



PETS 2026

// OPEN-SOURCE VIDEO FINGERPRINTING DEFENSE • PETS 2026

Dodge: A Client-Side Framework for Application-Layer Video Fingerprinting Defenses



<https://dodge.video>
slides, paper & code

Ethan Witwer^{1,†} · David Hasselquist^{1,2} · Tobias Pulls³ · Niklas Carlsson¹

¹ Linköping University ² Sectra Communications ³ Karlstad University

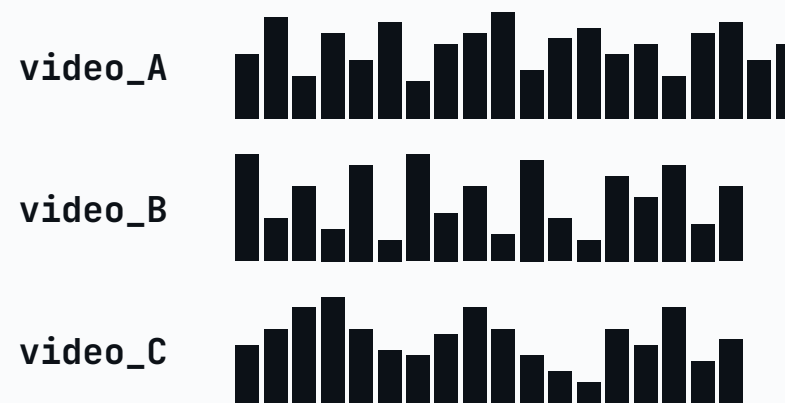
† PGP E568 6096 9240 F8B0 1376 690B 775C E981 B1FF 41DB

// THE THREAT

Encrypted video traffic leaks what you're watching.

- **Local, passive adversary** — a coffee shop neighbor, network admin, ISP, ...
- **Segment sizes are a fingerprint** — each title has a distinct size/timing pattern.
- **Encryption, VPNs & Tor don't help** — segment sizes and timing are still visible.

three titles · distinct identities



→ bytes hidden; size + timing still visible

// OUR SOLUTION

A defense **framework**, not a hard-coded defense.

hard-coded defense

Beaten by new attacks · switching means re-implementing · one strategy for every user group/use case.

dodge framework

A defense is a JSON **extended manifest** that uses simple building blocks. New defense = new file, no new code.

- **Cycles** — a generalized model of DASH streaming: every request is a full, partial, or padding cycle.
- **Minimal interface** — just give the player an extended manifest URL instead of a DASH MPD to stream.

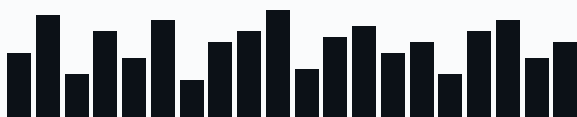
// GENERALIZED STREAMING: CYCLES

Shape segment delivery on the **client side**.

segments → cycles

shape ≠ identity

in: real



→ apply defense →

out: shaped



a defense is just a file

```
// sample extended manifest
{
  "base_uri": "https://ex.com/seg/",
  "streams": [{ "label": "video_1000k",
    "data": [
      { "index":0, "range":"-43999" },
      { "index":0, "range":"16000-", "buffer":true },
      { "index":1, "range":"-43999", "padding":true }
    ] }]
}
```

// PROOF-OF-CONCEPT DEFENSE

Dodge-mimic: make videos look identical.

- **k-anonymity** — make every video in a set have the same cycles.
- **Provable bound** — attacker accuracy should be $\leq 100/k\%$ ($k = 10 \Rightarrow \leq 10\%$).
- **Tunable** — k controls the trade-off between protection, overhead, and QoE.

