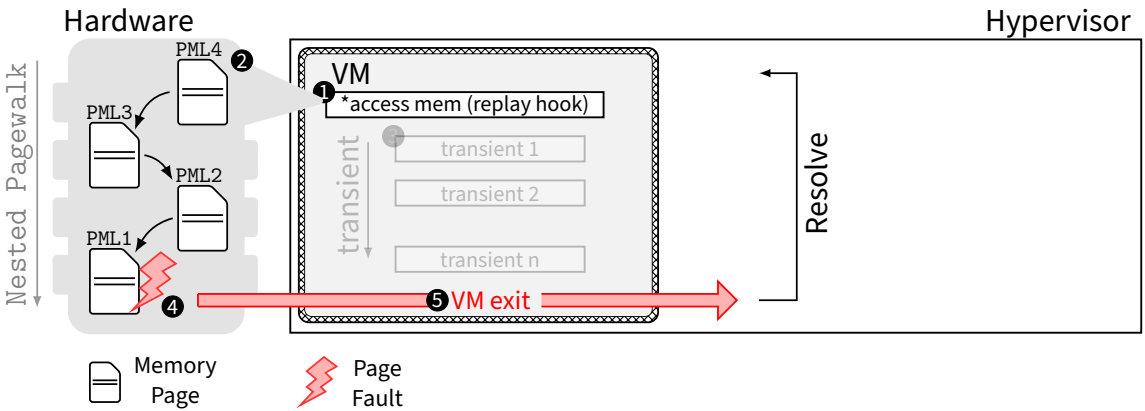
PowerHooK Overview



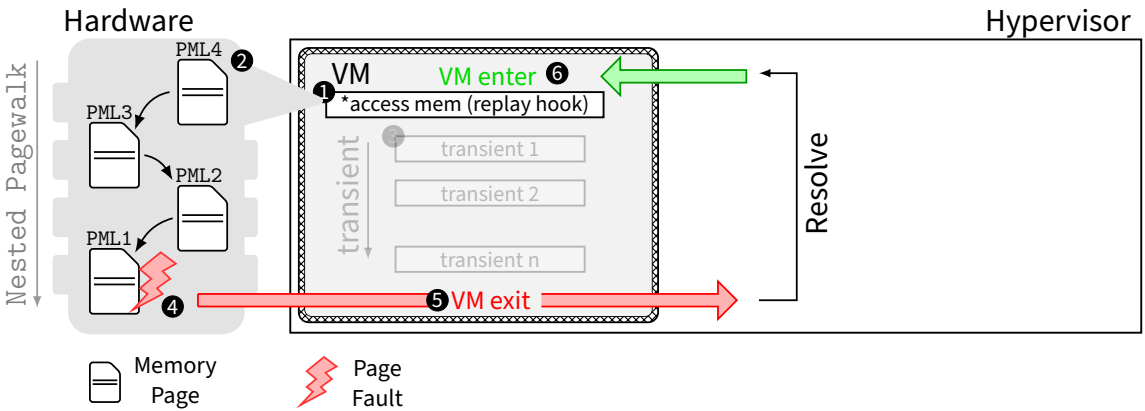
PowerHooK Overview



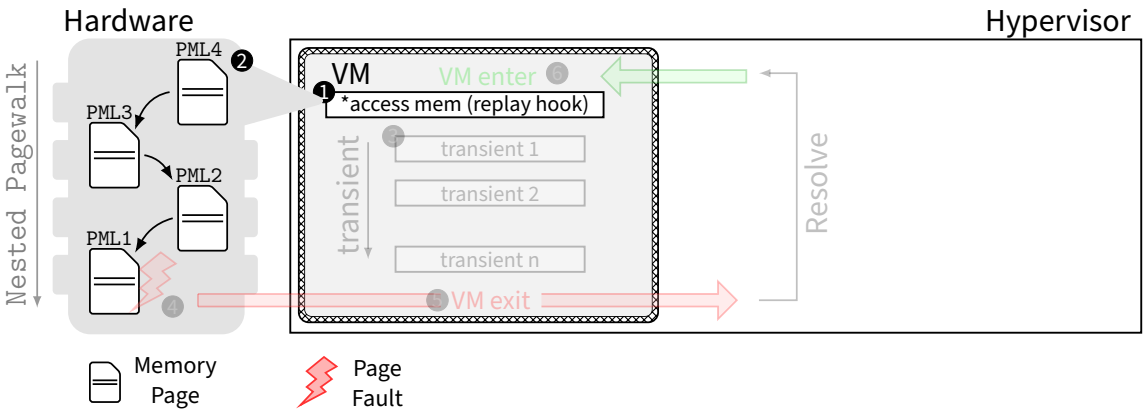
PowerHooK Overview



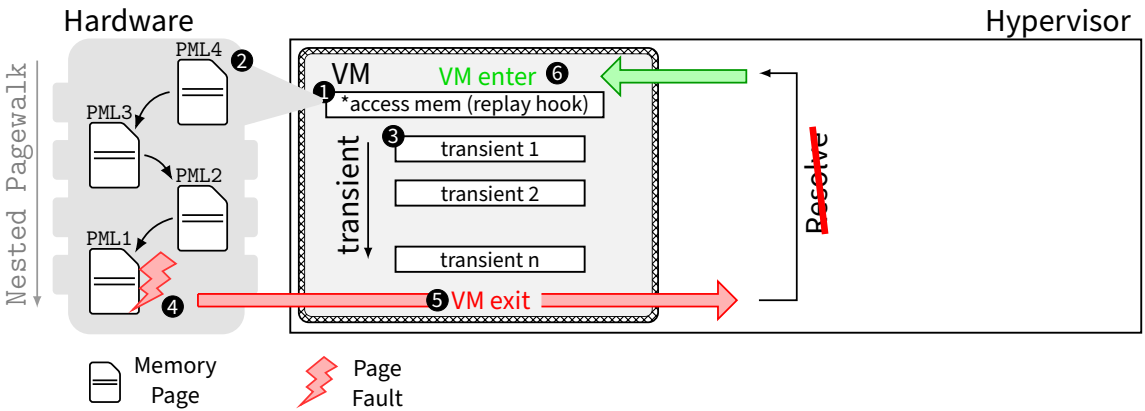
PowerHooK Overview



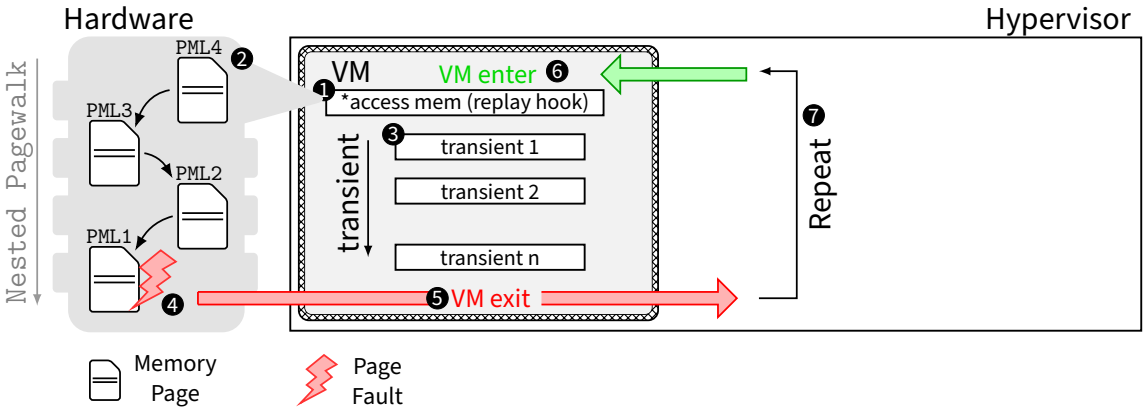
PowerHooK Overview



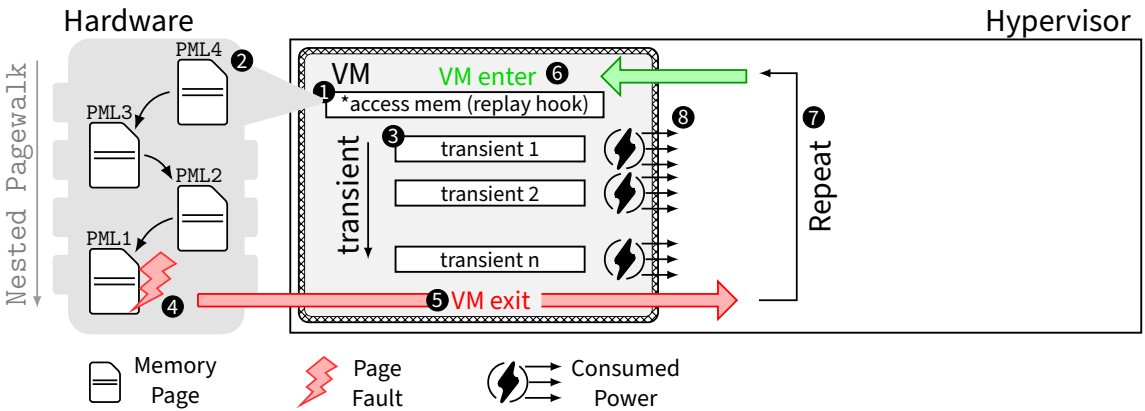
PowerHooK Overview



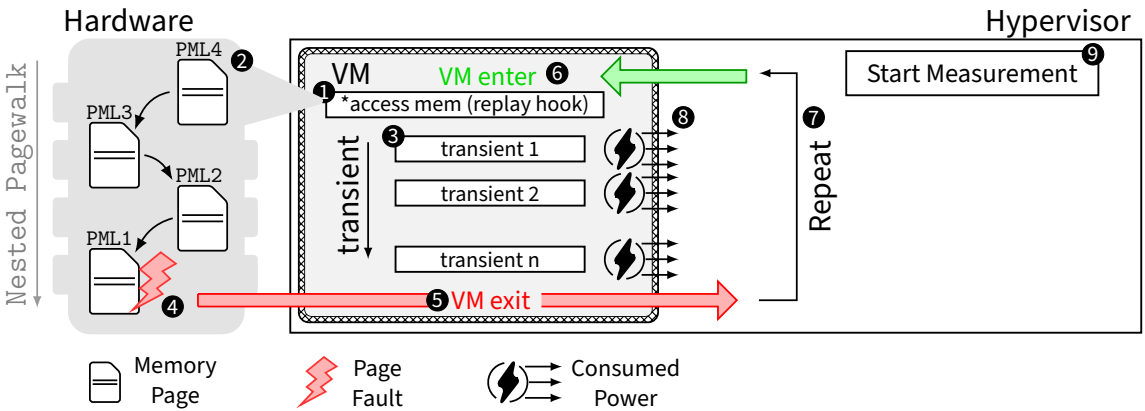
PowerHooK Overview



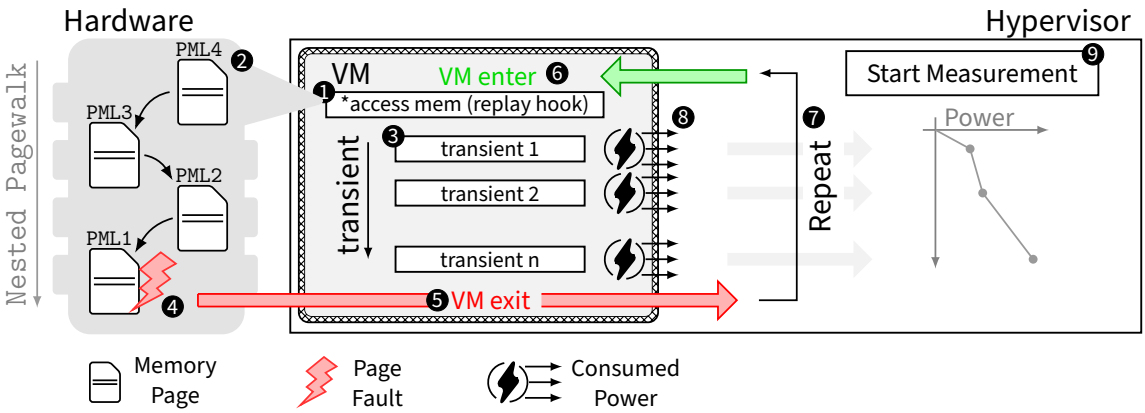
PowerHooK Overview



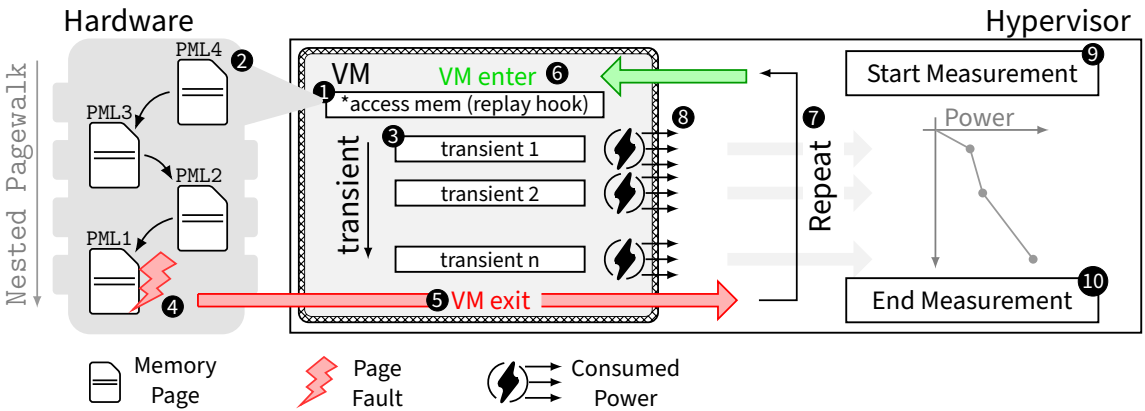
