TU Graz
SCIENCE
PASSION
TECHNOLOGY

Secret Spilling Drive:

Leaking User Behavior through SSD Contention

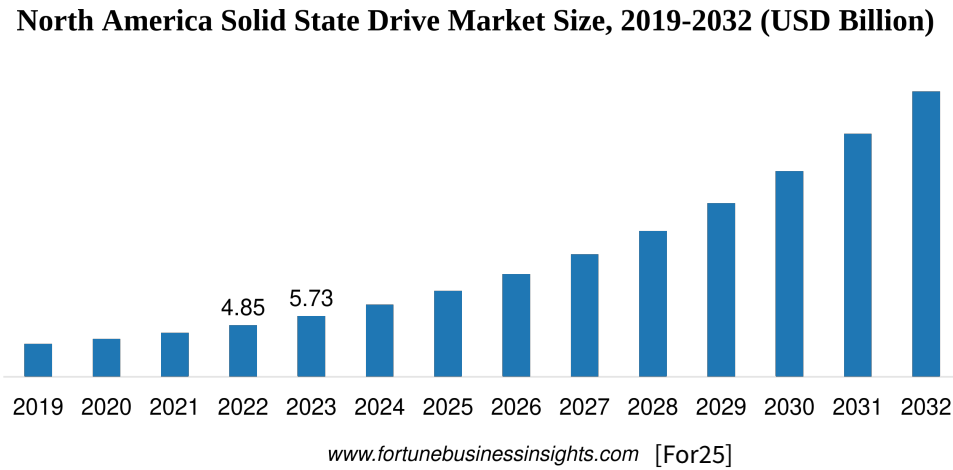
Jonas Juffinger[1] Fabian Rauscher[1] Giuseppe La Manna[2] Daniel Gruss[1]

Graz University of Technology[1], Graz, Austria | Amazon[2]

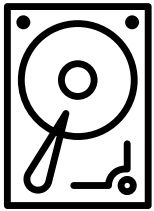
NDSS 2025

› isec.tugraz.at

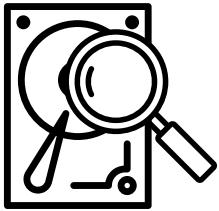
Solid State Drives



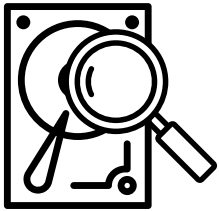
HDD



HDD

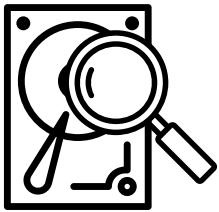


HDD Side Channel Attacks



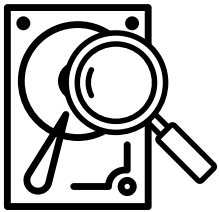
- Disk arm movement [KW91] (1991)
  - 56 bit/s covert channel

HDD Side Channel Attacks



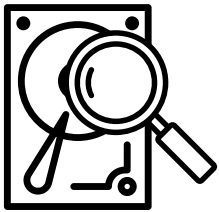
- Disk arm movement [KW91] (1991)
  - 56 bit/s covert channel
- Contention [LMS14]
  - 0.1 bit/s covert channel

HDD Side Channel Attacks



- Disk arm movement [KW91] (1991)
  - 56 bit/s covert channel
- Contention [LMS14]
  - 0.1 bit/s covert channel
- Emitted Magnetic Radiation [BKS15]
  - OS and application remote fingerprinting

HDD Side Channel Attacks

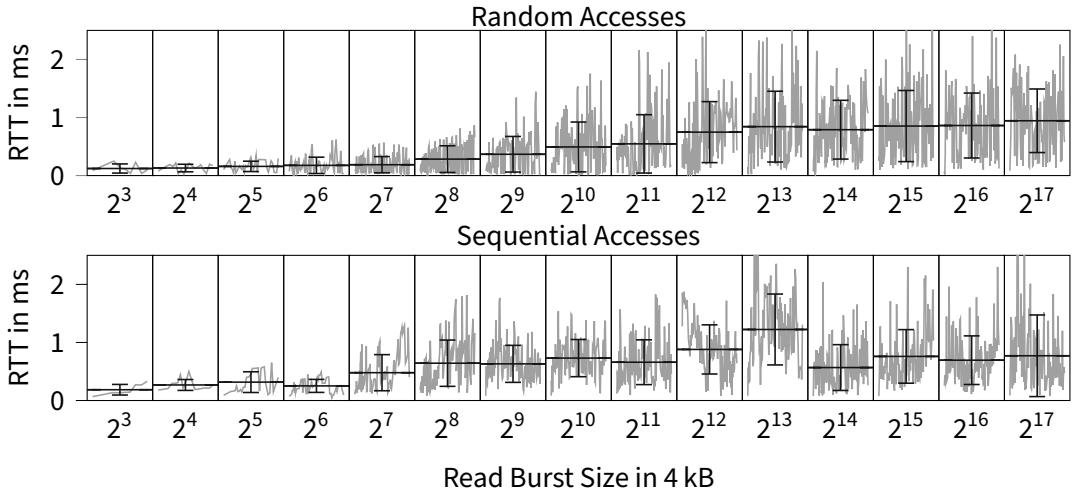


- Disk arm movement [KW91] (1991)
  - 56 bit/s covert channel
- Contention [LMS14]
  - 0.1 bit/s covert channel
- Emitted Magnetic Radiation [BKS15]
  - OS and application remote fingerprinting
- Emitted Noise [Gur+17]
  - 2 bit/s remote covert channel

What About SSDs?

SSD	Model Name	Size	DRAM Cache	PCIe
$\mathcal{A}$	Samsung 980 Pro	256 GB	512 MB LPDDR4	4.0
$\mathcal{B}$	Samsung 980	1 TB	64 MB HMB	3.0
$\mathcal{C}$	Samsung 970 Evo	1 TB	–	3.0
$\mathcal{D}$	Samsung MZVL21T0HCLR-00BL7	1 TB	1 GB LPDDR4	4.0
$\mathcal{E}$	Samsung 970 Evo Plus	2 TB	–	3.0
$\mathcal{F}$	Crucial P5	1 TB	512 MB LPDDR4	4.0
$\mathcal{G}$	Crucial P5 Plus	500 GB	1 GB LPDDR4	4.0
$\mathcal{H}$	Kingston SA2000M81000G	1 TB	1 GB DDR3L	3.0
$\mathcal{I}$	Toshiba KXG6AZNV1T02	1 TB	–	3.0
$\mathcal{J}$	ADATA XPG Gammix S50 Lite	512 GB	512 MB DDR4	4.0
$\mathcal{K}$	Gigabyte Aorus Gen4	500 GB	512 MB DDR4	4.0
$\mathcal{L}$	Western Digital Blue SN550	1 TB	64 MB HMB	3.0

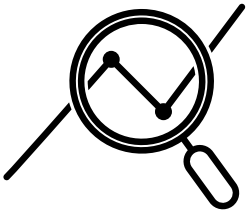
SSD Contention



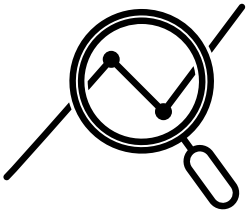
What Can We Detect?

What Can We Detect?

Two Variables:



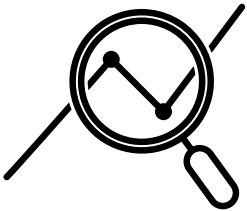
What Can We Detect?



