I Know What You Sync: Covert and Side Channel Attacks on File Systems via syncfs

Cheng Gu, Yicheng Zhang, Nael Abu-Ghazaleh

cgu024@ucr.edu

University of California, Riverside

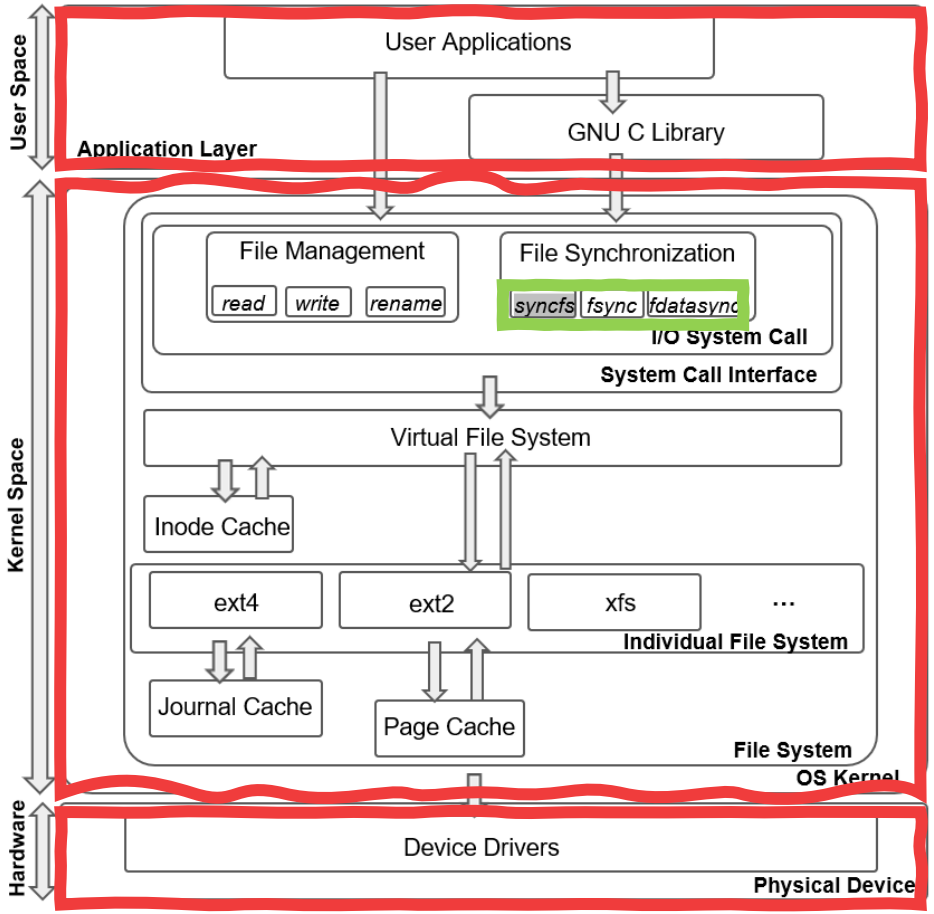
UC RIVERSIDE

Outline

- Background: File system structure and syncfs system call.
- Threat model and leakage Vectors.
- Covert channel attack.
- Two side channel attacks:
  - Web fingerprinting.
  - Video fingerprinting.