PowerHooK Overview



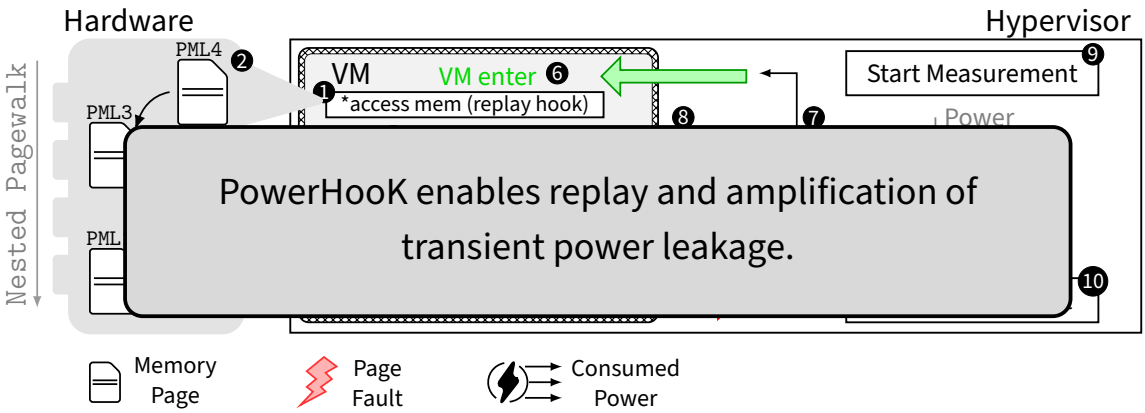
PowerHooK Overview



PowerHooK Overview

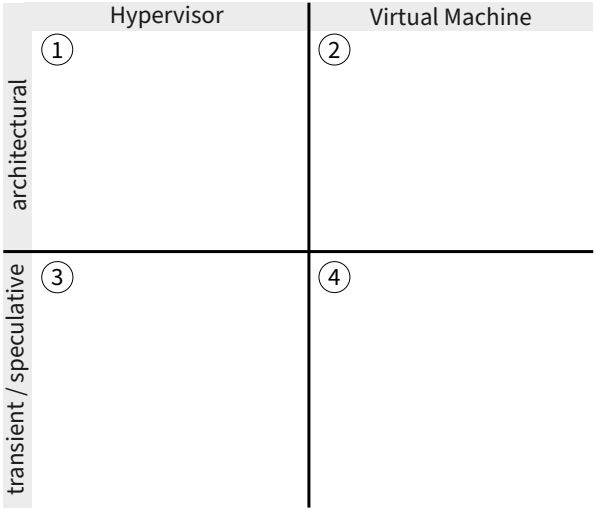


PowerHooK Overview

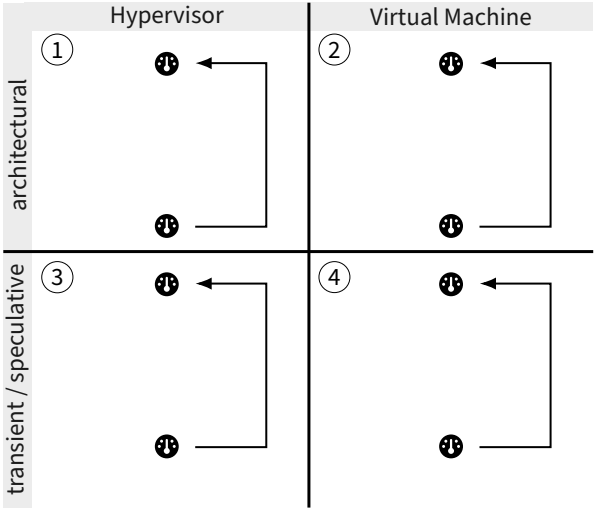


Systematic Analysis

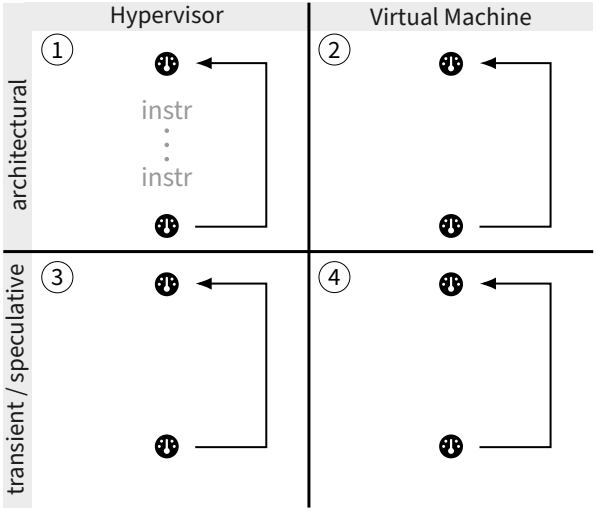
Systematic Analysis



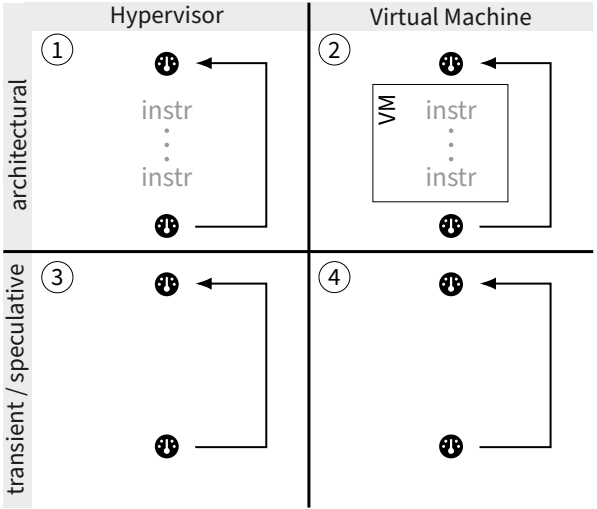
Systematic Analysis



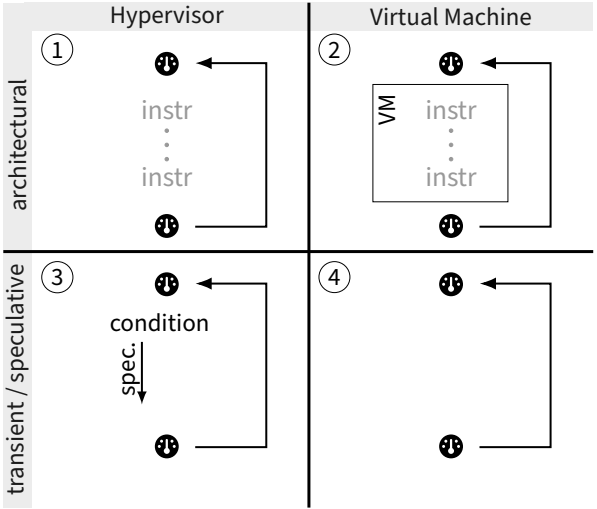
Systematic Analysis



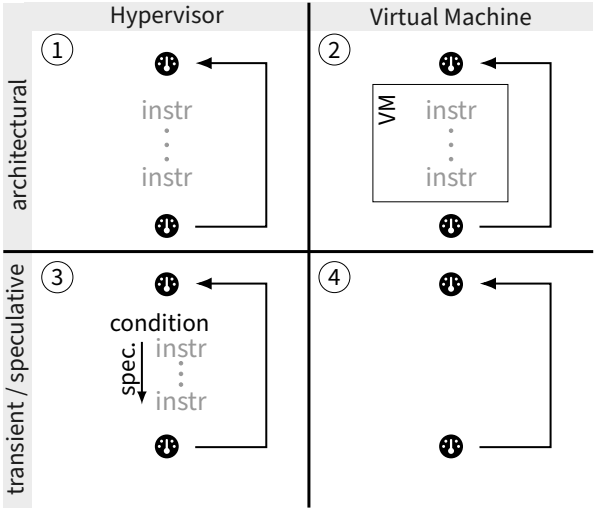
Systematic Analysis



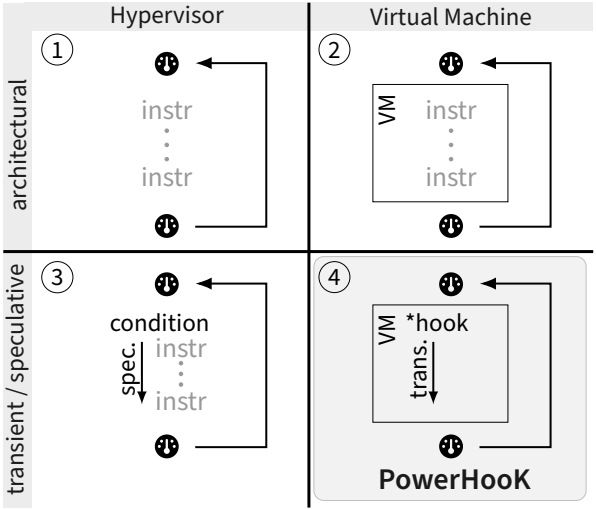
Systematic Analysis