Two Variables:

1. How much is read from the disk

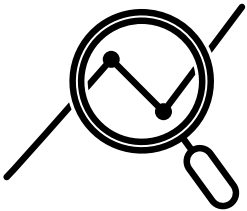
What Can We Detect?



Two Variables:

1. How much is read from the disk
   - victim read size

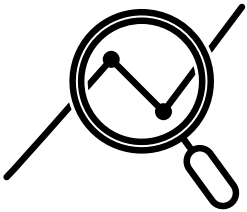
What Can We Detect?



Two Variables:

1. How much is read from the disk
   - victim read size
2. How often do we measure

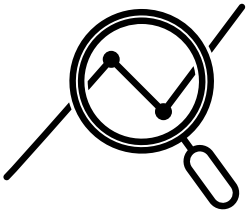
What Can We Detect?



Two Variables:

1. How much is read from the disk
   - victim read size
2. How often do we measure
   - observer read delay

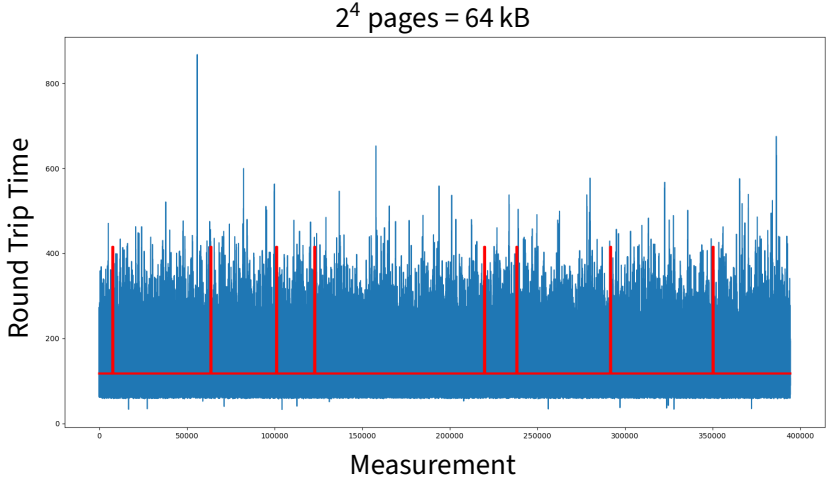
What Can We Detect?



Two Variables:

1. How much is read from the disk
   - victim read size
2. How often do we measure
   - observer read delay
   - To many measurements create contention

