galois

BALBOA

Bobbing and Weaving around Network Censorship

Marc B. Rosen, James Parker, Alex J. Malozemoff

This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA).

The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

56%

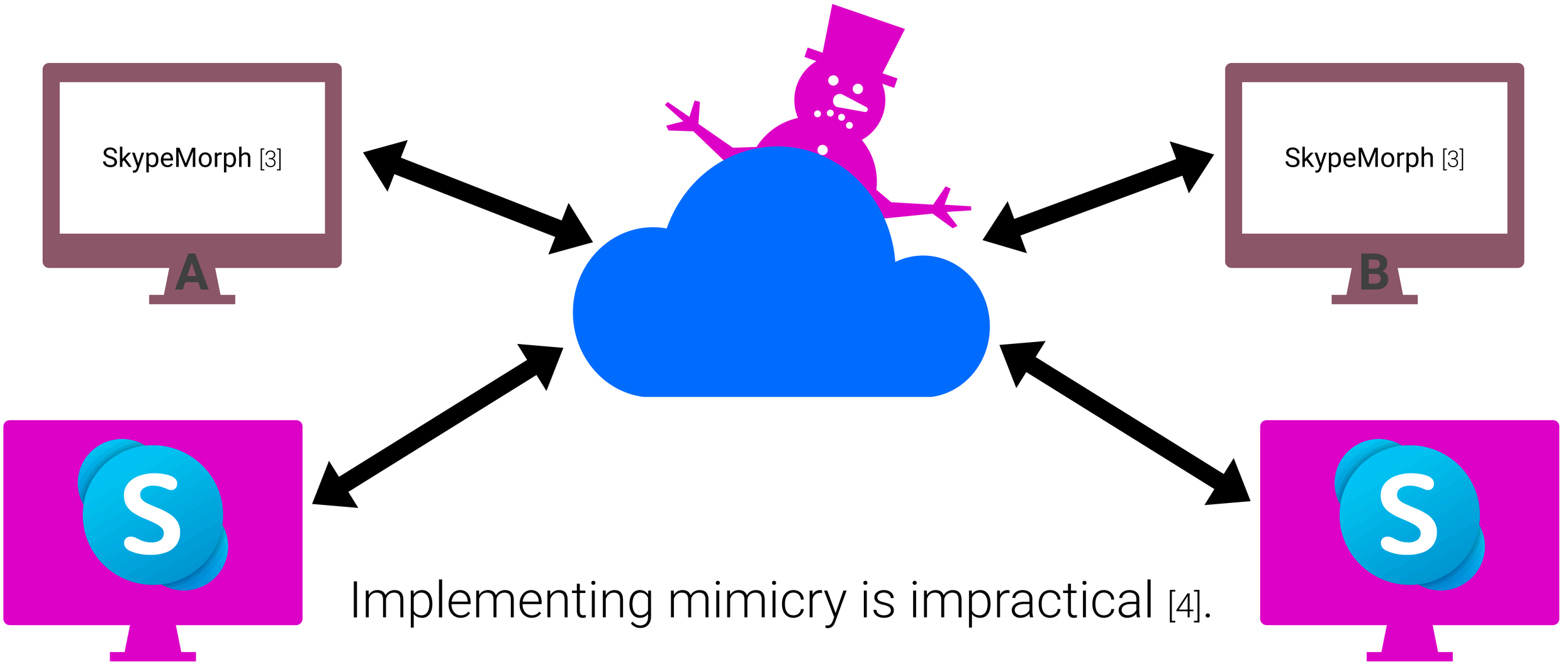
of global internet users “live in countries where political, social, or religious content was blocked online.” [1]