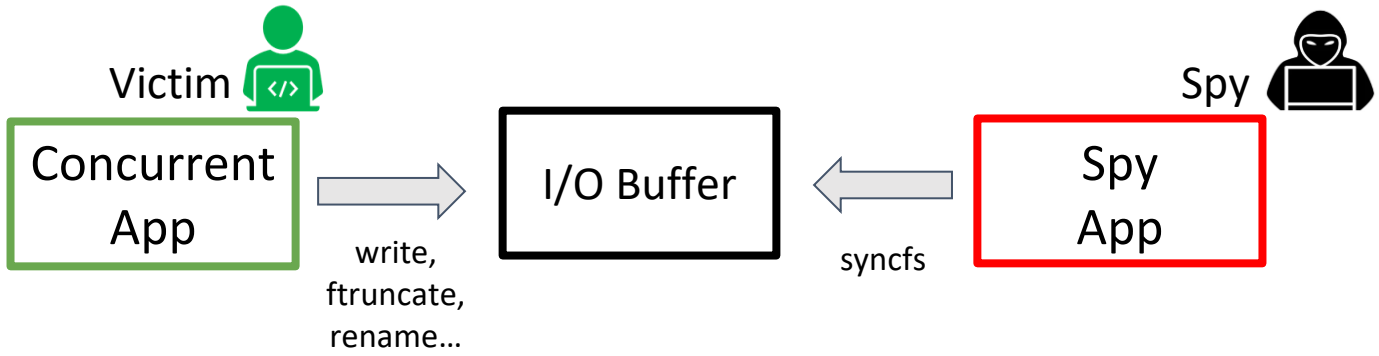
File System Structure

- Application layer.
- OS kernel.
  - System call interface.
  - Virtual file system.
  - Individual file system.
  - I/O buffers.
- Physical device.



Threat model

- A malicious program runs in the background.
  - Standard application-level permissions.
  - Co-locate on the same file system.
  - Periodically profiles the I/O buffers.



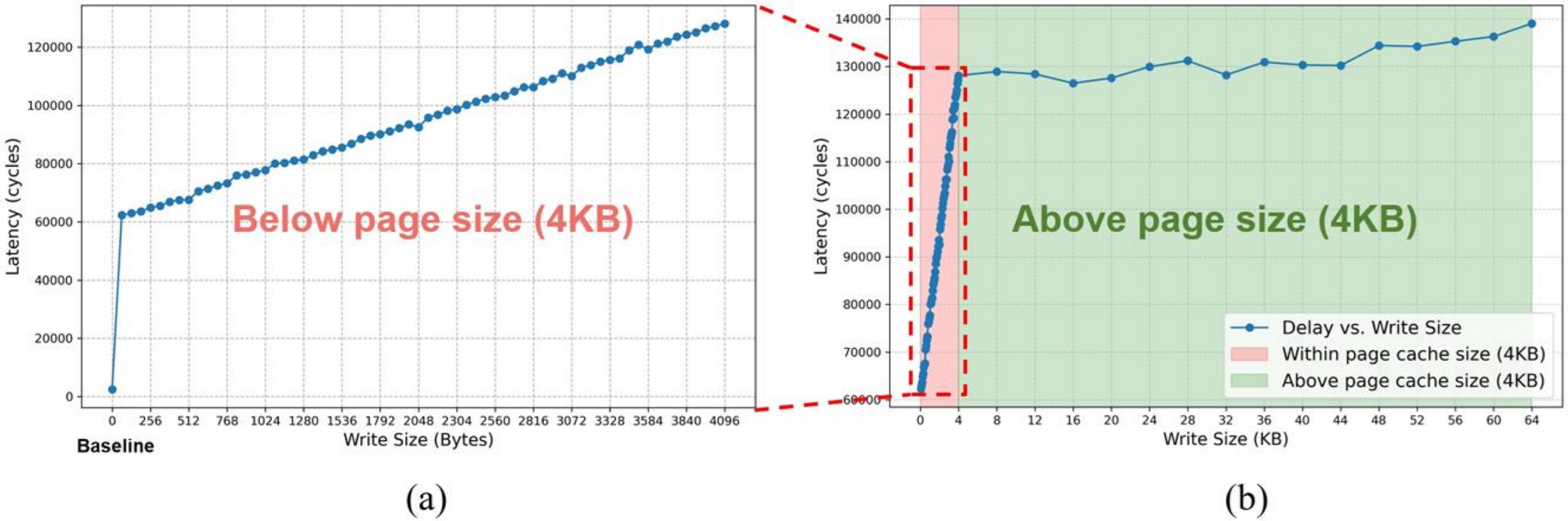
Leakage Vectors

- Measuring I/O syscall footprints via syncfs.
  - Different operations generate different latency.