Victim Read Size

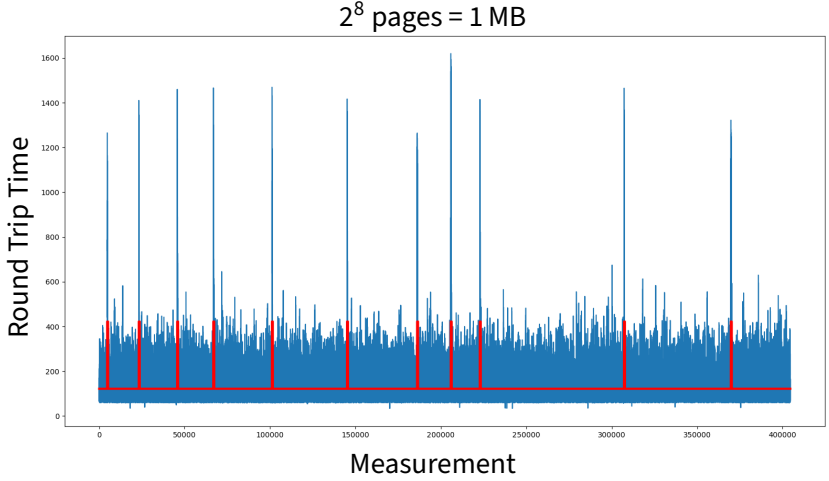


Victim Read Size

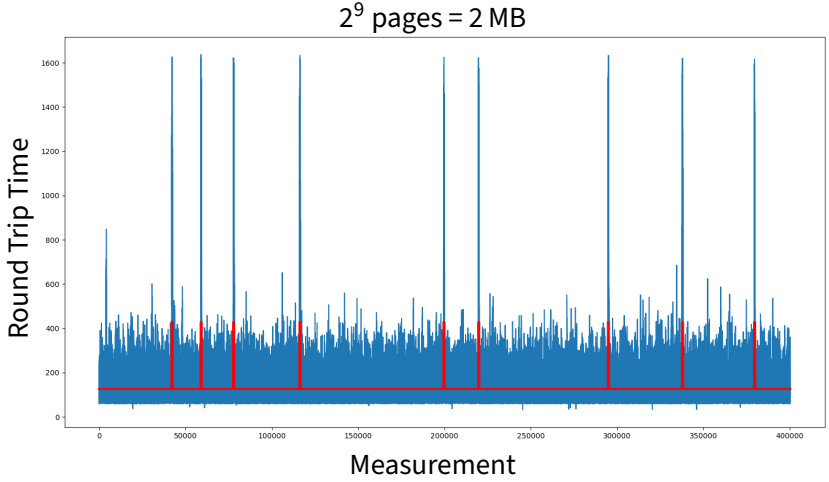
Victim Read Size

Victim Read Size

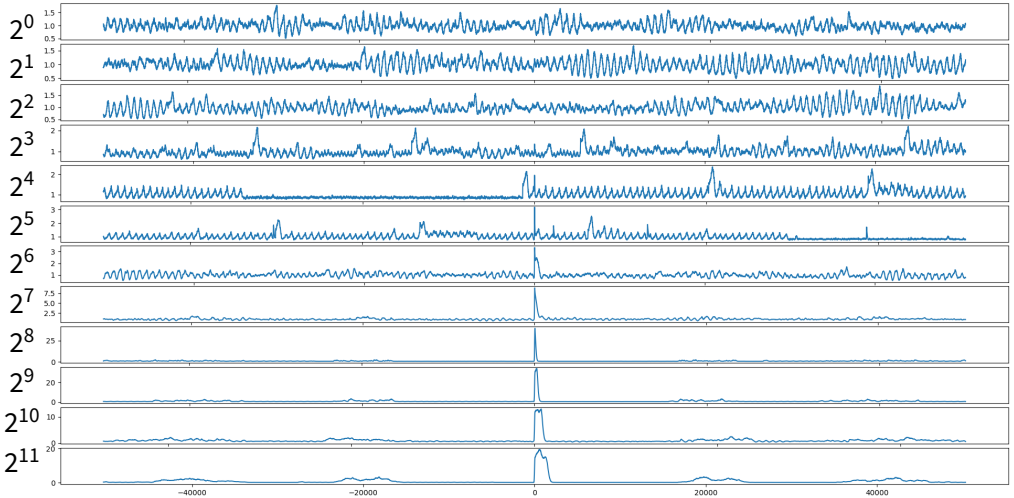
Victim Read Size



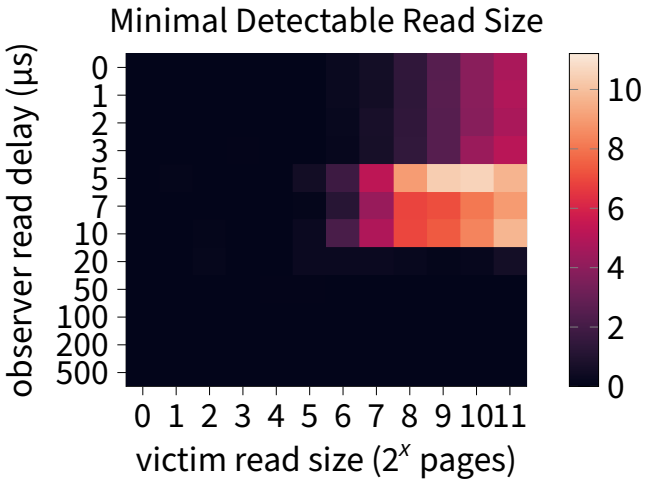
Victim Read Size

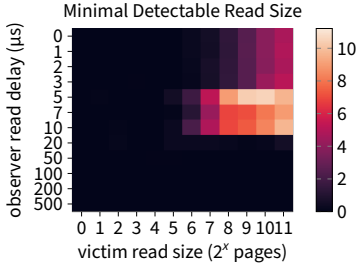


Victim Read Size – Correlation

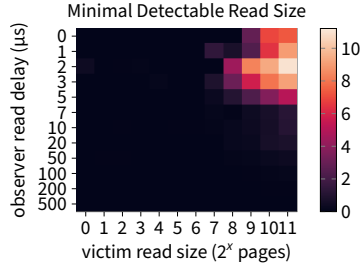


Minimal Detectable Read Size

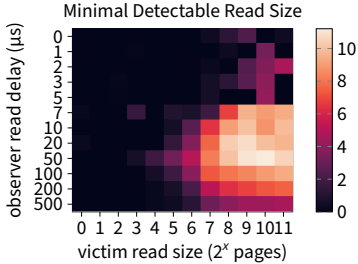




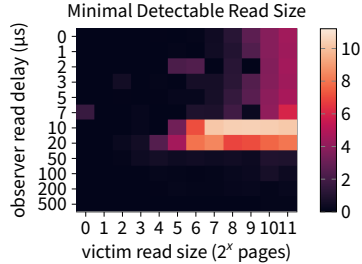
(a) SSD $\mathcal{A}$



(b) SSD $\mathcal{D}$

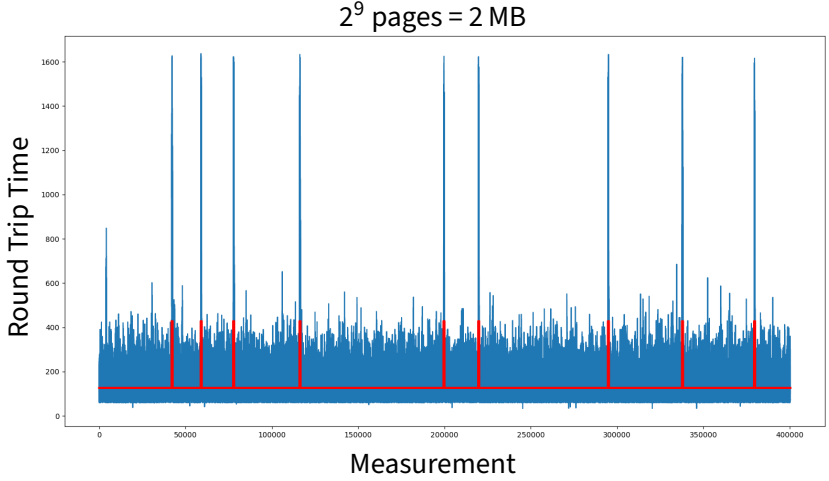


(c) SSD $\mathcal{H}$



(d) SSD $\mathcal{J}$

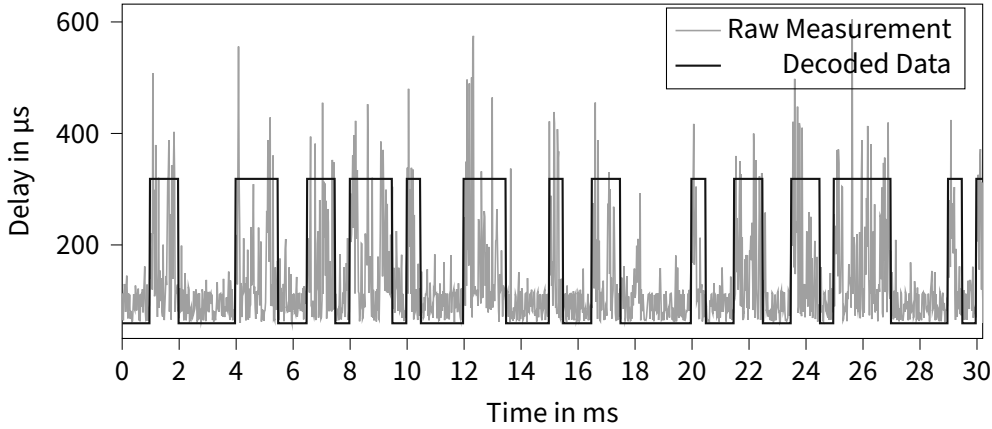
Data Transmission



Covert Channel

Between Processes and Virtual Machines

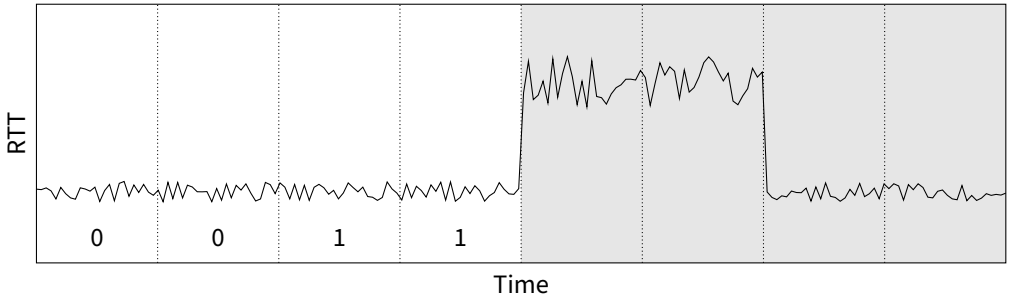
Covert Channel



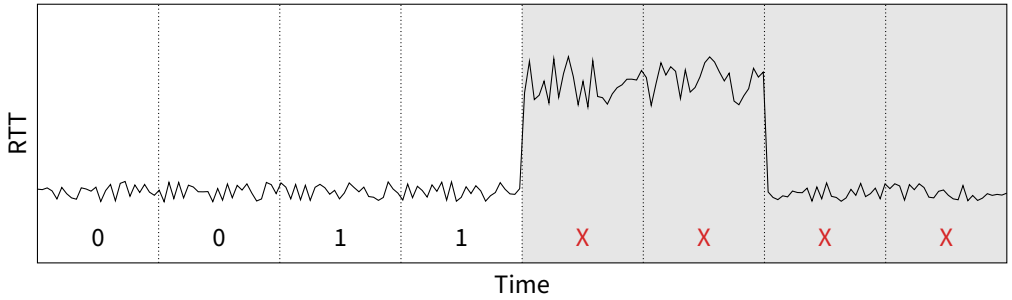
Covert Channel Results

	Process					Virtual Machine				
	1 000 bit/s, $f = 0.12$		Fastest per SSD			500 bit/s, $f = 0.5$		Fastest per SSD		
SSD	Error	Capacity	Trans. Rate	Error	Capacity	Error	Capacity	Trans. Rate	Error	Capacity
$\mathcal{A}$	13.4 %	431 bit/s	2 000 bit/s	14.5 %	808 bit/s	17.9 %	161 bit/s	1 000 bit/s	21.0 %	258 bit/s