Link Obfuscation

Look-Like Something

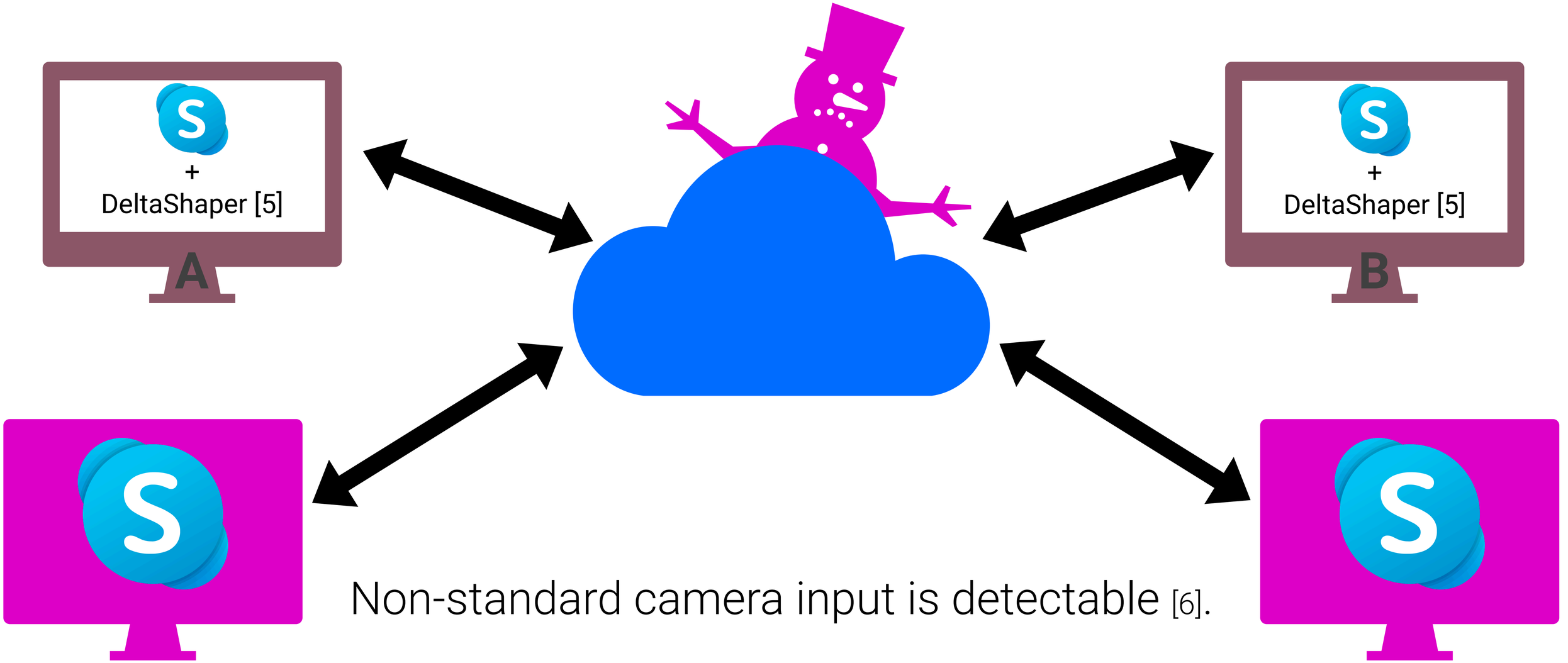
Encryption doesn’t hide metadata [2].

Mimicry



Implementing mimicry is impractical [4].

Tunneling



Non-standard camera input is detectable [6].