I/O operation	Affected buffers	Average latency (cycles)	Standard deviation
baseline	N/A	2509	491
write	Page cache, journal and inode	121092	11436
write(O_SYNC)	journal	41406	4670
ftruncate	journal and inode	61315	6916
rename	journal and inode	66774	8134

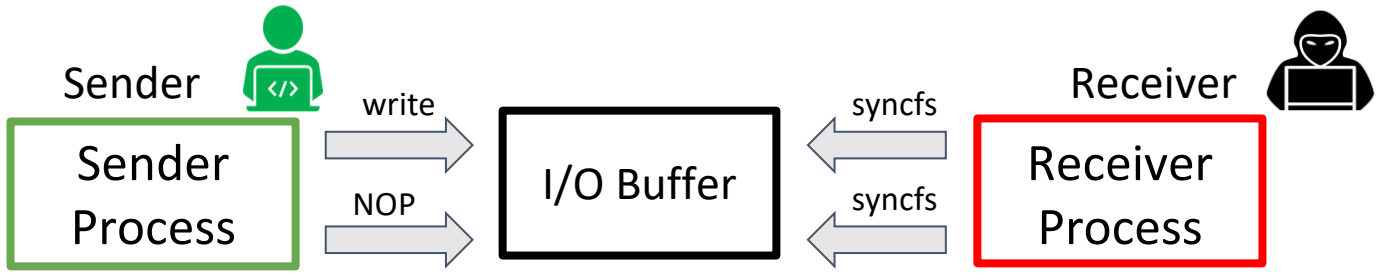
Leakage Vectors

- For write sizes below 4 KB, syncfs latency grows linearly. For write sizes above 4 KB, syncfs latency slows due to I/O parallelism, with fluctuations from dynamic flusher thread adjustments.



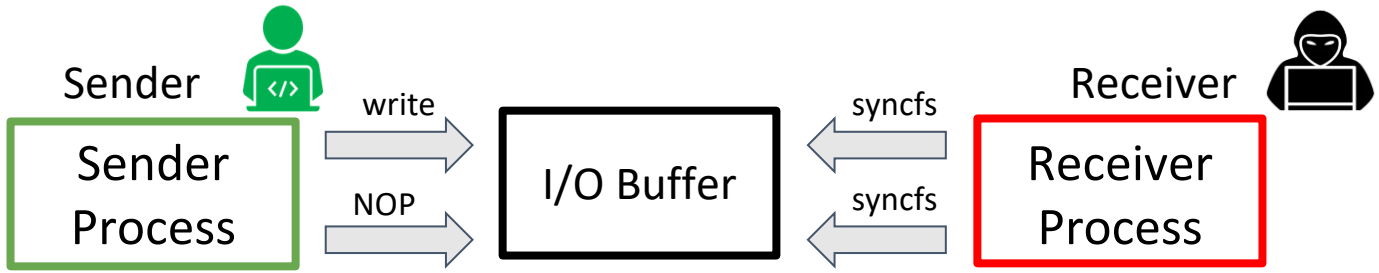
Covert Channel

- Sender and receiver locate on the same file system.



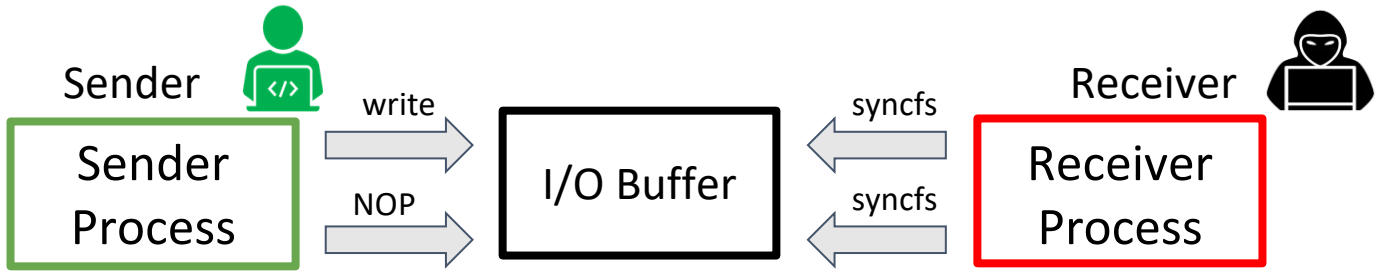
Covert Channel

- Sender and receiver locate on the same file system.
- Sender writes a string (64 Bytes) to a local file or no operation.