$\mathcal{B}$	16.3 %	359 bit/s	2 000 bit/s	14.9 %	787 bit/s	15.4 %	191 bit/s	2 000 bit/s	18.6 %	615 bit/s
$\mathcal{C}$	13.1 %	439 bit/s	5 000 bit/s	19.0 %	1 492 bit/s	15.8 %	186 bit/s	1 000 bit/s	18.8 %	303 bit/s
$\mathcal{D}$	19.6 %	285 bit/s	5 000 bit/s	16.4 %	1 784 bit/s	25.8 %	88 bit/s	1 000 bit/s	29.5 %	124 bit/s
$\mathcal{E}$	13.0 %	441 bit/s	5 000 bit/s	19.4 %	1 447 bit/s	13.3 %	217 bit/s	5 000 bit/s	18.9 %	1 503 bit/s
$\mathcal{F}$	17.4 %	333 bit/s	2 000 bit/s	17.5 %	660 bit/s	13.7 %	212 bit/s	1 000 bit/s	14.5 %	404 bit/s
$\mathcal{G}$	15.6 %	375 bit/s	2 000 bit/s	14.3 %	814 bit/s	18.2 %	158 bit/s	2 000 bit/s	18.8 %	605 bit/s
$\mathcal{H}$	25.0 %	188 bit/s	2 000 bit/s	24.2 %	403 bit/s	14.0 %	207 bit/s	2 000 bit/s	21.6 %	493 bit/s
$\mathcal{I}$	13.5 %	428 bit/s	2 000 bit/s	17.5 %	664 bit/s	19.4 %	145 bit/s	1 000 bit/s	21.0 %	258 bit/s
$\mathcal{J}$	13.2 %	437 bit/s	2 000 bit/s	17.8 %	647 bit/s	14.9 %	196 bit/s	2 000 bit/s	19.1 %	592 bit/s
$\mathcal{K}$	29.2 %	129 bit/s	2 000 bit/s	15.5 %	755 bit/s	14.6 %	200 bit/s	2 000 bit/s	16.6 %	702 bit/s
$\mathcal{L}$	13.1 %	439 bit/s	5 000 bit/s	20.8 %	1 313 bit/s	15.1 %	194 bit/s	1 000 bit/s	13.5 %	429 bit/s
Avg	16.9 %	357 bit/s	3 000 bit/s	17.7 %	964 bit/s	16.5 %	180 bit/s	1 750 bit/s	19.3 %	524 bit/s