To be indistinguishable to the censor, we want to…

(1) run a standard instance of a target application,

(2) with a standard input,

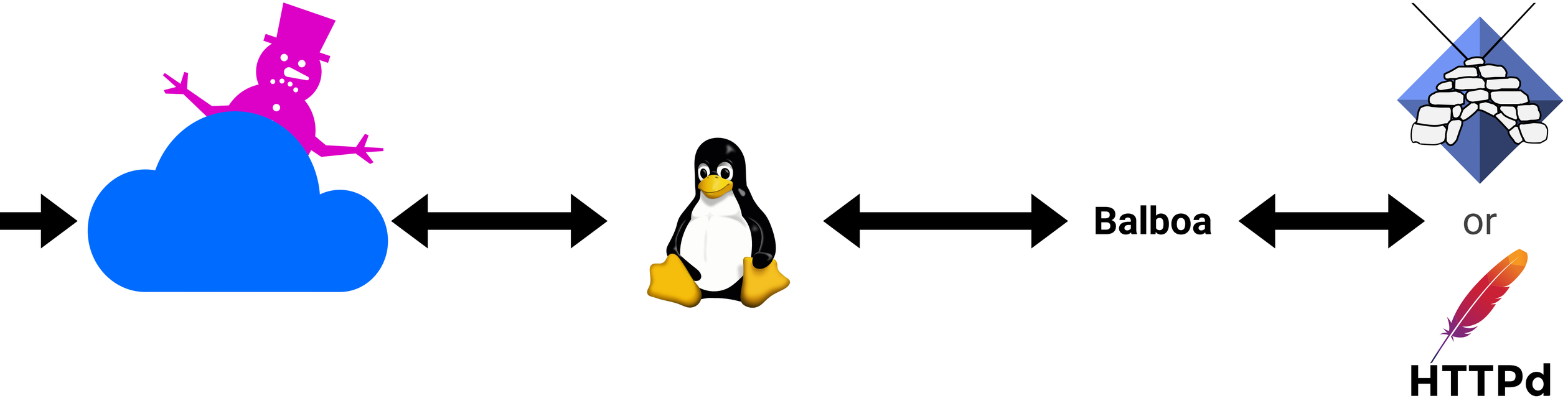
(3) while embedding data into the stream