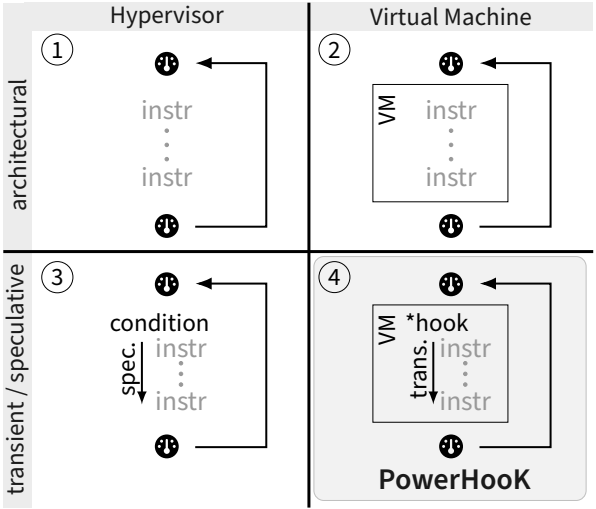
Systematic Analysis



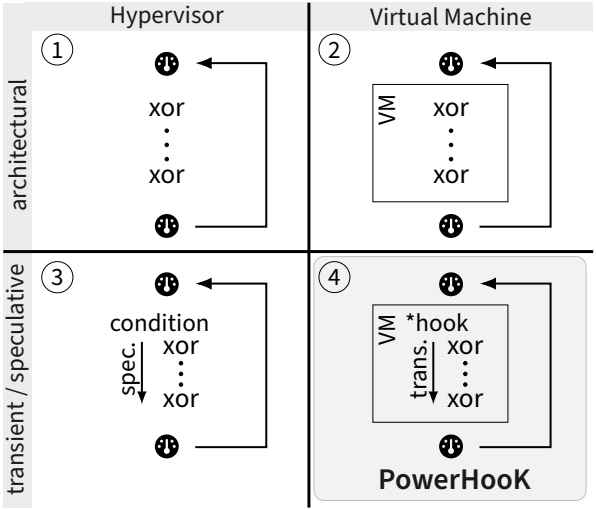
Systematic Analysis



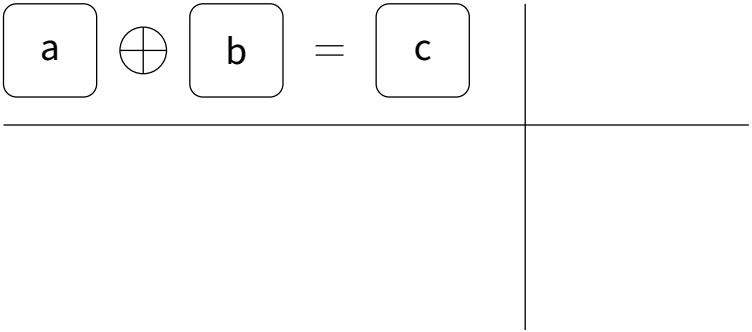
Systematic Analysis



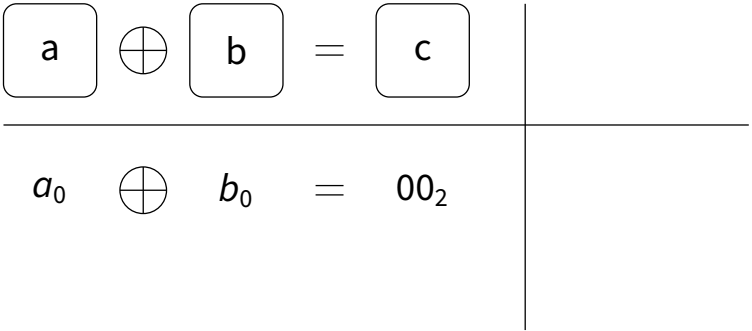
Systematic Analysis



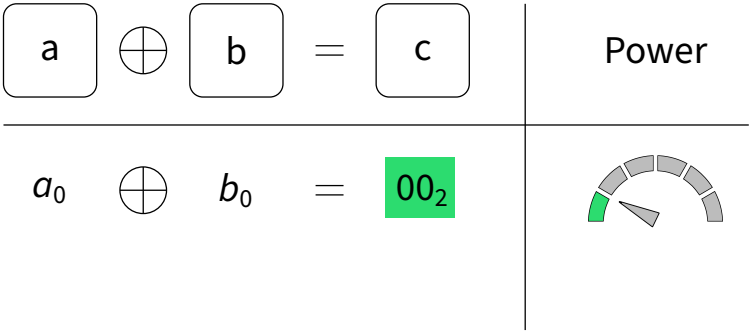
Systematic Analysis: Executed Workload



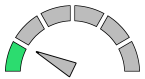
Systematic Analysis: Executed Workload



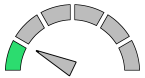
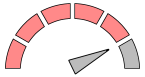
Systematic Analysis: Executed Workload