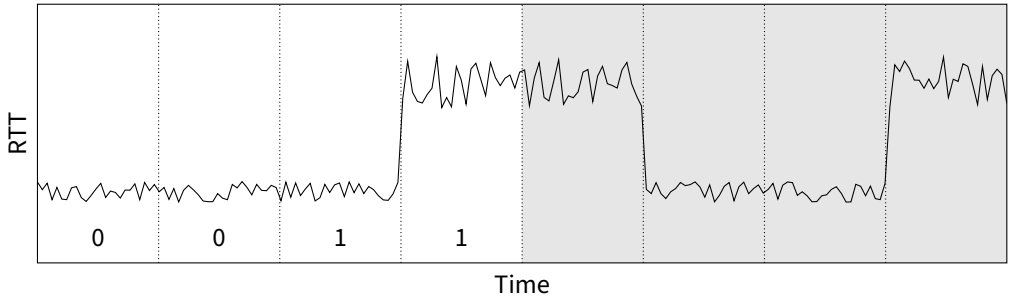
Threshold Detection



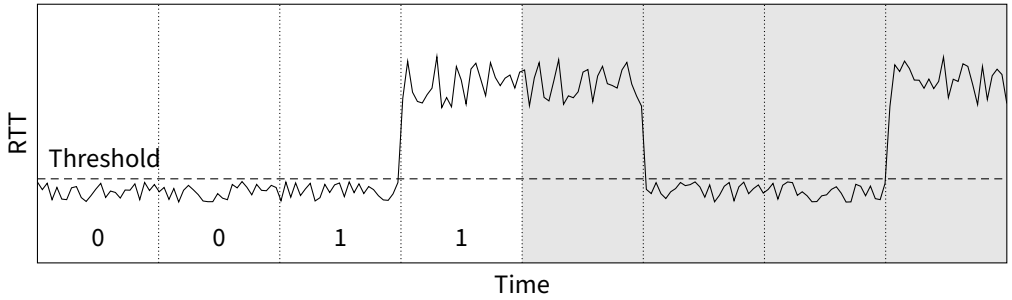
Threshold Detection



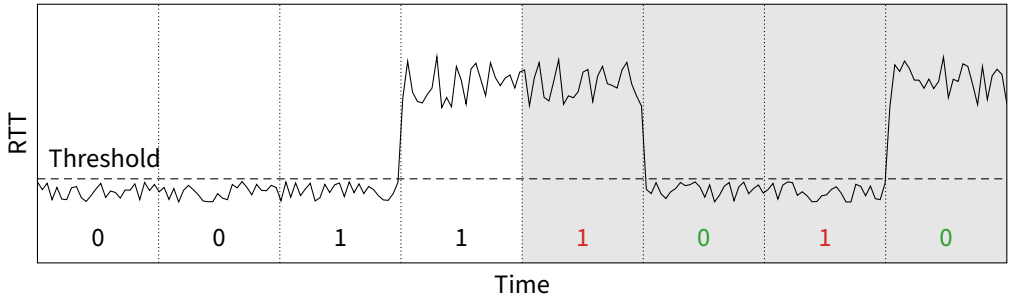
Threshold Detection



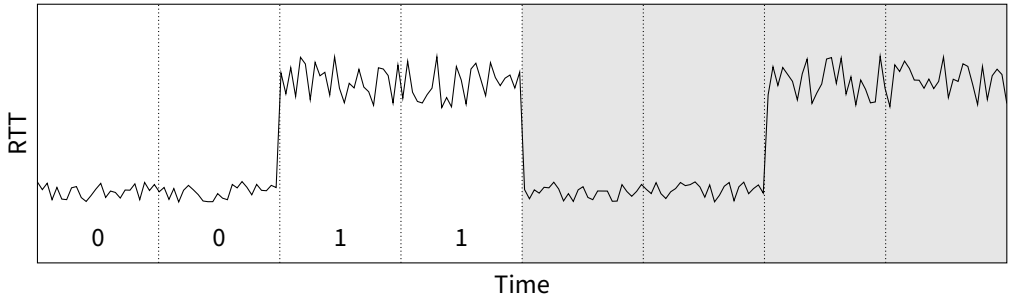
Threshold Detection



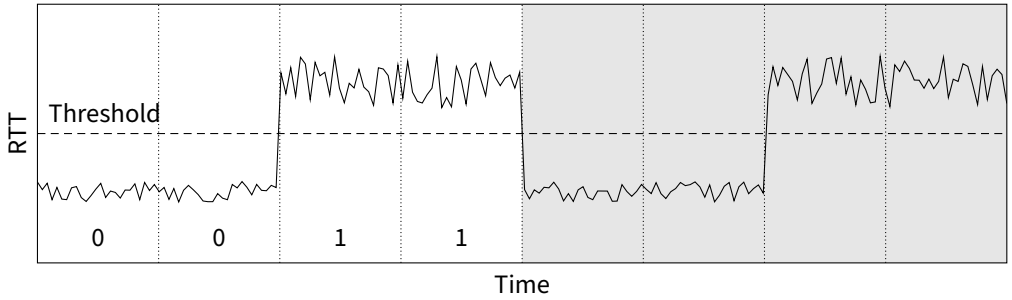
Threshold Detection



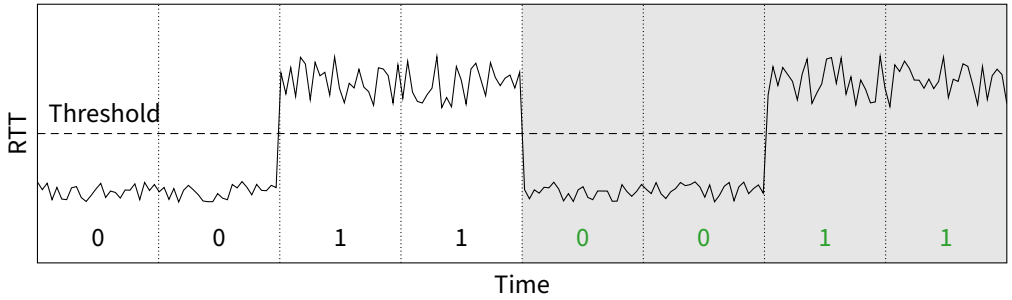
Threshold Detection



Threshold Detection



Threshold Detection



Covert Channel Results - Process

SSD	1 000 bit/s, $f = 0.12$		Fastest per SSD		
	Error	Capacity	Trans. Rate	Error	Capacity
$\mathcal{C}$	13.1 %	439 bit/s	5 000 bit/s	19.0 %	1 492 bit/s
$\mathcal{D}$	19.6 %	285 bit/s	5 000 bit/s	16.4 %	1 784 bit/s
$\mathcal{E}$	13.0 %	441 bit/s	5 000 bit/s	19.4 %	1 447 bit/s
$\mathcal{F}$	17.4 %	333 bit/s	2 000 bit/s	17.5 %	660 bit/s
$\mathcal{H}$	25.0 %	188 bit/s	2 000 bit/s	24.2 %	403 bit/s
$\mathcal{J}$	13.2 %	437 bit/s	2 000 bit/s	17.8 %	647 bit/s
			...		
Avg	16.9 %	357 bit/s	3 000 bit/s	17.7 %	964 bit/s

Covert Channel Results - Process

SSD	1 000 bit/s, $f = 0.12$		Fastest per SSD		
	Error	Capacity	Trans. Rate	Error	Capacity
$\mathcal{C}$	13.1 %	439 bit/s	5 000 bit/s	19.0 %	1 492 bit/s
$\mathcal{D}$	19.6 %	285 bit/s	5 000 bit/s	16.4 %	1 784 bit/s
$\mathcal{E}$	13.0 %	441 bit/s	5 000 bit/s	19.4 %	1 447 bit/s
$\mathcal{F}$	17.4 %	333 bit/s	2 000 bit/s	17.5 %	660 bit/s
$\mathcal{H}$	25.0 %	188 bit/s	2 000 bit/s	24.2 %	403 bit/s
$\mathcal{J}$	13.2 %	437 bit/s	2 000 bit/s	17.8 %	647 bit/s
			…		
Avg	16.9 %	357 bit/s	3 000 bit/s	17.7 %	964 bit/s

Covert Channel Results - Process

SSD	1 000 bit/s, $f = 0.12$		Fastest per SSD		
	Error	Capacity	Trans. Rate	Error	Capacity
$\mathcal{C}$	13.1 %	439 bit/s	5 000 bit/s	19.0 %	1 492 bit/s
$\mathcal{D}$	19.6 %	285 bit/s	5 000 bit/s	16.4 %	1 784 bit/s
$\mathcal{E}$	13.0 %	441 bit/s	5 000 bit/s	19.4 %	1 447 bit/s
$\mathcal{F}$	17.4 %	333 bit/s	2 000 bit/s	17.5 %	660 bit/s
$\mathcal{H}$	25.0 %	188 bit/s	2 000 bit/s	24.2 %	403 bit/s
$\mathcal{J}$	13.2 %	437 bit/s	2 000 bit/s	17.8 %	647 bit/s
			...		
Avg	16.9 %	357 bit/s	3 000 bit/s	17.7 %	964 bit/s

Covert Channel Results - Virtual Machine

SSD	500 bit/s, $f = 0.5$		Fastest per SSD		
	Error	Capacity	Trans. Rate	Error	Capacity
$\mathcal{A}$	17.9 %	161 bit/s	1 000 bit/s	21.0 %	258 bit/s
$\mathcal{B}$	15.4 %	191 bit/s	2 000 bit/s	18.6 %	615 bit/s
$\mathcal{D}$	25.8 %	88 bit/s	1 000 bit/s	29.5 %	124 bit/s
$\mathcal{E}$	13.3 %	217 bit/s	5 000 bit/s	18.9 %	1 503 bit/s
$\mathcal{I}$	19.4 %	145 bit/s	1 000 bit/s	21.0 %	258 bit/s
$\mathcal{K}$	14.6 %	200 bit/s	2 000 bit/s	16.6 %	702 bit/s
			…		
Avg	16.5 %	180 bit/s	1 750 bit/s	19.3 %	524 bit/s

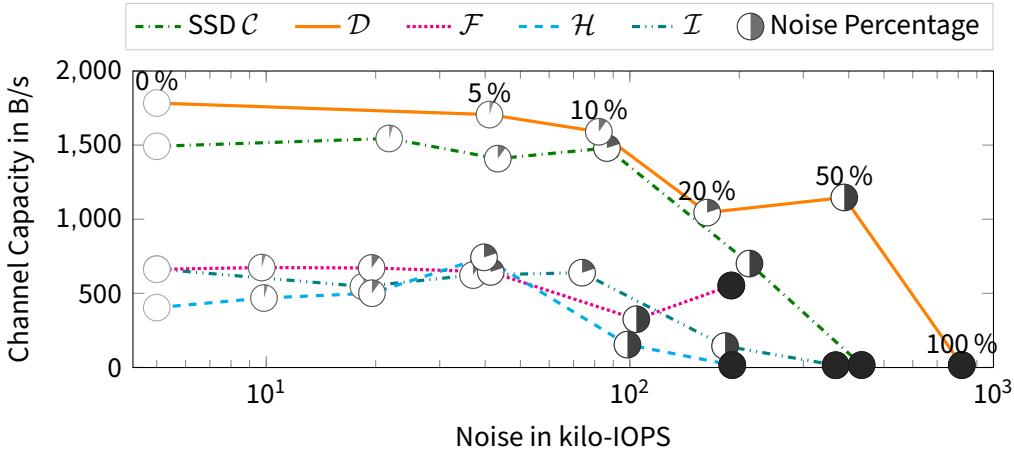
Covert Channel Results - Virtual Machine

