RED HAT SUMMIT

BOSTON, MA
JUNE 23-26, 2015

Container Security

Kurt Seifried
Software Engineer

June 2015

What this talk is not

This talk is not about Docker security

- If you want to learn about Docker security go listen to Daniel Walsh =)

What this talk is

Securing apps and other shenanigans

- Reading PDFs (Adobe Reader has 400+ CVEs)
- Web browsing (Firefox has 1300+ CVEs)
- Web browsing privately (Panopticlick)
- SSL/TLS MitM testing (total pain to setup)

Reading PDFs
(and other scary file formats)

Reading PDFs

- Reduce the attack surface
- Remove network “--net=none”
  - using X to display still works
- Blow the system away once done
  - Be careful of any volume mounts

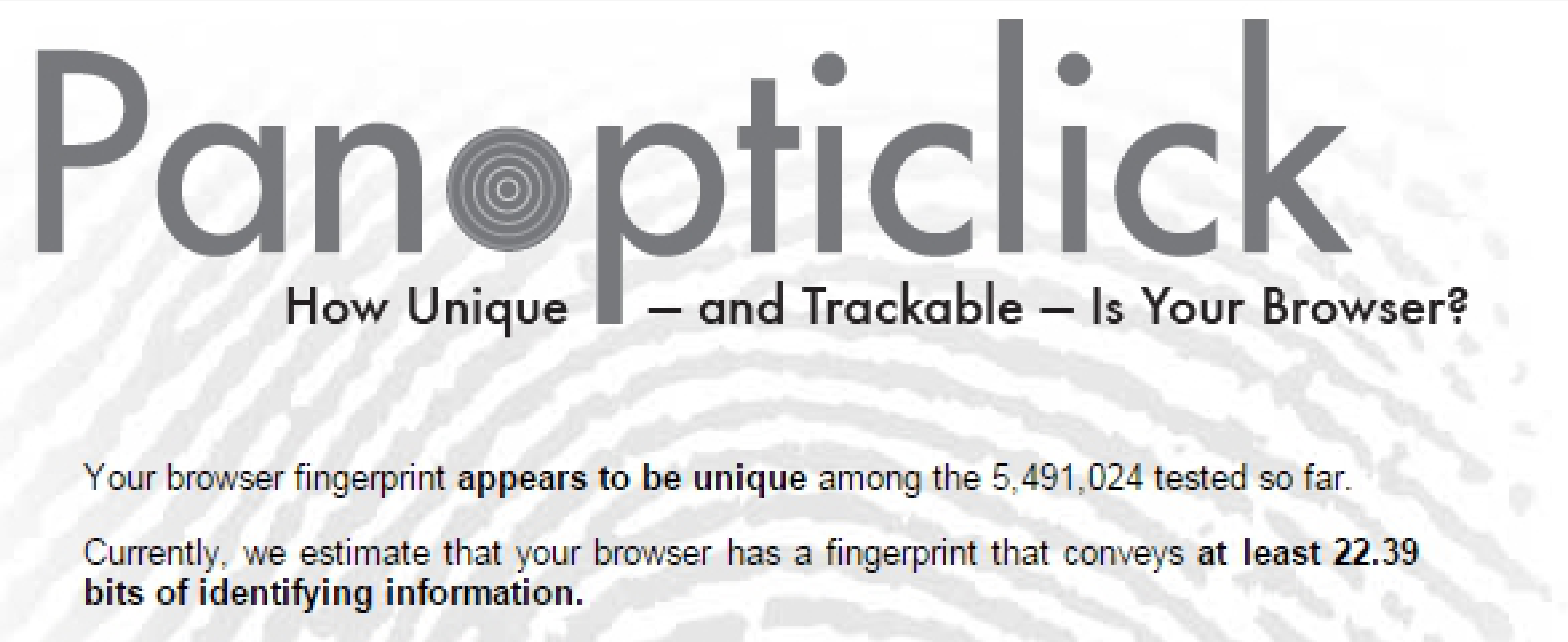
Web browsing

Web browsing

- Use volume mounts for .mozilla
  - -v /home/user/.mozilla2/:/home/user/.mozilla/
  - find ./mozilla* -type f -name “*.sqlite” -exec sh -c 'sqlite3 {} .dump > {}.dump' \;
  - diff the all files and voila, that's what changed

Web browsing privately

Web browser tracking



Panopticlick

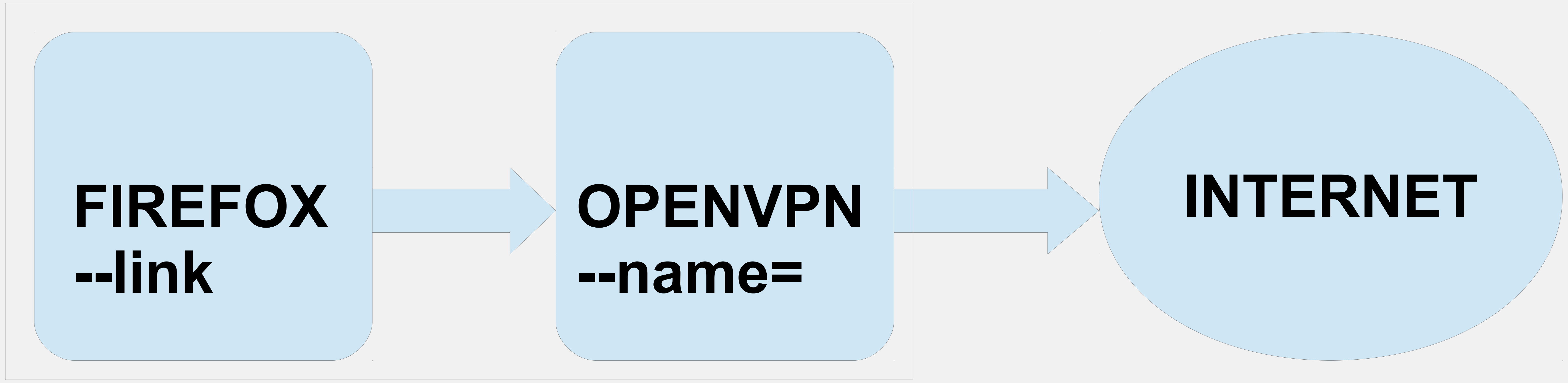
How Unique – and Trackable – Is Your Browser?

Your browser fingerprint **appears to be unique** among the 5,491,024 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 22.39 bits of identifying information.**

So....

- Browse through VPN, so no leaks (DNS, X-Forwarded-For, etc.)
- Use --name and –link or pass env variables
- Reset default gw on firefox and:



SSL/TLS MitM Testing

Setting up for testing is a PITA

- You need a client, a MitM host and the server, you need routing, etc.
- So 3 VMs or 3 docker files... guess which fits in an email?

Questions?

RED HAT SUMMIT

LEARN. NETWORK.
EXPERIENCE OPEN SOURCE.