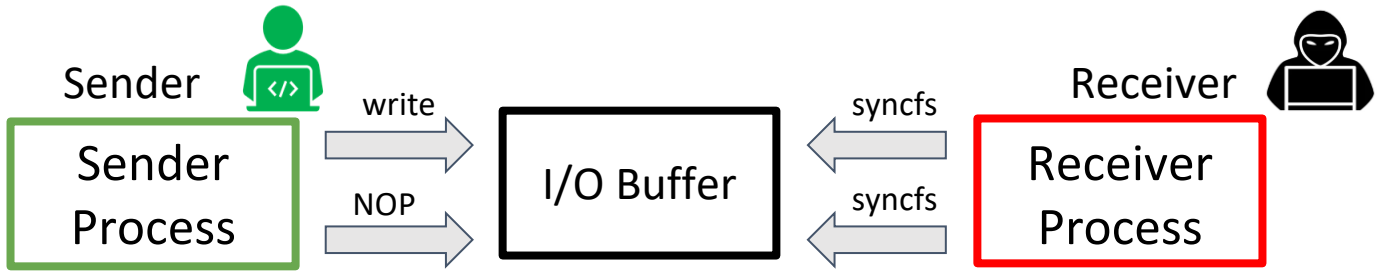
Covert Channel

- Sender and receiver locate on the same file system.
- Sender writes a string (64 Bytes) to a local file or no operation.
- Receiver measures syncfs delay.