SSD	500 bit/s, $f = 0.5$		Fastest per SSD		
	Error	Capacity	Trans. Rate	Error	Capacity
$\mathcal{A}$	17.9 %	161 bit/s	1 000 bit/s	21.0 %	258 bit/s
$\mathcal{B}$	15.4 %	191 bit/s	2 000 bit/s	18.6 %	615 bit/s
$\mathcal{D}$	25.8 %	88 bit/s	1 000 bit/s	29.5 %	124 bit/s
$\mathcal{E}$	13.3 %	217 bit/s	5 000 bit/s	18.9 %	1 503 bit/s
$\mathcal{I}$	19.4 %	145 bit/s	1 000 bit/s	21.0 %	258 bit/s
$\mathcal{K}$	14.6 %	200 bit/s	2 000 bit/s	16.6 %	702 bit/s
			...		
Avg	16.5 %	180 bit/s	1 750 bit/s	19.3 %	524 bit/s

Covert Channel Results - Virtual Machine

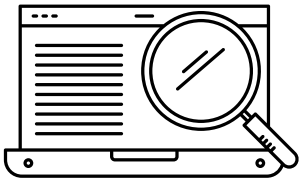
SSD	500 bit/s, $f = 0.5$		Fastest per SSD		
	Error	Capacity	Trans. Rate	Error	Capacity
$\mathcal{A}$	17.9 %	161 bit/s	1 000 bit/s	21.0 %	258 bit/s
$\mathcal{B}$	15.4 %	191 bit/s	2 000 bit/s	18.6 %	615 bit/s
$\mathcal{D}$	25.8 %	88 bit/s	1 000 bit/s	29.5 %	124 bit/s
$\mathcal{E}$	13.3 %	217 bit/s	5 000 bit/s	18.9 %	1 503 bit/s
$\mathcal{I}$	19.4 %	145 bit/s	1 000 bit/s	21.0 %	258 bit/s
$\mathcal{K}$	14.6 %	200 bit/s	2 000 bit/s	16.6 %	702 bit/s
			…		
Avg	16.5 %	180 bit/s	1 750 bit/s	19.3 %	524 bit/s

Noise Impact



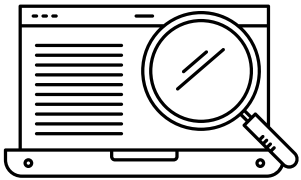
Website Fingerprinting

Website Fingerprinting



Identify websites currently opened on the same machine.

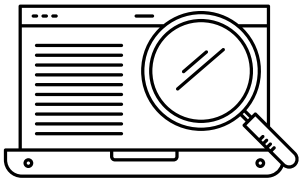
Website Fingerprinting



Identify websites currently opened on the same machine.

- Web browsers cache assets on the disk

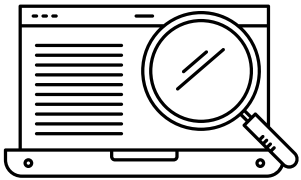
Website Fingerprinting



Identify websites currently opened on the same machine.

- Web browsers cache assets on the disk
- They are read from the disk on each load

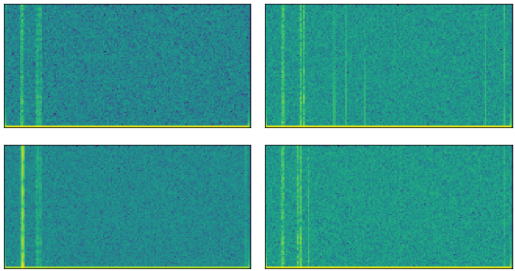
Website Fingerprinting



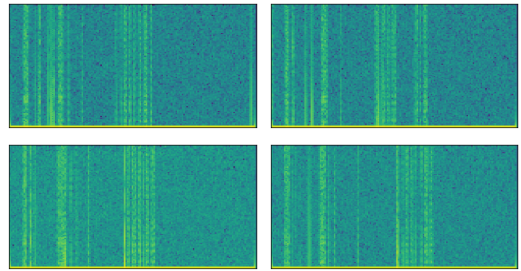
Identify websites currently opened on the same machine.

- Web browsers cache assets on the disk
- They are read from the disk on each load
- Create a unique fingerprint