one set ($k = 3$) • same representation

video_A 

video_B 

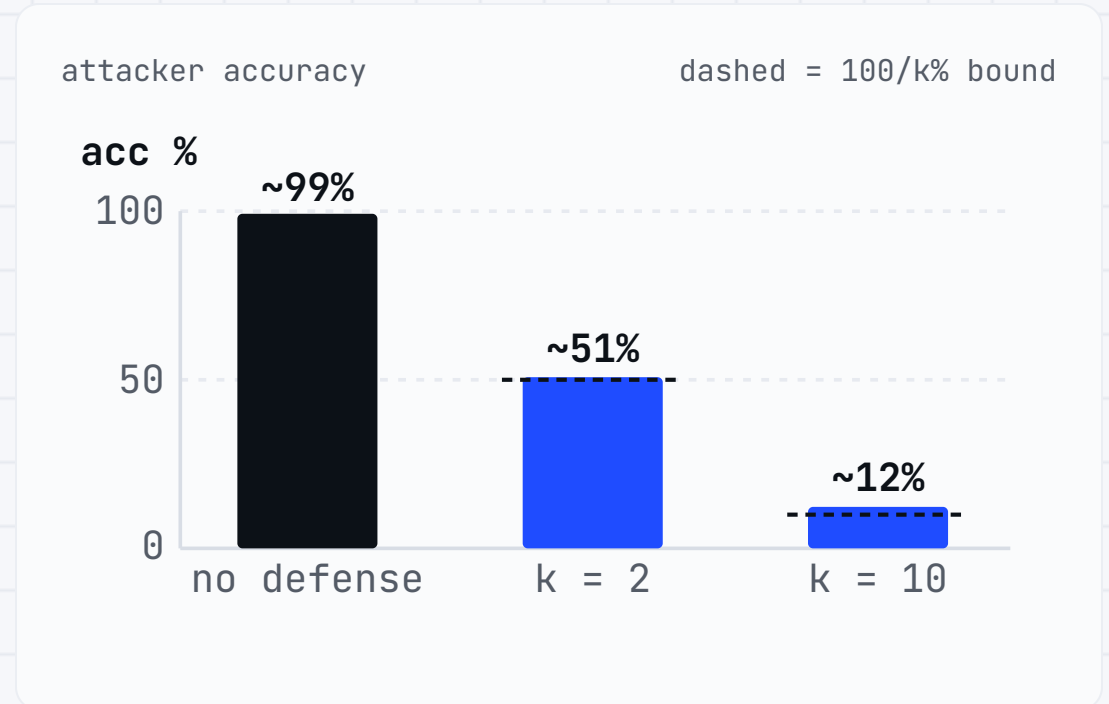
video_C 

■ same shape for every video $\Rightarrow$ indistinguishable

// TESTING RESULTS

Near theoretical bounds, moderate cost.

- **Accuracy at the bound** — avoidable leakage removed $\Rightarrow$ $\sim 100/k\%$ accuracy.
- **Moderate overhead** — $\sim 21\%$ ($k = 2$) to $\sim 73\%$ ($k = 10$) bandwidth overhead.
- **Smooth playback** — negligible QoE hit; start-up delay & stalls are small.



// DEPLOYMENT STEPS

Swap 2 JavaScript files. No server changes.

dash.js

→
replace one JS file, add one

Dodge

- **Opt-in dash.js module** — the DASH reference player, already deployed across the web.
- **No special infrastructure** — no server-side changes, no re-encoding, no new dependencies.
- **Host manifests anywhere** — on the video server, a trusted server, or locally.

// DEPLOYMENT STATUS

Soon an official part of dash.js!

To be merged in dash.js v5.3.0, August 2026.

Dodge is soon to be a part of the official DASH reference player used by major content providers. We're also releasing a browser extension on dodge.video (it should be out in a few days).

// TAKEAWAYS

Effective video fingerprinting defense that's deployable today.

- **Threat** — encrypted segment sizes can be used to fingerprint videos.
- **Framework** — defenses are just extended manifest files, not hard-coded.
- **Dodge-mimic** — shows Dodge's potential to remove information leakage while maintaining modest overhead and a good user experience.
- **Deployable** — opt-in dash.js module, available now and soon to be merged in v5.3.0; can also be run via the browser extension.



<https://dodge.video>

slides · paper · code

Come talk at the **poster!**