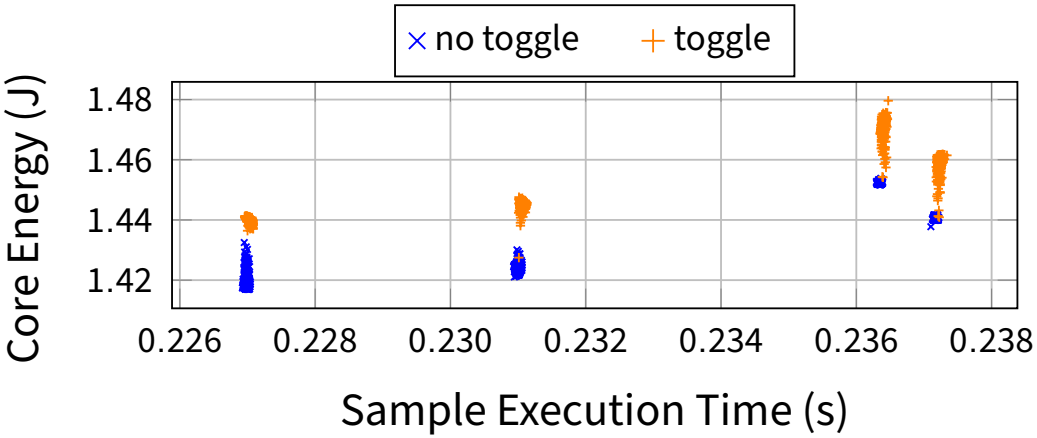
Systematic Analysis: Executed Workload

a ⊕ b = c	Power
$a_0 \oplus b_0 = 00_2$	
$a_1 \oplus b_1 = 11_2$	

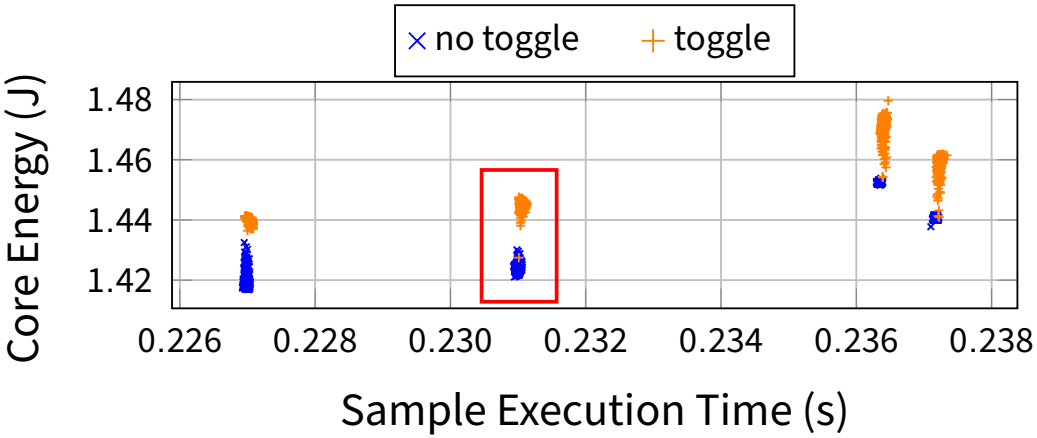
Systematic Analysis: Executed Workload

a	⊕	b	=	c	Power
a_0	⊕	b_0	=	00_2	
a_1	⊕	b_1	=	11_2	

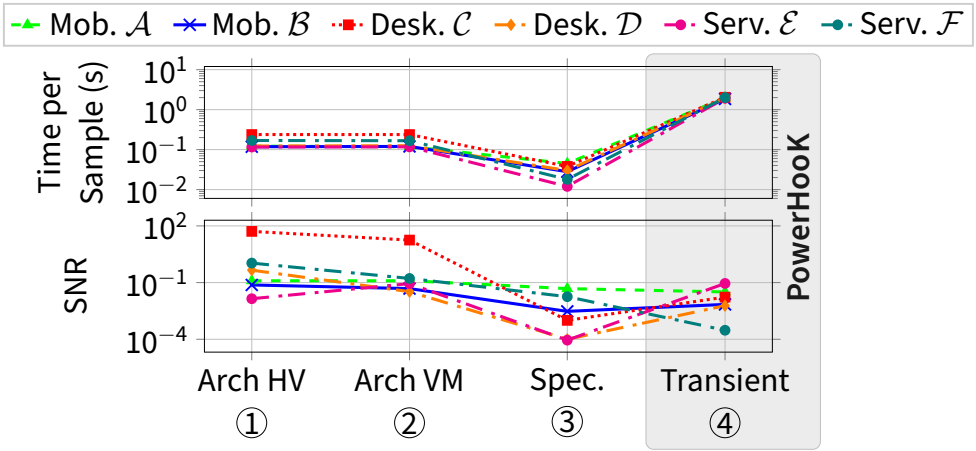
Systematic Analysis: Generic Filtering



Systematic Analysis: Generic Filtering

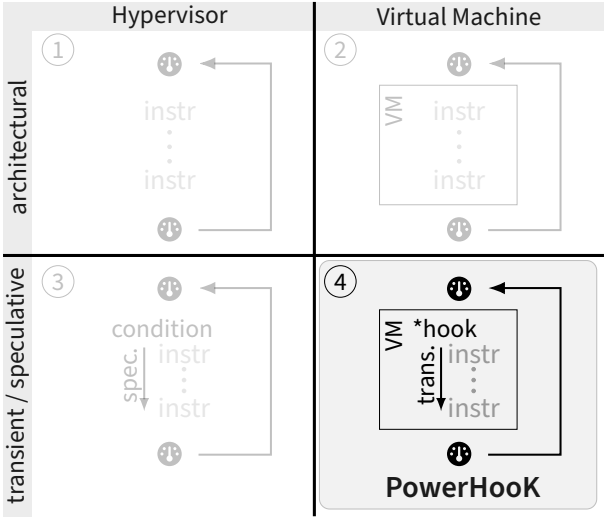


Systematic Analysis: Evaluation

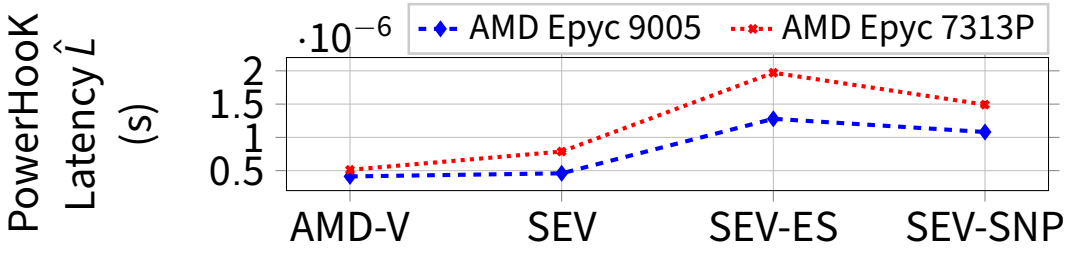


PowerHooK Execution Time Across SEV Technologies

PowerHooK Execution Time Across SEV Technologies



PowerHooK: Replay Execution Time



Synthetic AES-NI CPA Attack across AMD SEV

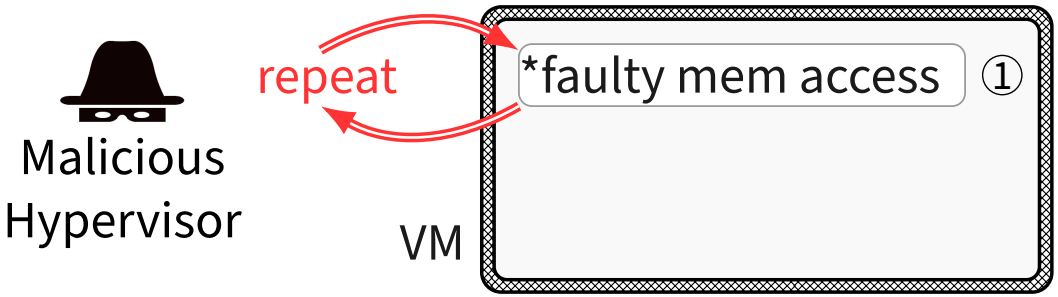
Malicious Hypervisor

