TU Graz
SCIENCE
PASSION
TECHNOLOGY

TEEcorrelate

An Information-Preserving Defense against Performance-Counter Attacks on TEEs

Hannes Weissteiner Fabian Rauscher Robin Leander Schröder Jonas Juffinger
Stefan Gast Jan Wichelmann Thomas Eisenbarth Daniel Gruss

Graz University of Technology

USENIX 2025

› isec.tugraz.at

Prior Work

Prior Work

Prior Work

Stefan Gast et al. **CounterSEVeillance: Performance-Counter Attacks on AMD SEV-SNP.** NDSS. 2025

- AMD SEV-SNP: Confidential VM implementation by AMD

Prior Work

Stefan Gast et al. **CounterSEVeillance: Performance-Counter Attacks on AMD SEV-SNP.** NDSS. 2025

- AMD SEV-SNP: Confidential VM implementation by AMD
- Performance counters were enabled during CVM execution

Prior Work

Stefan Gast et al. **CounterSEVeillance: Performance-Counter Attacks on AMD SEV-SNP.** NDSS. 2025

- AMD SEV-SNP: Confidential VM implementation by AMD
- Performance counters were enabled during CVM execution

→ Fine-grained data leakage through various performance counters

Prior Work

Stefan Gast et al. **CounterSEVeillance: Performance-Counter Attacks on AMD SEV-SNP.** NDSS. 2025

- AMD SEV-SNP: Confidential VM implementation by AMD
- Performance counters were enabled during CVM execution

→ Fine-grained data leakage through various performance counters
  - **Retired Branches** + **Retired Taken Branches** → break RSA, TOTP

Prior Work

Stefan Gast et al. **CounterSEVeillance: Performance-Counter Attacks on AMD SEV-SNP.** NDSS. 2025

- AMD SEV-SNP: Confidential VM implementation by AMD
- Performance counters were enabled during CVM execution

→ Fine-grained data leakage through various performance counters

- **Retired Branches** + **Retired Taken Branches** → break RSA, TOTP
- **Div Cycles Busy** → breaks HQC (PQ-KEM)

Prior Work

Stefan Gast et al. **CounterSEVeillance: Performance-Counter Attacks on AMD SEV-SNP.** NDSS. 2025

- AMD SEV-SNP: Confidential VM implementation by AMD
- Performance counters were enabled during CVM execution

→ Fine-grained data leakage through various performance counters

- **Retired Branches** + **Retired Taken Branches** → break RSA, TOTP
- **Div Cycles Busy** → breaks HQC (PQ-KEM)

- Mitigation by AMD: **Disable performance counters**

Defense: TEEcorrelate

- Defends against fine-grained PC leakage

Defense: TEEcorrelate

- Defends against fine-grained PC leakage
- **Decorrelates** real and reported performance counter values

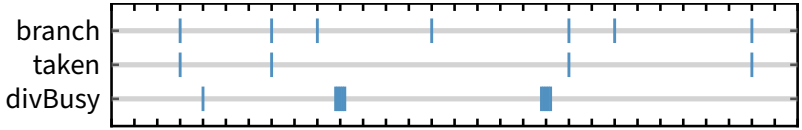
Defense: TEEcorrelate

- Defends against fine-grained PC leakage
- **Decorrelates** real and reported performance counter values
- Keeps coarse-grained trends intact

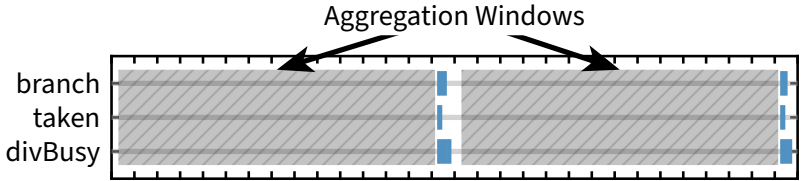
Defense: TEEcorrelate

- Defends against fine-grained PC leakage
- **Decorrelates** real and reported performance counter values
- Keeps coarse-grained trends intact
- 2 main components:

Temporal Decorrelation

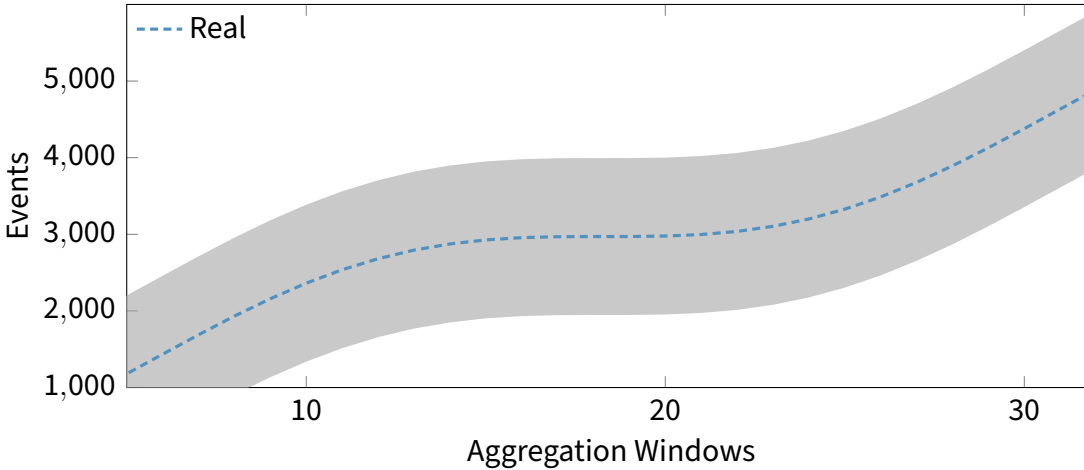


(a) Native Events

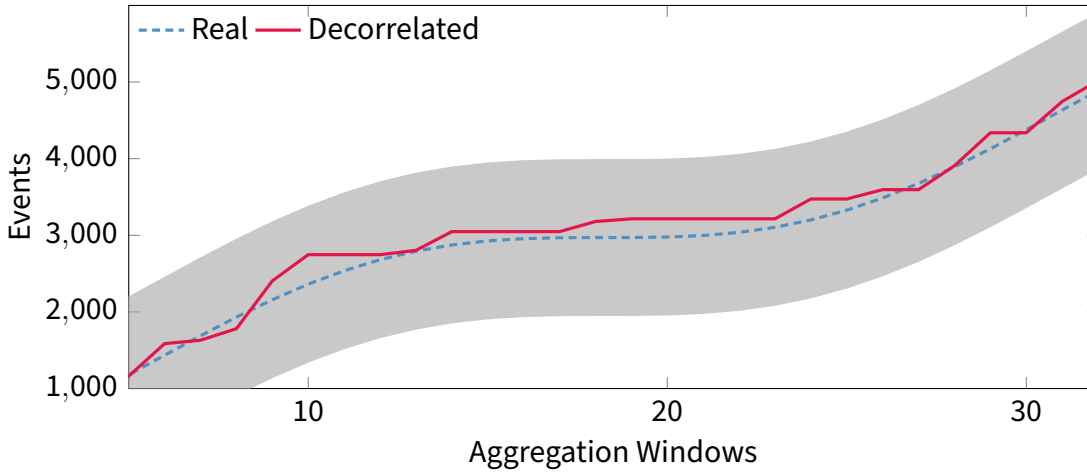


(b) Temporal decorrelated events

Value Decorrelation



Value Decorrelation



Results

- Assuming an **unrealistically strong adversary**

Results

- Assuming an **unrealistically strong adversary**
- $\approx$ 150.000 traces to leak 1 bit

Results

- Assuming an **unrealistically strong adversary**
- $\approx$ 150.000 traces to leak 1 bit
  - TOTP brute-force: 18.14s $\rightarrow$ 34.7 days
  - TOTP secret recovery: 0.58s $\rightarrow$ 285.4 days
  - RSA key recovery: 7.15m $\rightarrow$ 824.6 days

Results

- Assuming an **unrealistically strong adversary**
- $\approx$ 150.000 traces to leak 1 bit
  - TOTP brute-force: $18.14s \rightarrow$ 34.7 days
  - TOTP secret recovery: $0.58s \rightarrow$ 285.4 days
  - RSA key recovery: $7.15m \rightarrow$ 824.6 days
- Estimated runtime overhead: $\approx 0.09\%$

Conclusion

- TEEcorrelate $\rightarrow$ Lightweight defense against fine-grained PC leakage

Conclusion

- TEEcorrelate $\rightarrow$ Lightweight defense against fine-grained PC leakage
- Keeps performance counters usable in TEEs

Conclusion

- TEEcorrelate $\rightarrow$ Lightweight defense against fine-grained PC leakage
- Keeps performance counters usable in TEEs
- Applicable to any TEE implementation

Conclusion

- TEEcorrelate $\rightarrow$ Lightweight defense against fine-grained PC leakage
- Keeps performance counters usable in TEEs
- Applicable to any TEE implementation

Conclusion

- TEEcorrelate → Lightweight defense against fine-grained PC leakage
- Keeps performance counters usable in TEEs
- Applicable to any TEE implementation

hannes.weissteiner@tugraz.at
hweissi@infosec.exchange
hannesweissteiner.com

Acknowledgments

This research was made possible by generous funding from:

Supported in part by the European Research Council (ERC project FSSec 101076409) and the Austrian Science Fund (FWF SFB project SPyCoDe 10.55776/F85), Deutsche Forschungsgemeinschaft (project ReTEE) and the National Research Center for Applied Cybersecurity ATHENE as part of the PORTUNUS project in the research area Crypto. Additional funding was provided by generous gifts from Red Hat, Google, and Intel. Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the funding parties.

TEEcorrelate

An Information-Preserving Defense against Performance-Counter Attacks on TEEs

Hannes Weissteiner Fabian Rauscher Robin Leander Schröder Jonas Juffinger
Stefan Gast Jan Wichelmann Thomas Eisenbarth Daniel Gruss

Graz University of Technology

USENIX 2025

› isec.tugraz.at