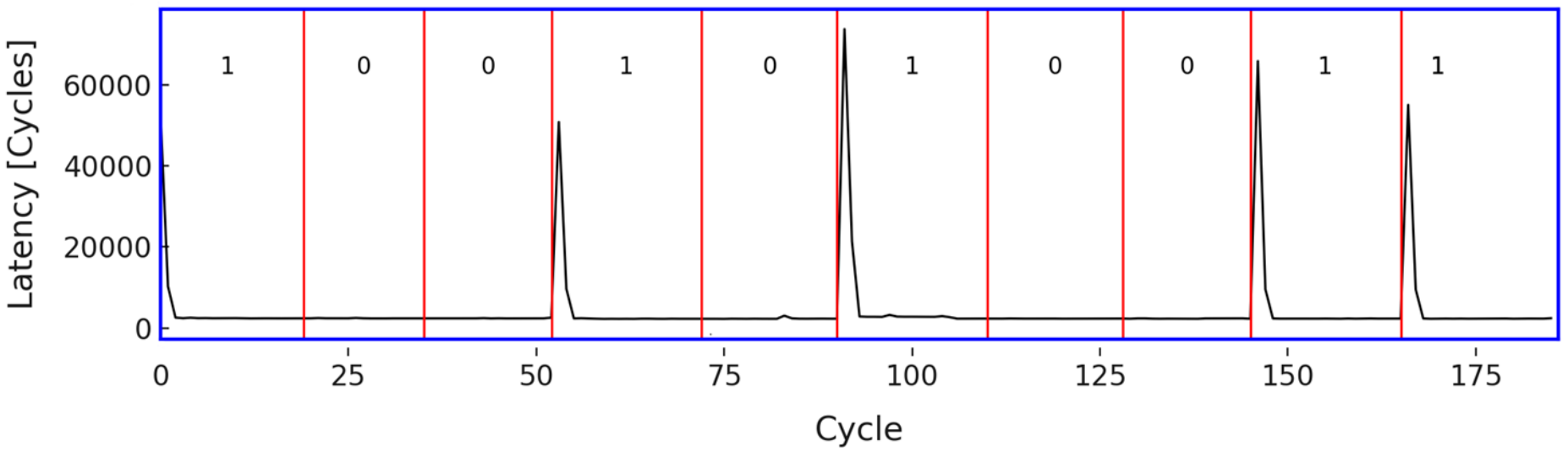


Covert Channel

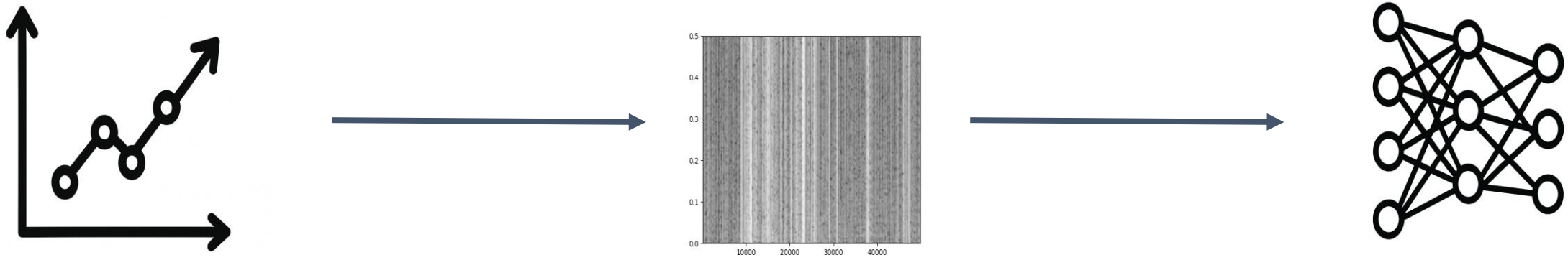
- Sender and receiver locate on the same file system.
- Sender writes a string (64 Bytes) to a local file or no operation.
- Receiver measures syncfs delay.
- Bandwidth: 7.6 Kbps.
- Error Rate: 1.9%.