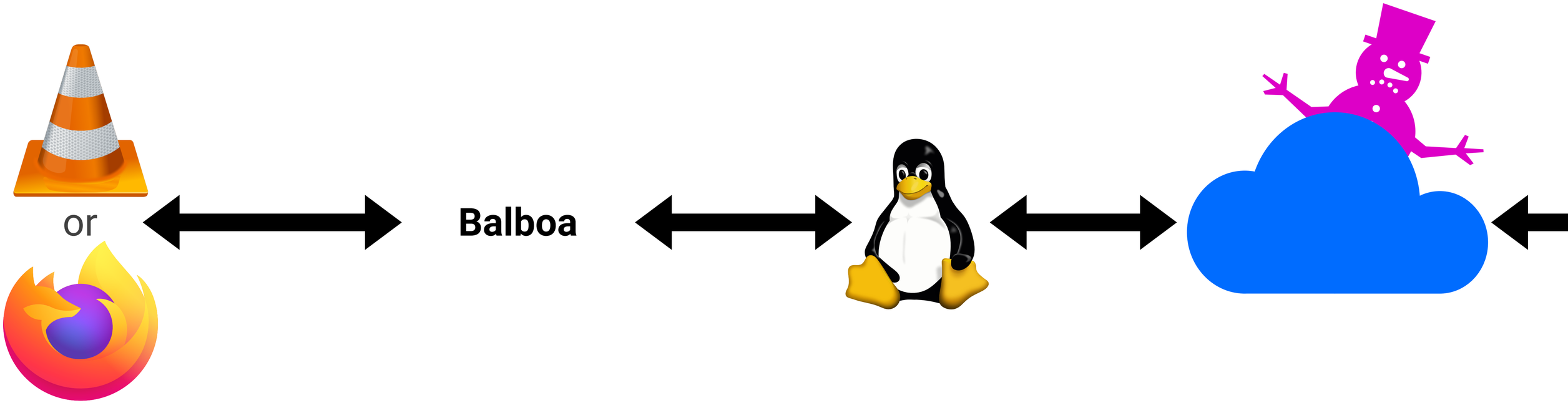
Balboa is a framework which…

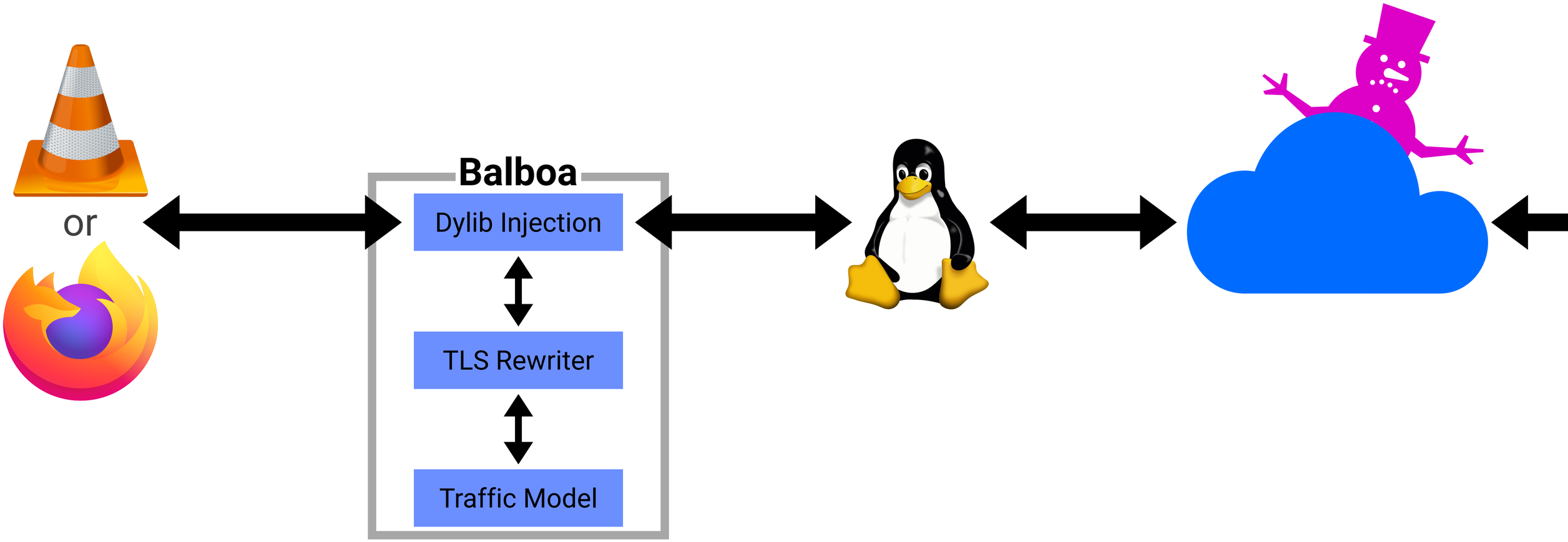
(1) runs an *unmodified* binary of a TLS-enabled target application,