Website Spectrograms

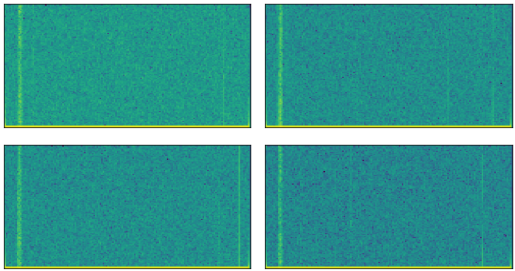


(a) google.com

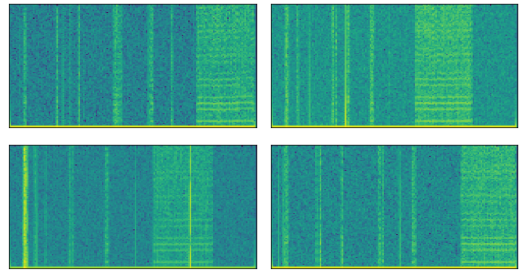


(b) youtube.com

Website Spectrograms

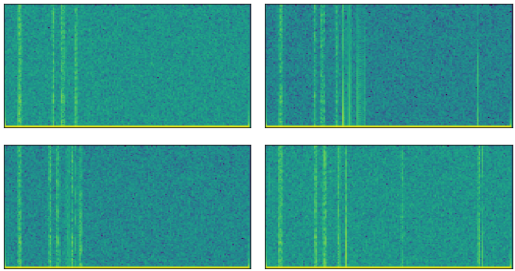


(c) facebook.com

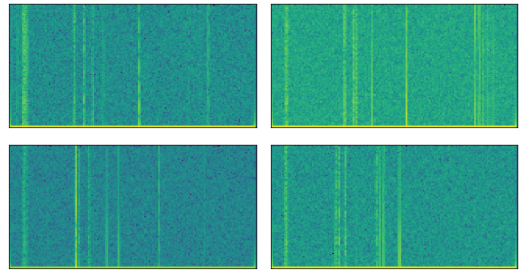


(d) qq.com

Website Spectrograms

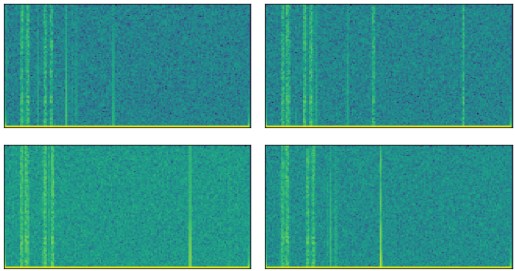


(e) xhamster.com

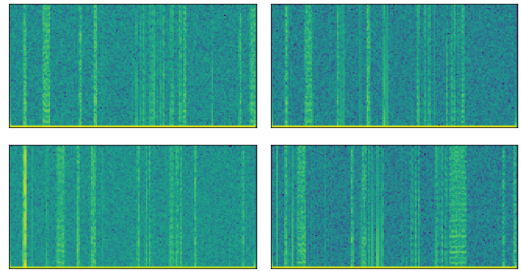


(f) imdb.com

Website Spectrograms

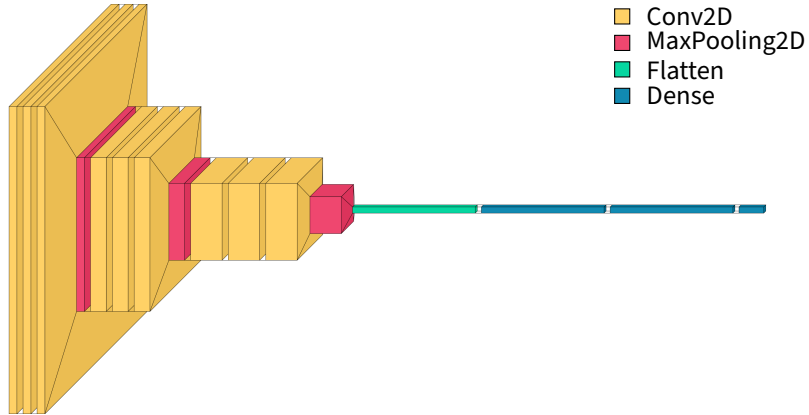


(g) force.com

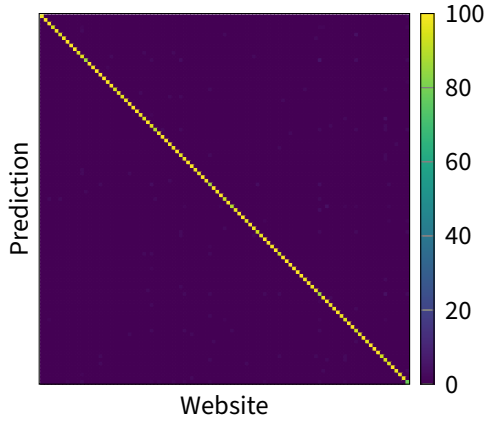


(h) dropbox.com

Convolutional Neural Network



Website Fingerprinting - Results

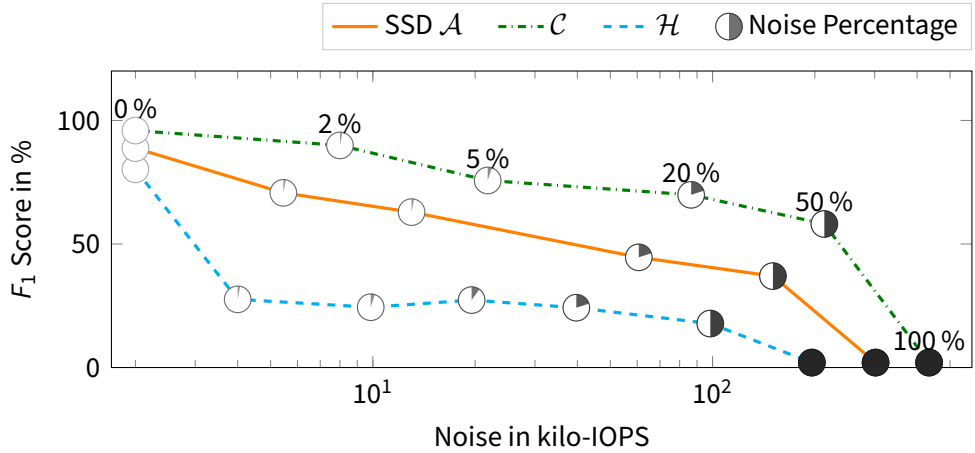


Website Fingerprinting - Results

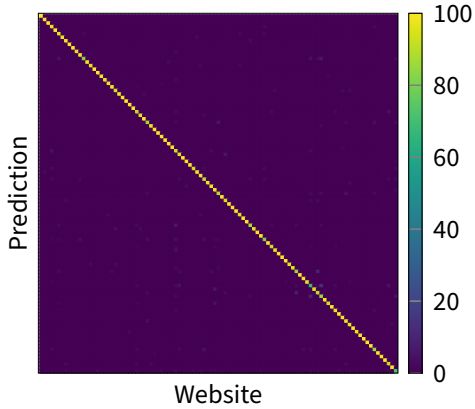
100 Websites + Open World Dataset

SSD	DRAM Cache	PCIe	Accuracy ↓
Crucial P5	✓	4.0	97.0 %
Gigabyte Aorus Gen4	✓	4.0	97.0 %
Samsung 970 Evo Plus	✗	3.0	96.6 %
	...		
ADATA XPG Gammix S50 Lite	✓	4.0	88.7 %
Kingston SA2000M81000G	✓	3.0	80.2 %