Covert Channel

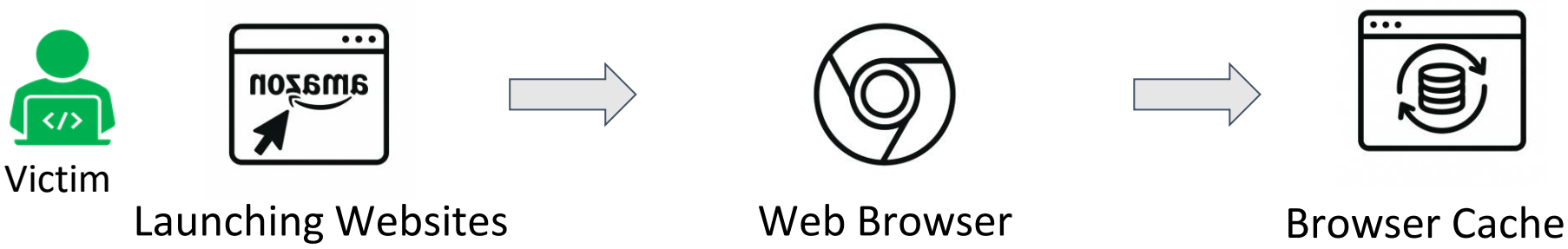


Side-channel Attacks Overview



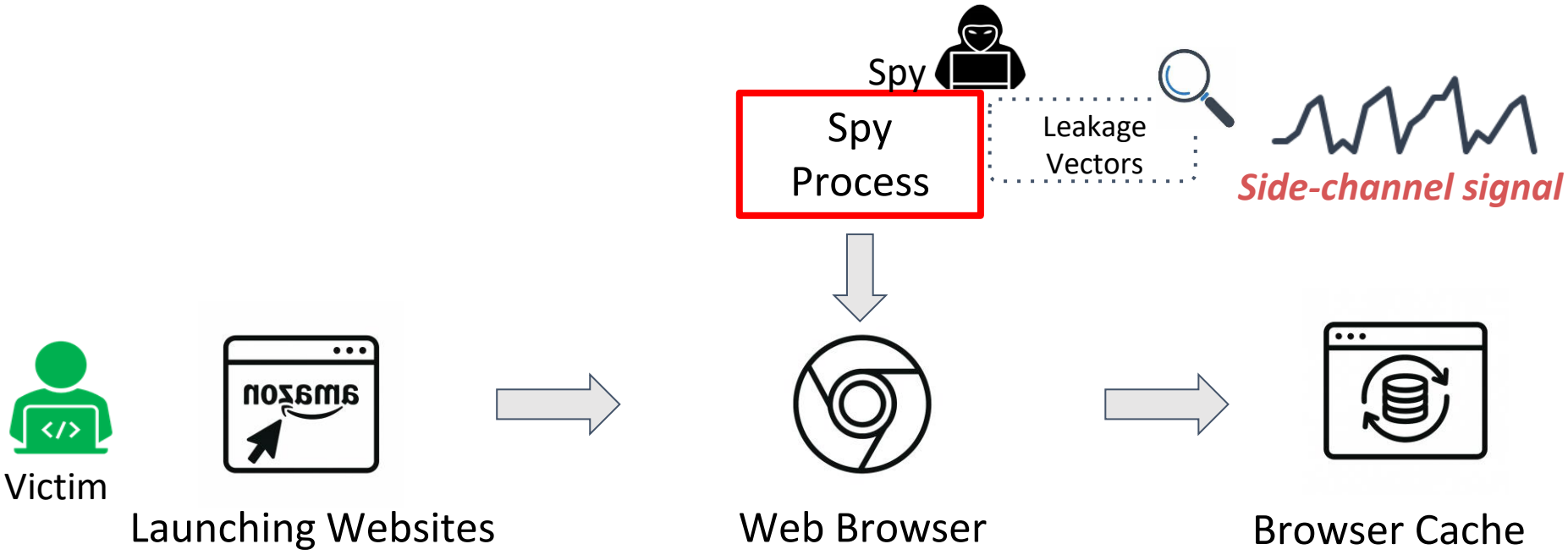
Attack 1: Web Fingerprinting

- **Victim:** Launching websites on a web browser.



Attack 1: Web Fingerprinting

- **Victim:** Launching websites on a web browser.
- **Spy:** Collecting side channel signal in the background.