(2) on its standard input,

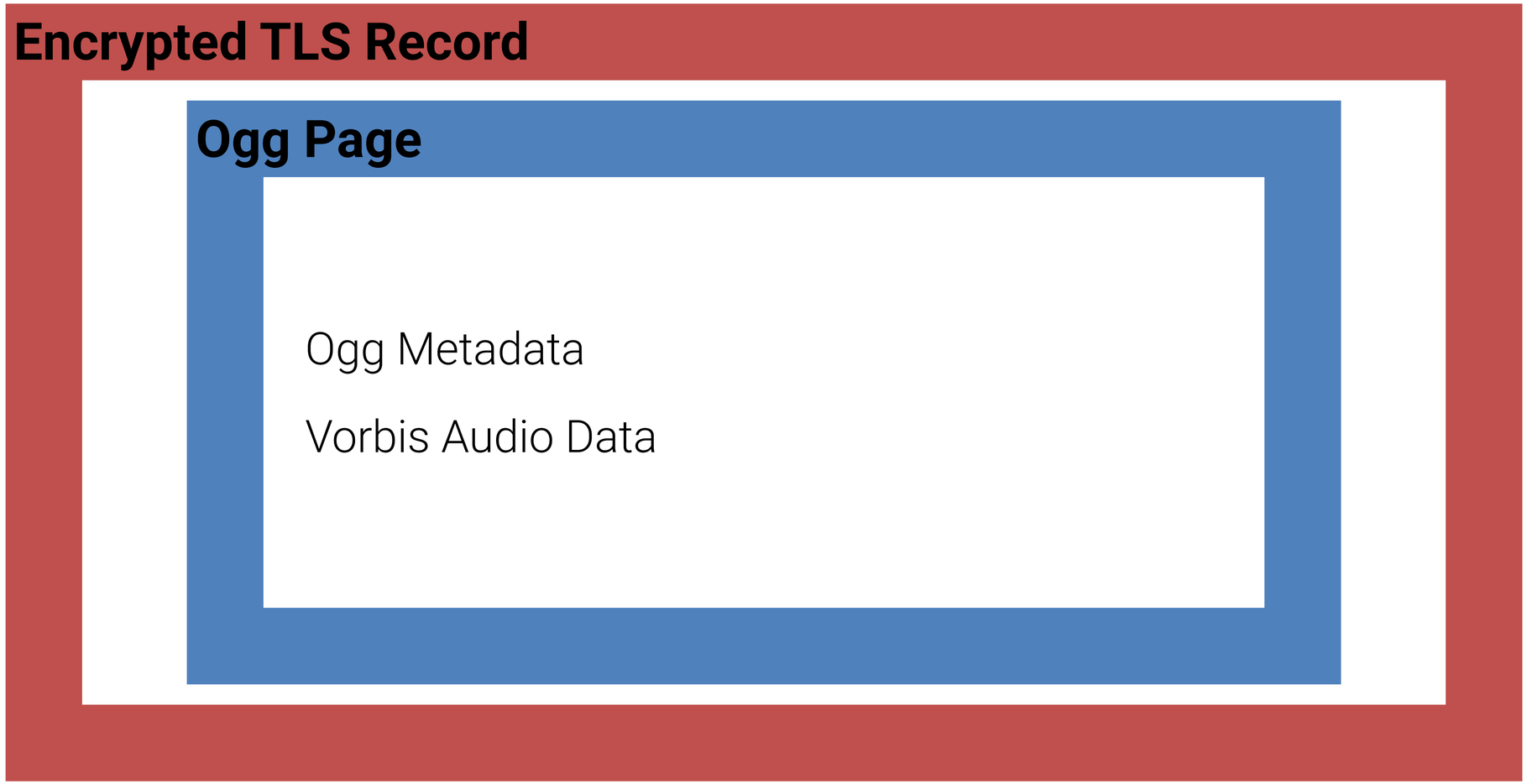
(3) while manipulating its TCP stream to embed/extract covert data