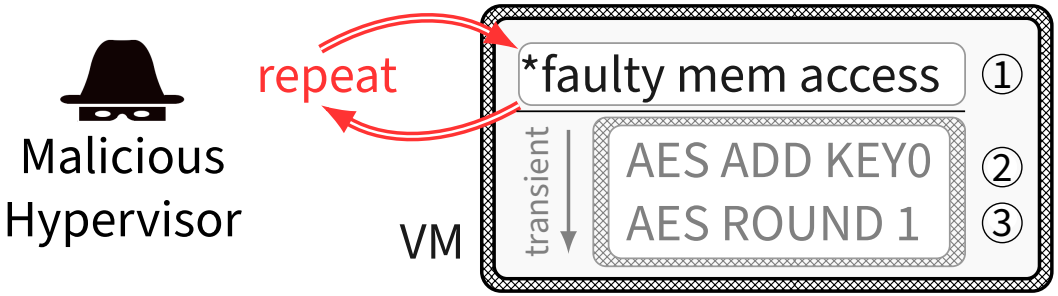
VM

Malicious Hypervisor

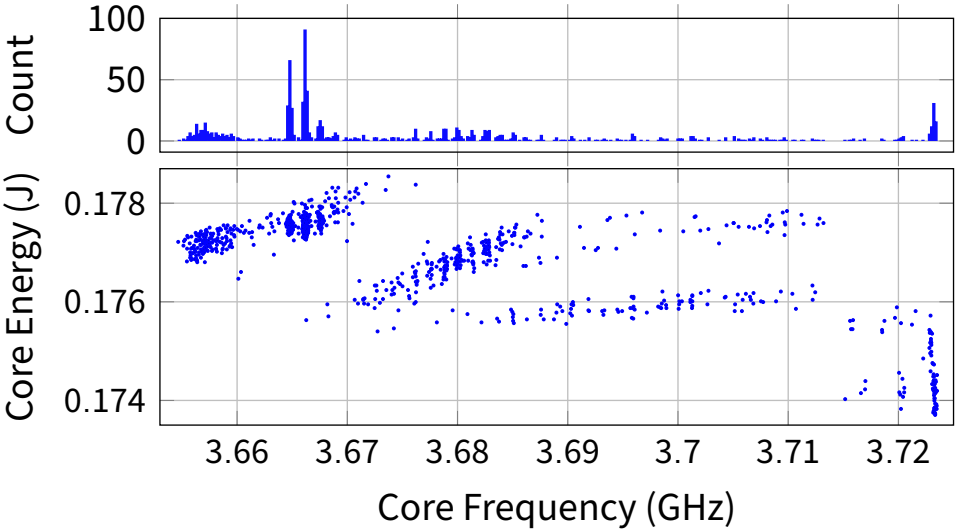
VM

*faulty mem access ①

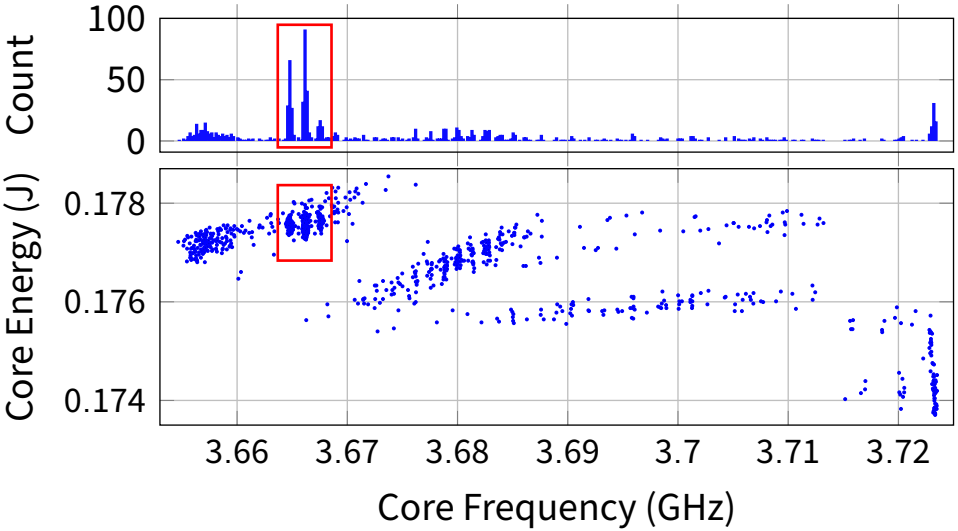

repeat
*faulty mem access
①
Malicious
Hypervisor
VM


repeat
*faulty mem access
①
transient
AES ADD KEY0
②
AES ROUND 1
③
VM
Malicious
Hypervisor

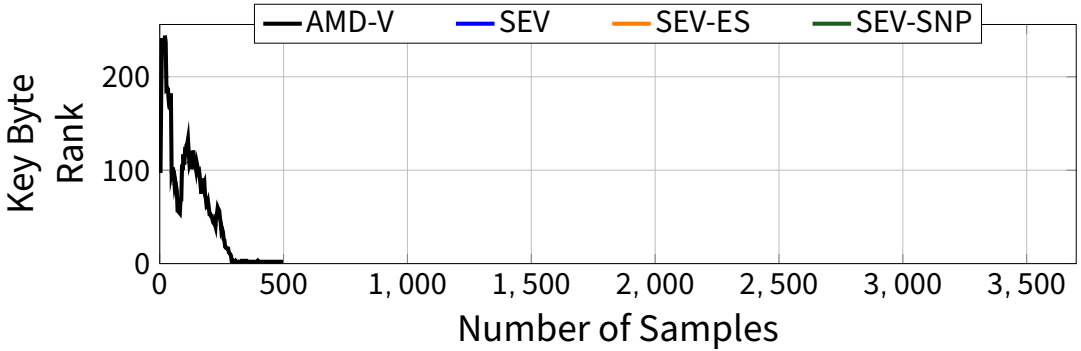
AES-NI Leakage Characterization: Filtering



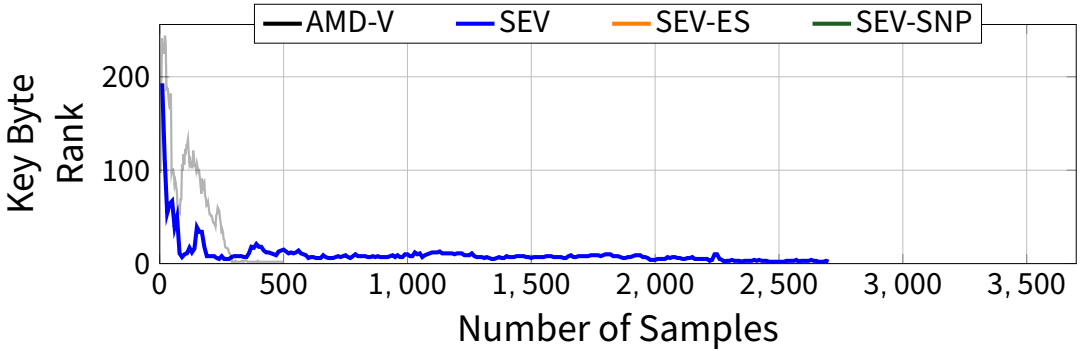
AES-NI Leakage Characterization: Filtering



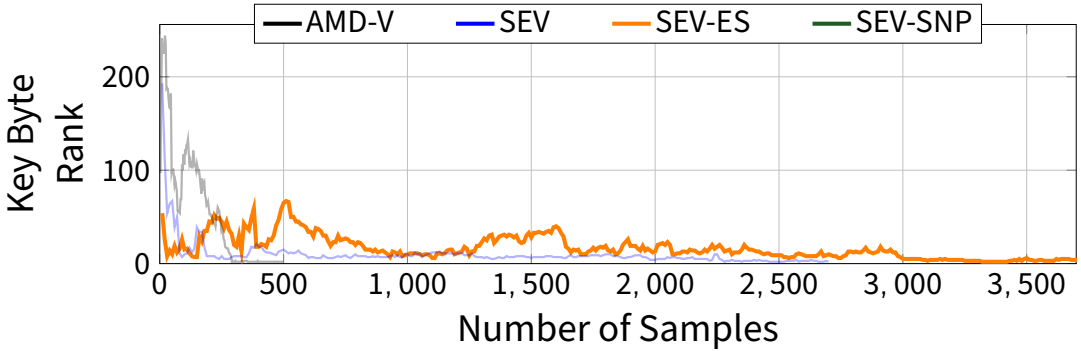
AES-NI Leakage Characterization: Evaluation



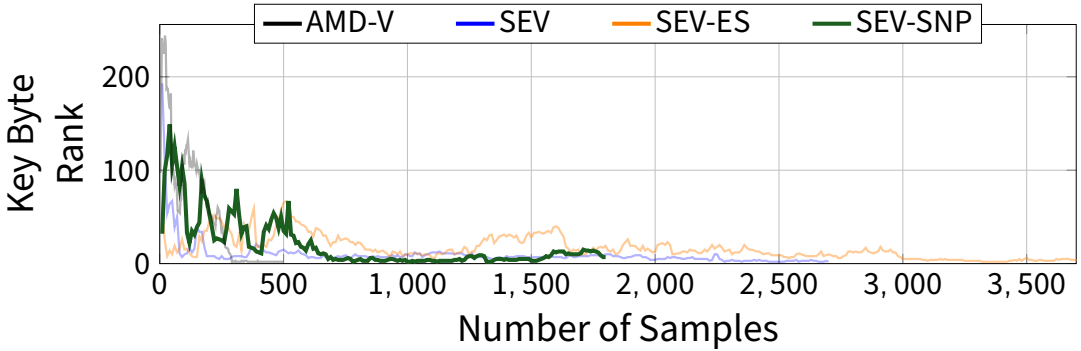
AES-NI Leakage Characterization: Evaluation



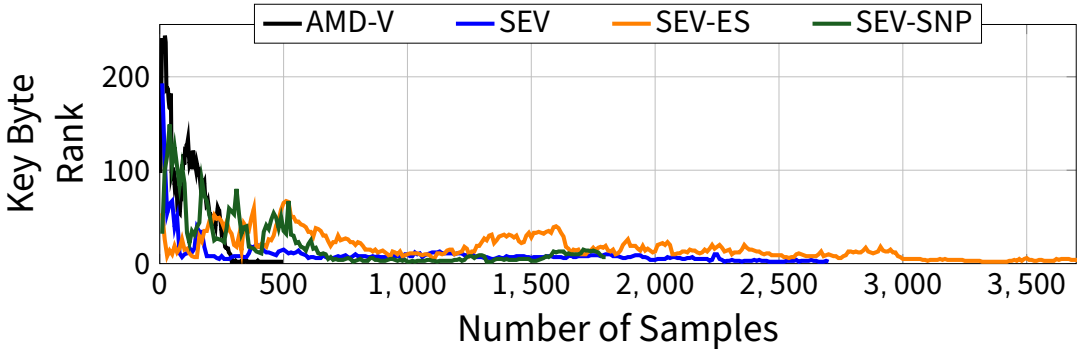
AES-NI Leakage Characterization: Evaluation