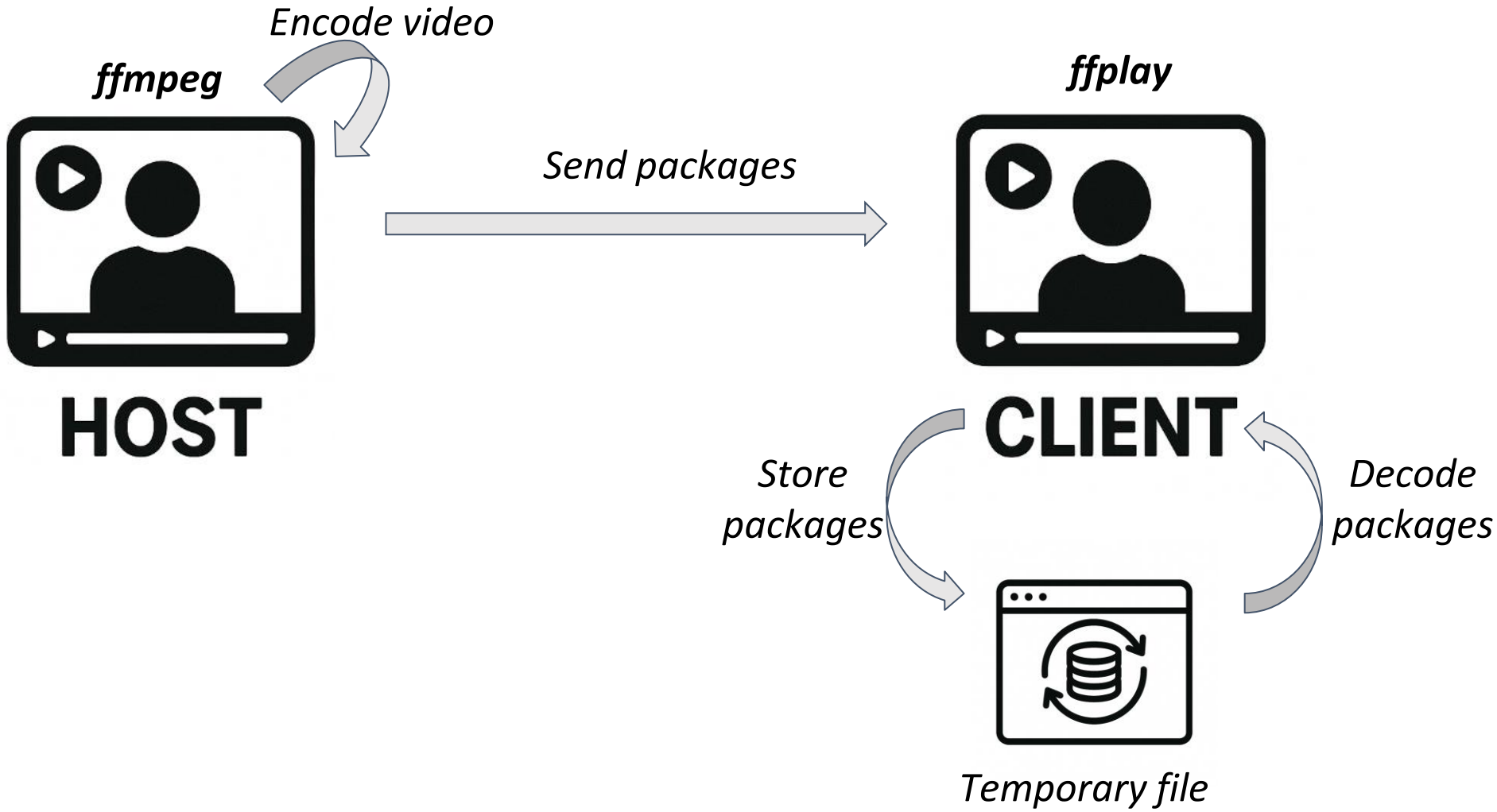


Classification Results

	F1	Precision	Recall
	$\mu(\sigma)$	$\mu(\sigma)$	$\mu(\sigma)$
Close world	93.82 (6.96)	94.99 (5.58)	93.77 (7.09)
Open world	93.25 (6.79)	94.67 (5.42)	93.25 (6.67)

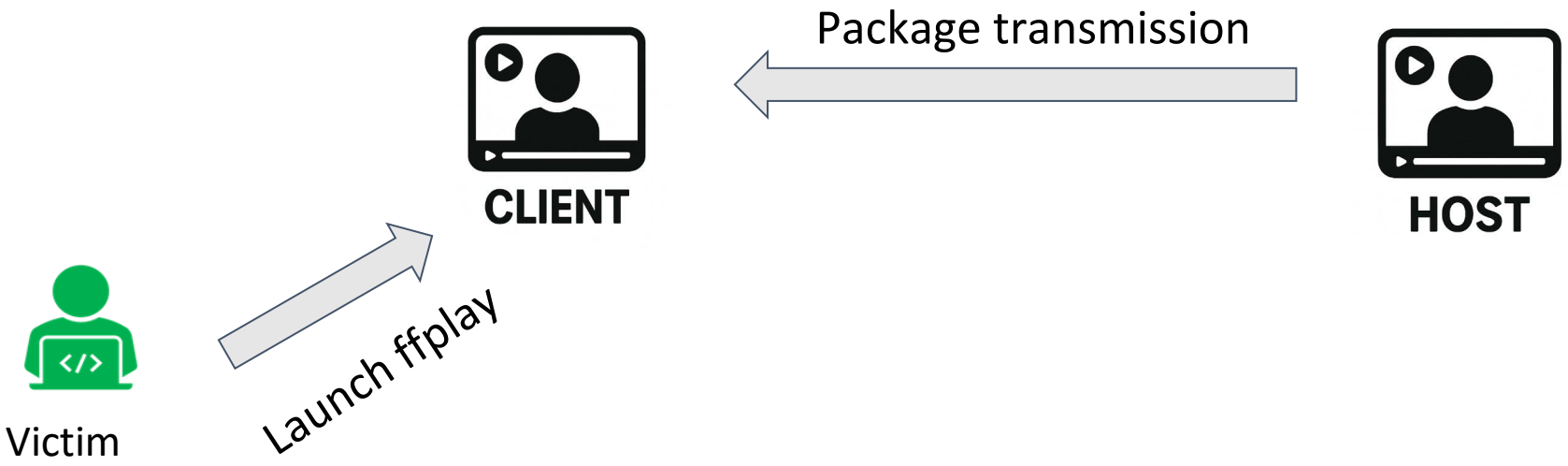
- Close world:
  - Top 100 websites.
- Open world:
  - Other class.