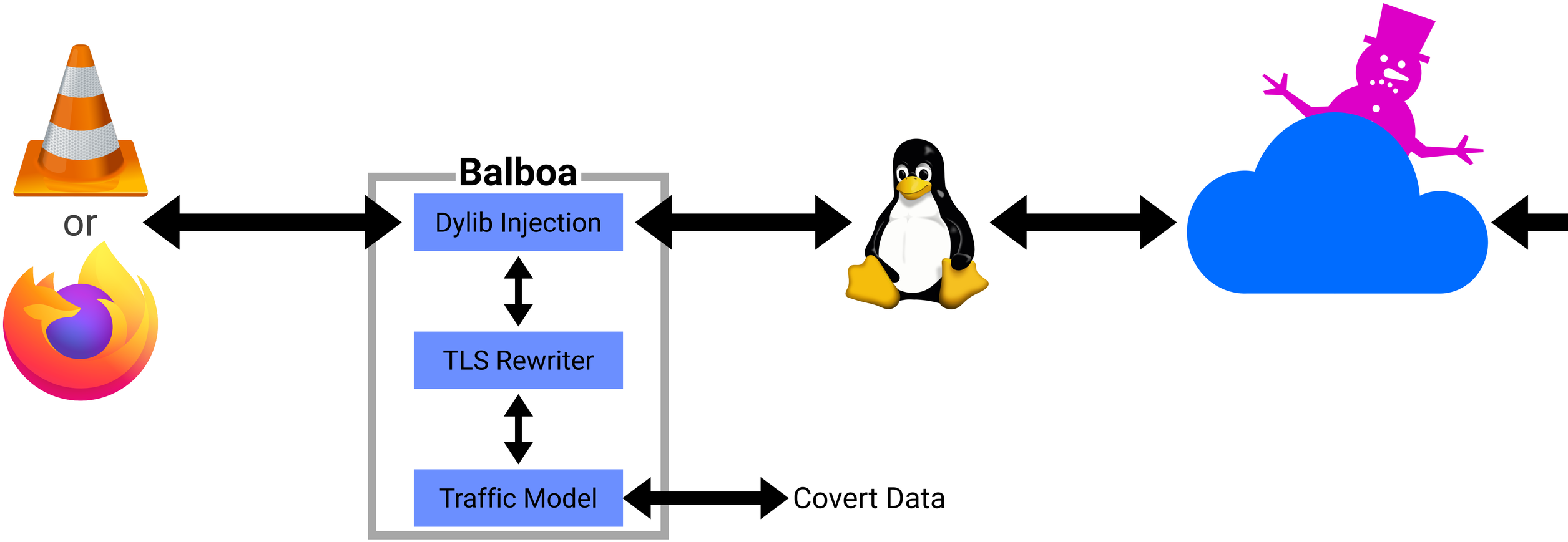






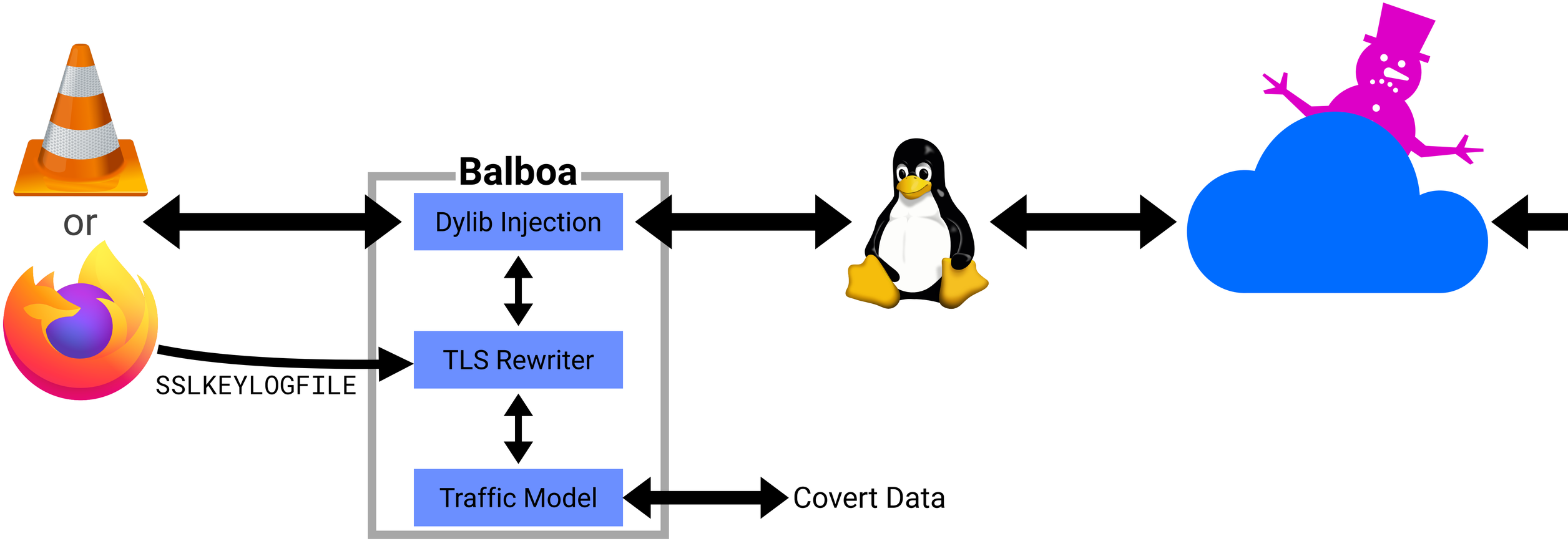
Traffic Model: Internet Radio

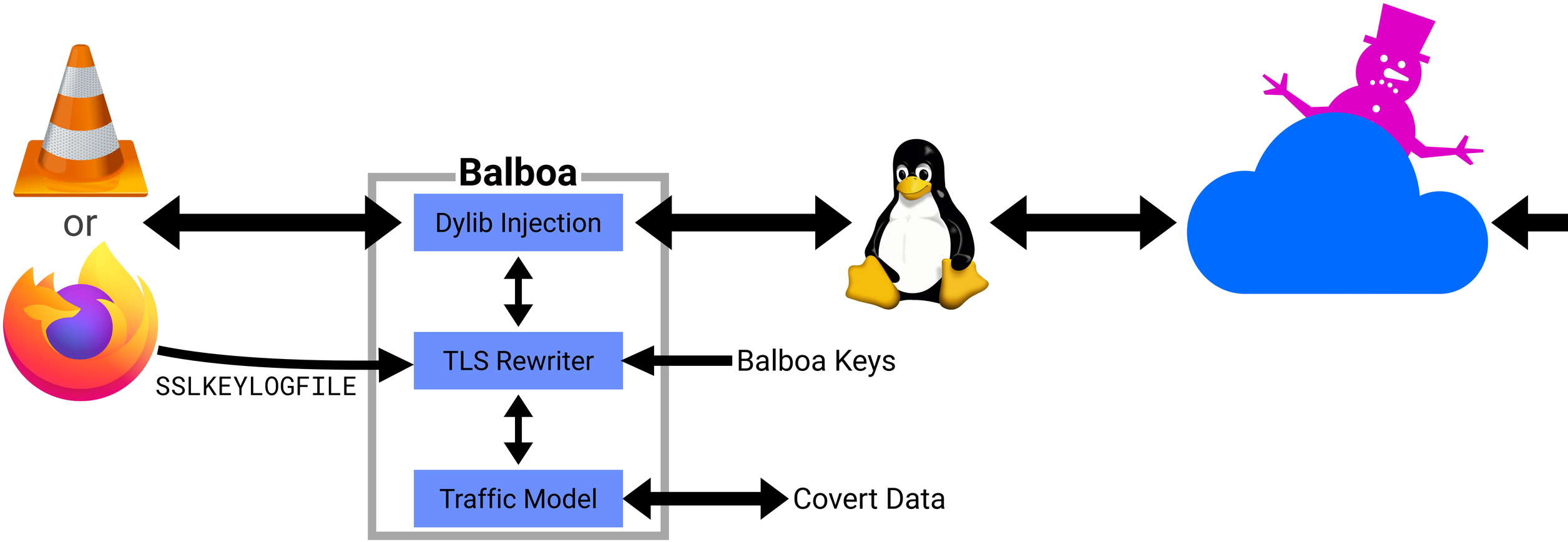