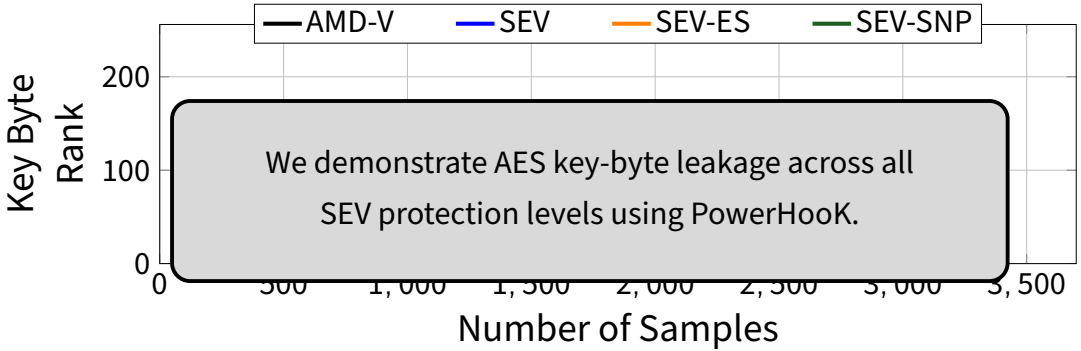
AES-NI Leakage Characterization: Evaluation