Attack 2: Voice Fingerprinting



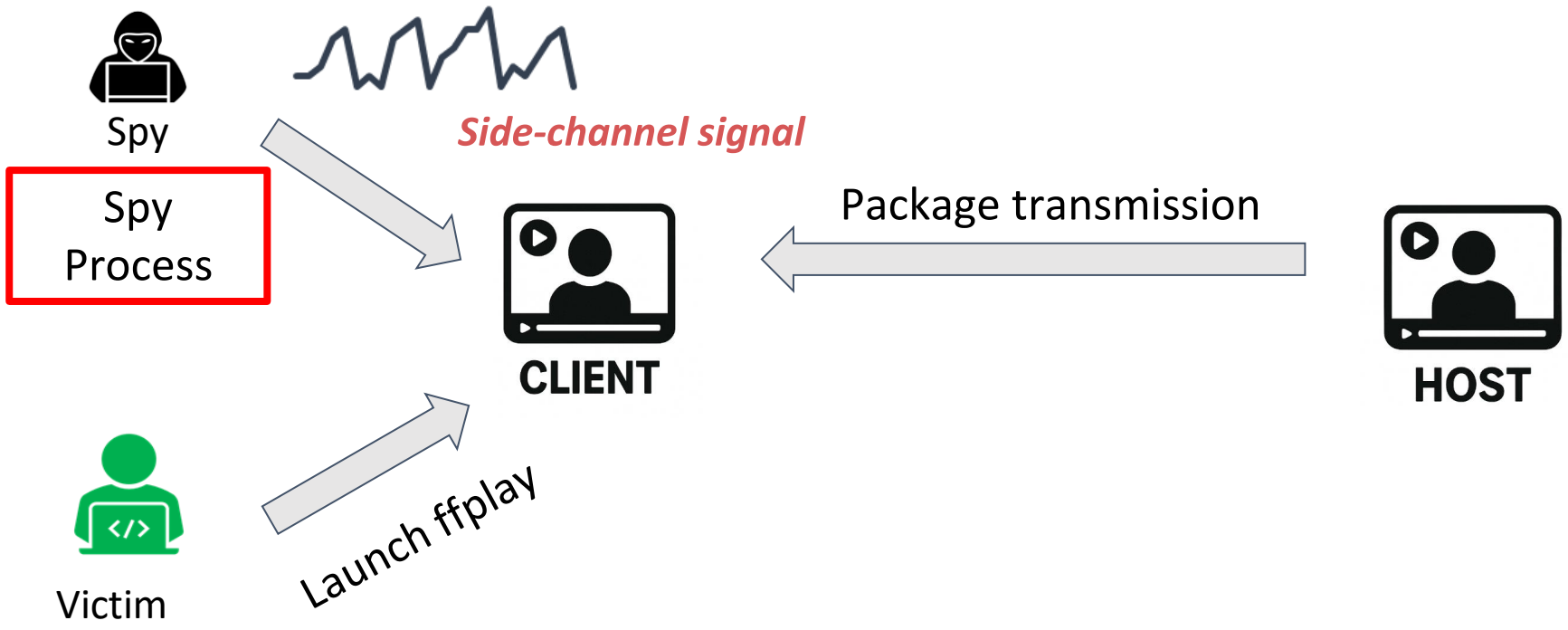
Attack 2: Voice Fingerprinting

- **Victim:** Running ffplay to watch videos.



Attack 2: Voice Fingerprinting

- **Victim:** Running ffplay to watch videos.
- **Spy:** Collecting side channel signal in the background.



Classification Results

- Two video platforms:
  - Youtube (F1 score of 92.74%).
  - Bilibili (F1 score of 87.03%).
- Open world/ close world set-up:
  - Top 20 videos.
  - Other class.

Conclusion

- New attack vector.
  - Leaking I/O operations via syncfs system call.
- Covert channel attack.
  - Bandwidth: 7.6 Kbps.
  - Error Rate: 1.9%.
- Side channel attack.
  - Web fingerprinting (F1 score of 93.25%).
  - Video fingerprinting (F1 score of 92.74% and 87.03%).

Thank you!

Any questions?