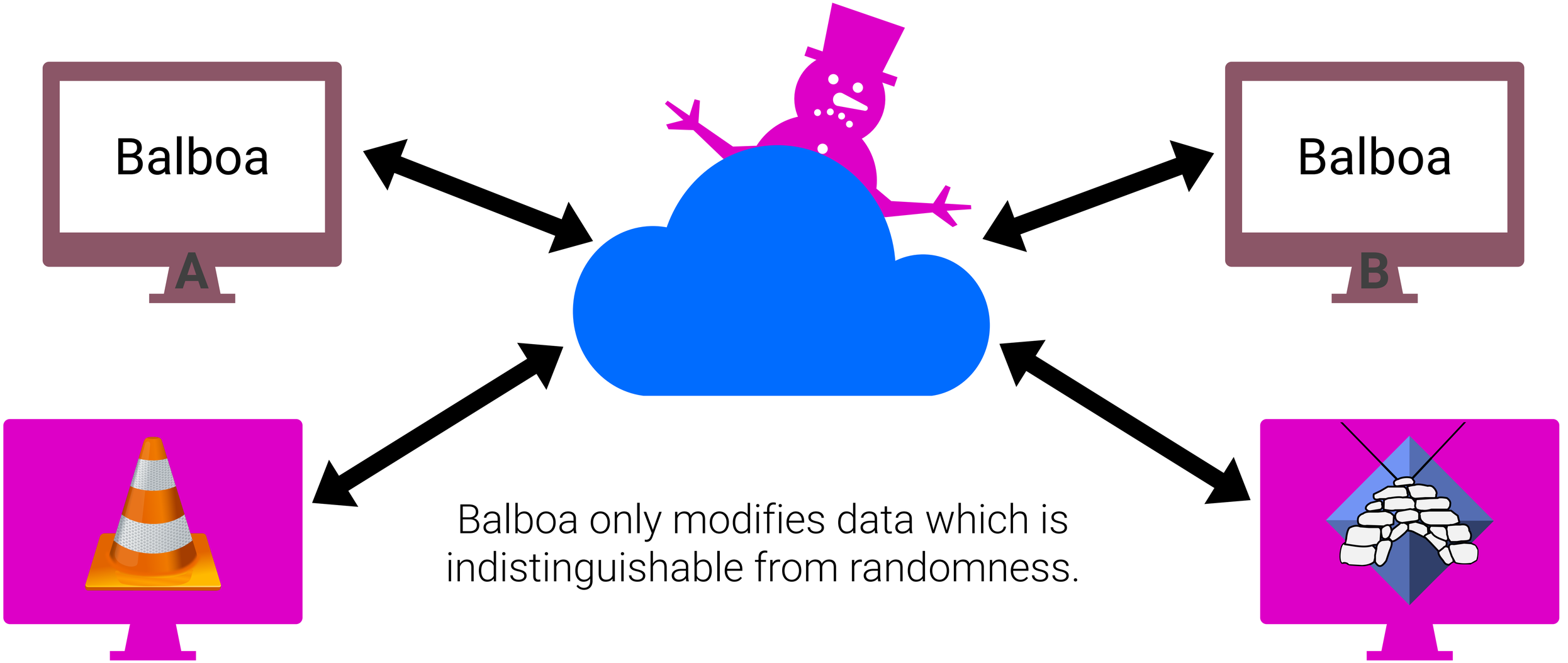
Dynamic Library Injection

```
connect(client_fd, ip, port)

write(client_fd, buffer, len) → bytes_written

read(client_fd, buffer, len) → bytes_read
```