AES-NI Leakage Characterization: Evaluation

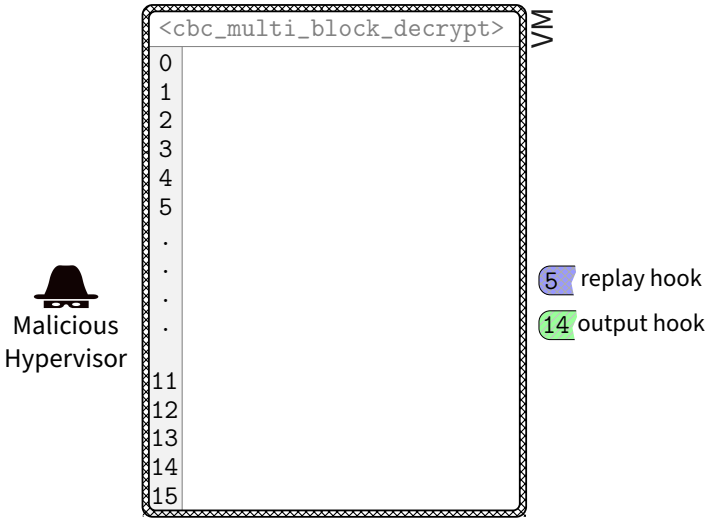


AES-NI Leakage Characterization: Evaluation

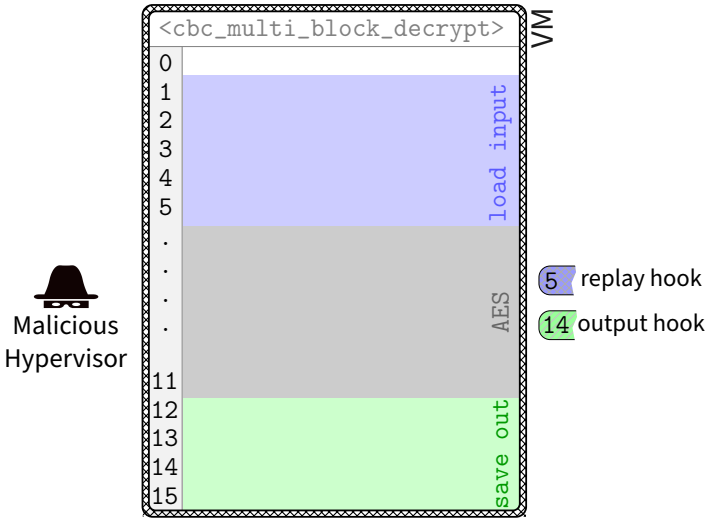


Real-World Attack Case Study: AES-CBC Multi-Block Decryption

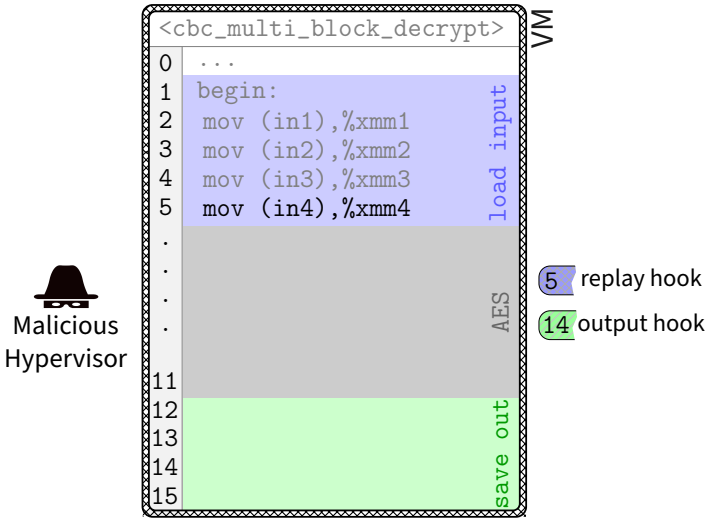
Real-World Attack Case Study



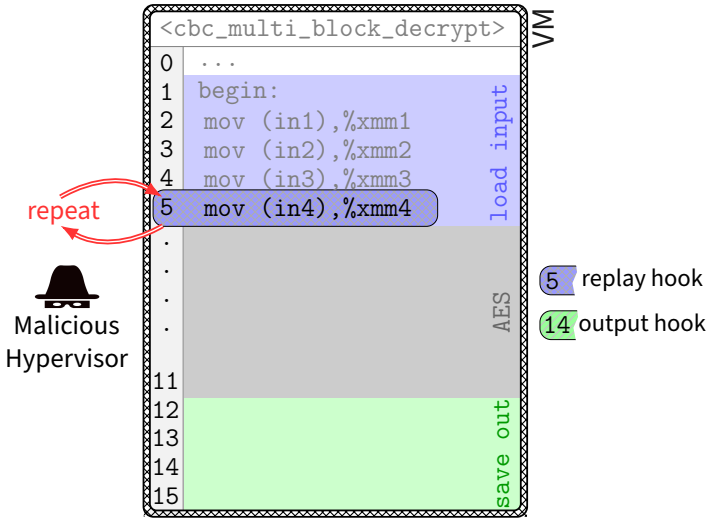
Real-World Attack Case Study



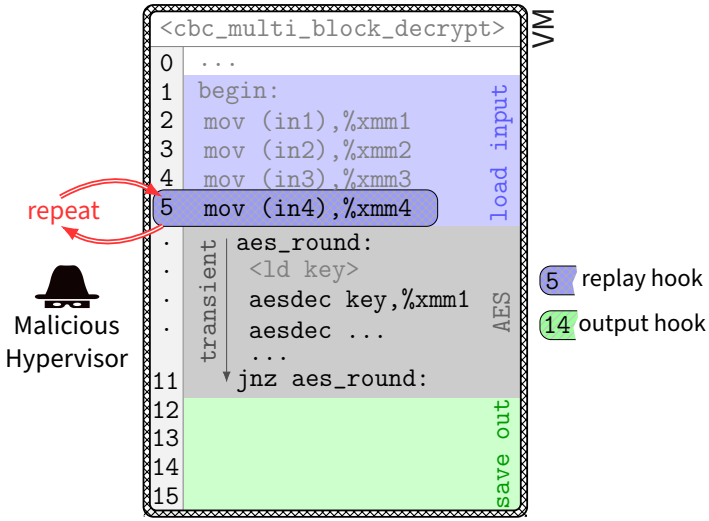
Real-World Attack Case Study



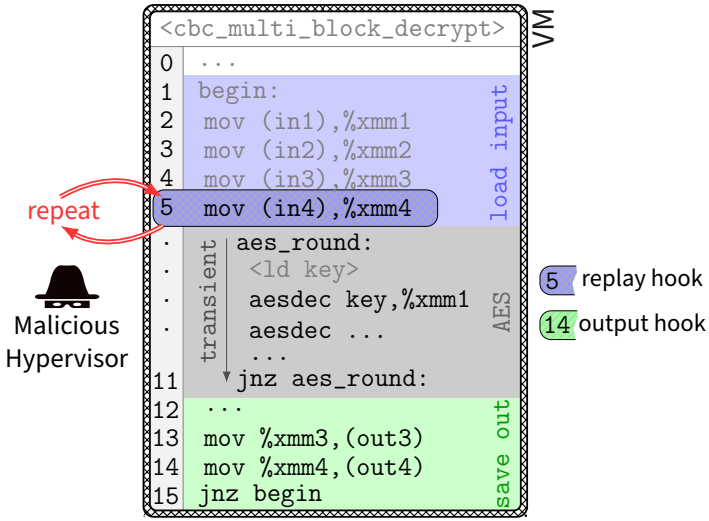
Real-World Attack Case Study



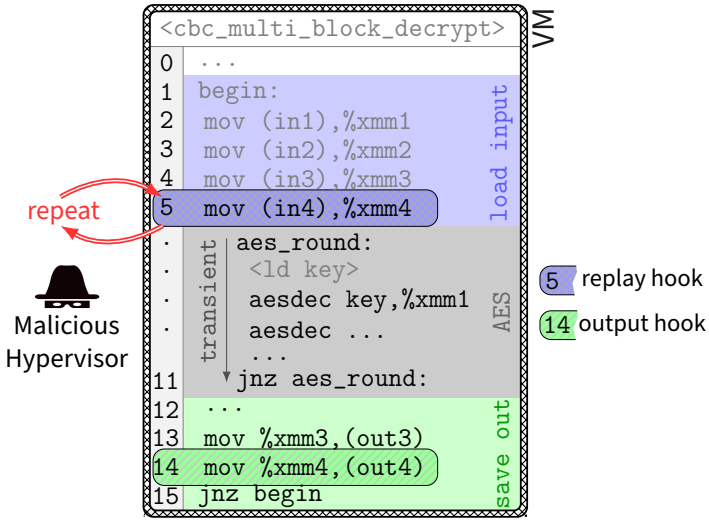
Real-World Attack Case Study



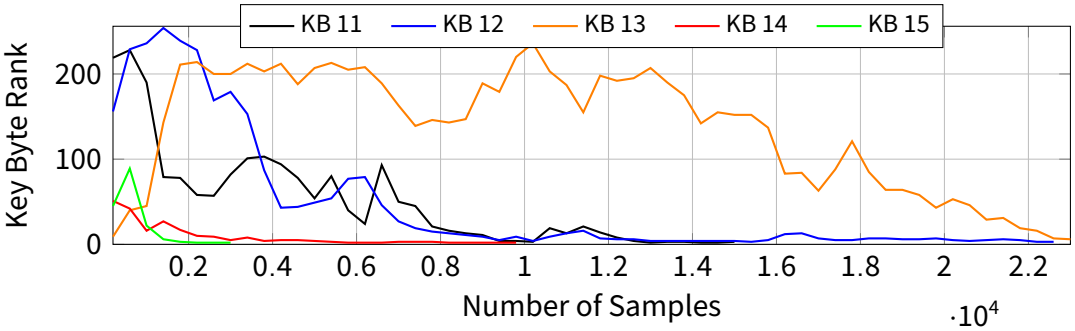
Real-World Attack Case Study



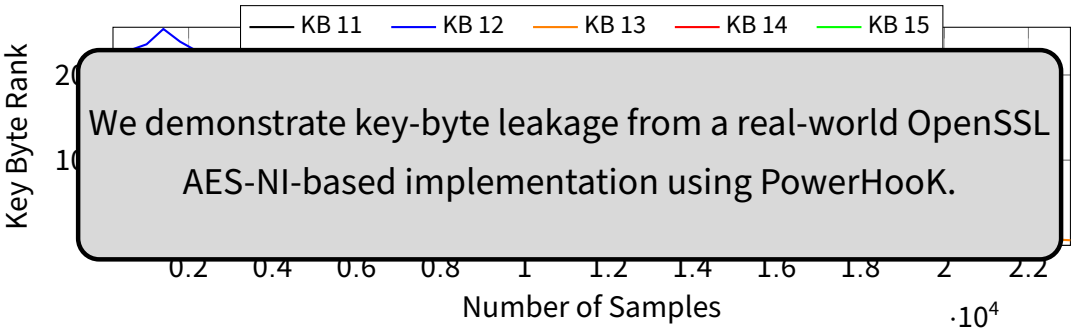
Real-World Attack Case Study



Real-World Attack Case Study: Evaluation



Real-World Attack Case Study: Evaluation



We demonstrate key-byte leakage from a real-world OpenSSL AES-NI-based implementation using PowerHooK.

Conclusion

Transient-replay power side channels against **AMD SEV VMs**

Conclusion

Transient-replay power side channels against **AMD SEV VMs**

- Denoising software-based power side channels:
  - Malicious hypervisor uses a transient-replay gadget to amplify and denoise transient power traces
  - Enables single-run power side-channel attacks against VMs protected by AMD SEV technologies

Conclusion

Transient-replay power side channels against **AMD SEV VMs**

- Denoising software-based power side channels:
  - Malicious hypervisor uses a transient-replay gadget to amplify and denoise transient power traces
  - Enables single-run power side-channel attacks against VMs protected by AMD SEV technologies
- Systematic leakage analysis:
  - Comparing architectural, speculative, and transient power leakage across VM boundaries

Conclusion

Transient-replay power side channels against **AMD SEV VMs**

- Denoising software-based power side channels:
  - Malicious hypervisor uses a transient-replay gadget to amplify and denoise transient power traces
  - Enables single-run power side-channel attacks against VMs protected by AMD SEV technologies
- Systematic leakage analysis:
  - Comparing architectural, speculative, and transient power leakage across VM boundaries
- Leakage Characterization:
  - Synthetic first-round AES-NI CPA attack benchmark across AMD-V, SEV, SEV-ES, SEV-SNP.

Conclusion

Transient-replay power side channels against **AMD SEV VMs**

- Denoising software-based power side channels:
  - Malicious hypervisor uses a transient-replay gadget to amplify and denoise transient power traces
  - Enables single-run power side-channel attacks against VMs protected by AMD SEV technologies
- Systematic leakage analysis:
  - Comparing architectural, speculative, and transient power leakage across VM boundaries
- Leakage Characterization:
  - Synthetic first-round AES-NI CPA attack benchmark across AMD-V, SEV, SEV-ES, SEV-SNP.
- Real-world AES-NI key-byte recovery:
  - OpenSSL AES key-byte recovery from a single SEV-ES VM invocation of AES-NI accelerated CBC

PowerHooK:
Enabling Software-Based Power Side Channels Against AMD SEV Technologies via Transient-Execution Replay

SCIENCE
PASSION
TECHNOLOGY

Mathias Oberhuber[1] Martin Unterguggenberger[1] Martin Wistauder[1]
Andreas Kogler[2] Rishub Nagpal[1] Stefan Mangard[1]

[1]Graz University of Technology [2]Graz University of Technology Alumni

› isec.tugraz.at