Noise Impact

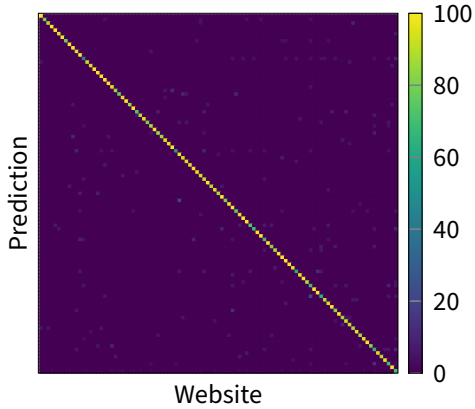


Noise Impact - Heatmap - SSD $\mathcal{C}$



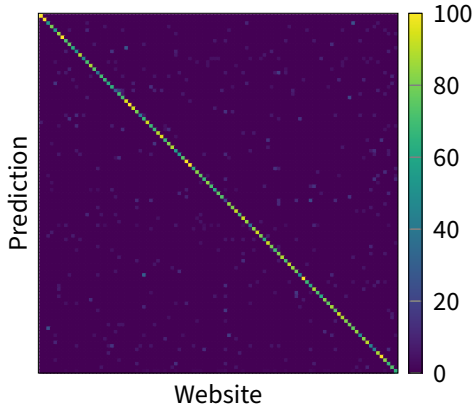
0 % Noise – 95.9 %

Noise Impact - Heatmap - SSD $\mathcal{C}$



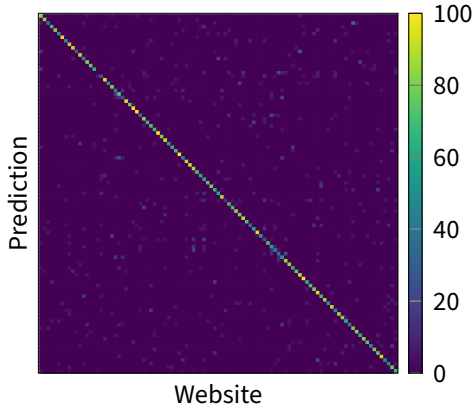
2 % Noise – 89.9 %

Noise Impact - Heatmap - SSD $\mathcal{C}$



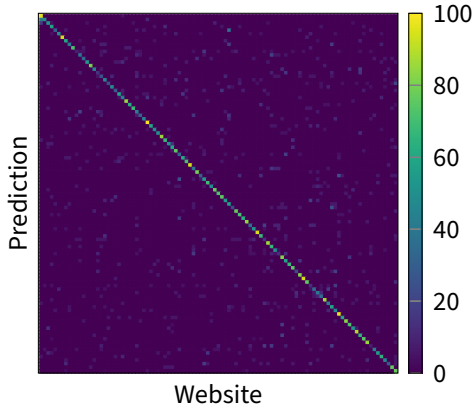
5 % Noise – 75.7 %

Noise Impact - Heatmap - SSD $\mathcal{C}$



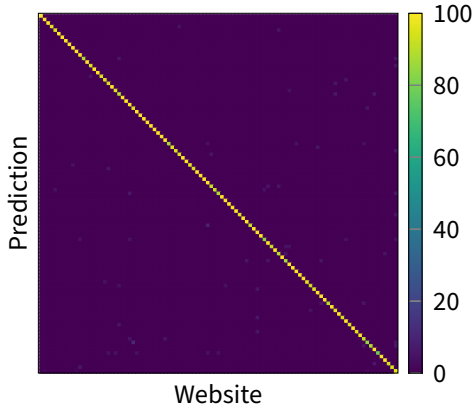
20 % Noise – 69.9 %

Noise Impact - Heatmap - SSD $\mathcal{C}$



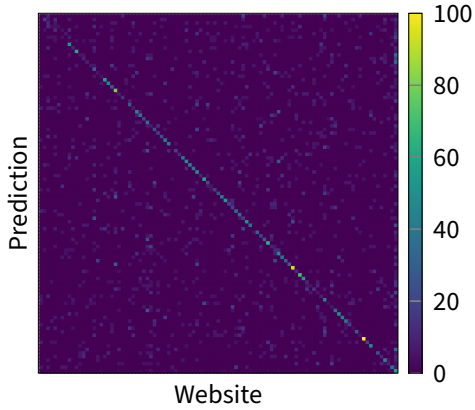
50 % Noise – 58.1 %

Noise Impact - Heatmap - SSD $\mathcal{H}$



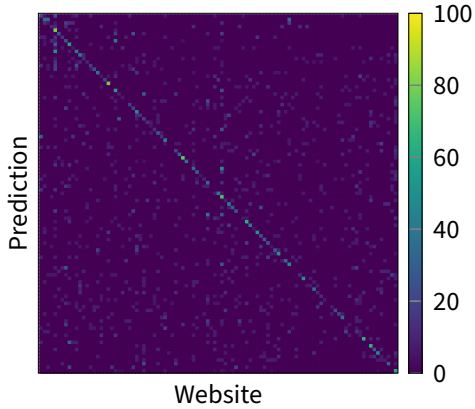
0 % Noise – 80.2 %

Noise Impact - Heatmap - SSD $\mathcal{H}$



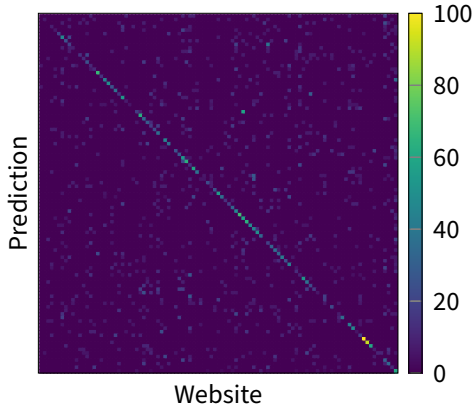
2 % Noise – 27.6 %

Noise Impact - Heatmap - SSD $\mathcal{H}$



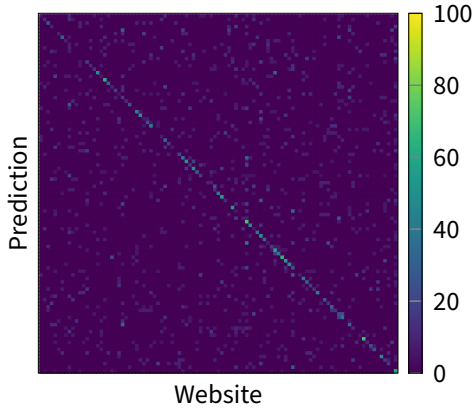
5 % Noise – 24.4 %

Noise Impact - Heatmap - SSD $\mathcal{H}$



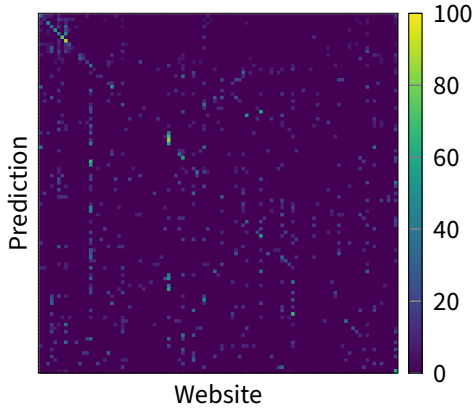
10 % Noise – 27.3 %

Noise Impact - Heatmap - SSD $\mathcal{H}$



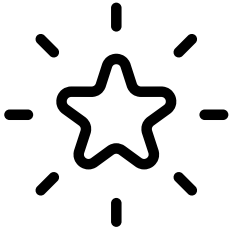
20 % Noise – 24.2 %

Noise Impact - Heatmap - SSD $\mathcal{H}$



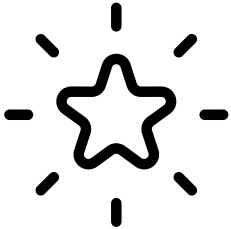
50 % Noise – 17.8 %

Final Remarks



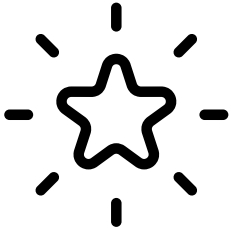
- High IOPS do not protect against contention

Final Remarks



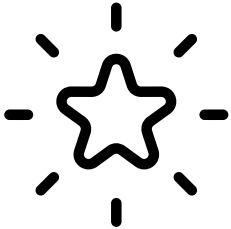
- High IOPS do not protect against contention
- They enable a high bandwidth side channel

Final Remarks



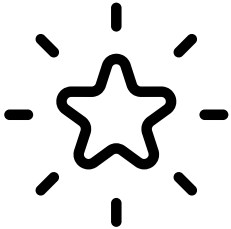
- High IOPS do not protect against contention
- They enable a high bandwidth side channel
- **Covert Channel** with up to 1.8 kbit/s

Final Remarks



- High IOPS do not protect against contention
- They enable a high bandwidth side channel
- **Covert Channel** with up to 1.8 kbit/s
- **Website Fingerprinting** with up to 97 % accuracy

Final Remarks



- High IOPS do not protect against contention
- They enable a high bandwidth side channel
- **Covert Channel** with up to 1.8 kbit/s
- **Website Fingerprinting** with up to 97 % accuracy
- **Difficult** to mitigate

Acknowledgments

This research was made possible by generous funding from:

This research is supported in part by the European Research Council (ERC project FSSec 101076409), and the Austrian Science Fund (FWF SFB project SPyCoDe 10.55776/F85 and FWF project NeRAM I6054). 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.

TU Graz
SCIENCE
PASSION
TECHNOLOGY

Secret Spilling Drive:

Leaking User Behavior through SSD Contention

Jonas Juffinger[1] Fabian Rauscher[1] Giuseppe La Manna[2] Daniel Gruss[1]

Graz University of Technology[1], Graz, Austria | Amazon[2]

NDSS 2025

› isec.tugraz.at

Bibliography I

[BKS15] S. Biedermann, S. Katzenbeisser, and J. Szefer. **Hard Drive Side-Channel Attacks using Smartphone Magnetic Field Sensors**. FC. 2015.

[For25] Fortune Business Insights. **Solid State Drive Market Size, Share & Industry Trends Analysis.** 2025. URL: https://www.fortunebusinessinsights.com/solid-state-drive-market-109839.

[Gur+17] M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici. **Acoustic data exfiltration from speakerless air-gapped computers via covert hard-drive noise ('DiskFiltration')**. ESORICS. 2017.

[KW91] P. A. Karger and J. C. Wray. **Storage Channels in Disk Arm Optimization**. S&P. 1991.

[LMS14] B. Lipinski, W. Mazurczyk, and K. Szczypiorski. **Improving Hard Disk Contention-based Covert Channel in Cloud Computing Environment**. S&P Workshops. 2014.