Security Evaluation



Evaluation: Internet Radio

	VLC	MPlayer	MPV	Audacious
Accuracy with 5ms ± 1ms latency	0.72 ± 0.08	0.50 ± 0.10	0.53 ± 0.09	0.73 ± 0.06
Accuracy with 10ms ± 1ms latency	0.67 ± 0.09	0.55 ± 0.10	0.55 ± 0.09	0.68 ± 0.06

Evaluation: Web Browsing

	Firefox	Curl
Scenario	Browsing Wikipedia	File Download
Accuracy with 5ms ± 1ms latency	0.69 ± 0.01	0.71 ± 0.08
Accuracy with 10ms ± 1ms latency	0.66 ± 0.01	0.79 ± 0.08

BALBOA

Bobbing and Weaving around Network Censorship

Marc B. Rosen, James Parker, Alex J. Malozemoff

Questions? Email us! balboa@galois.com

https://github.com/GaloisInc/balboa
https://github.com/GaloisInc/stallone

Citations

1. https://freedomhouse.org/sites/default/files/2020-10/10122020_FOTN2020_Complete_Report_FINAL.pdf
2. Charles V. Wright, Lucas Ballard, Scott E. Coull, Fabian Monrose, and Gerald M. Masson. Uncovering spoken phrases in encrypted voice over IP conversations. *ACM Transactions on Information and System Security (TIS- SEC)*, 13(4):1–30, 2010.
3. Hooman Mohajeri Moghaddam, Baiyu Li, Mohammad Derakhshani, and Ian Goldberg. Skypemorph: Protocol obfuscation for tor bridges. In *Proceedings of the 2012 ACM conference on Computer and communications se- curity*, pages 97–108, 2012.
4. Amir Houmansadr, Chad Brubaker, and Vitaly Shmatikov. The parrot is dead: Observing unobservable network communications. In *Symposium on Security & Privacy*. IEEE, 2013.
5. Diogo Barradas, Nuno Santos, and Luís Rodrigues. DeltaShaper: Enabling unobservable censorship-resistant TCP tunneling over videoconferencing streams. *Privacy Enhancing Technologies*, 2017(4):1–18, 2017.
6. Diogo Barradas, Nuno Santos, and Luís Rodrigues. Effective detection of multimedia protocol tunneling using machine learning. In *USENIX Security Symposium*. USENIX, 2018.