TRUESEC

Your Clocks Have Ears!

Timing-Based Browser-Based Local Network Port Scanner

Dongsung "Donny" Kim

TRUESEC

About Me

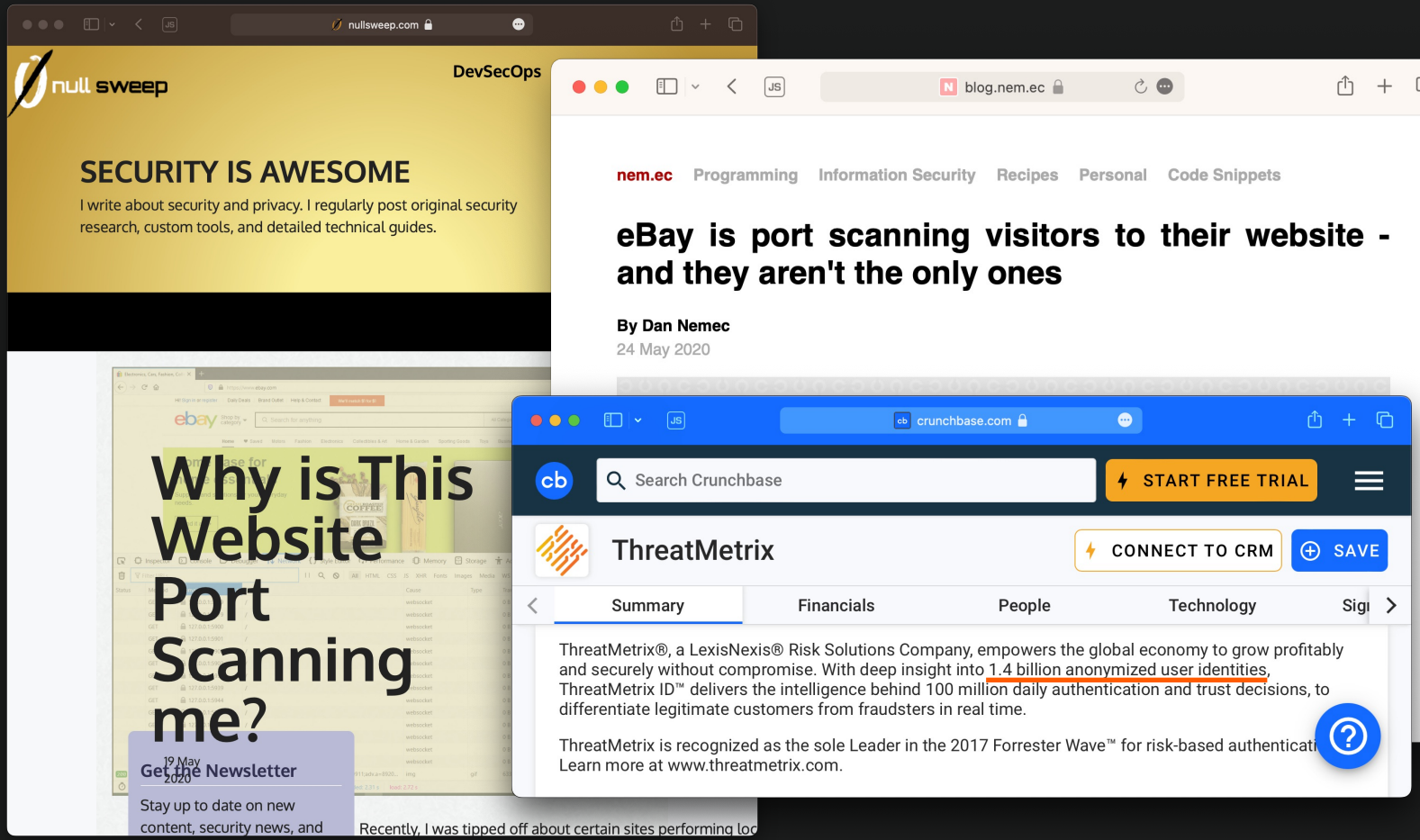


Surname

- Dongsung "Donny" Kim
- IT-Security Expert @ Security Office
- Twitter `@kid1ng`
- Bluesky `@kidi.ng`
- Discord `kiding`
- Website `kidi.ng`

Security Office

- Based in Sweden and South Korea
- Part of the Truesec Group
- `https://security-office.co.kr`


nullsweep.com
null sweep
DevSecOps
SECURITY IS AWESOME
I write about security and privacy. I regularly post original security research, custom tools, and detailed technical guides.
Why is This Website Port Scanning me?
19 May 2020
Get the Newsletter
Stay up to date on new content, security news, and
Recently, I was tipped off about certain sites performing loc
blog.nem.ec
nem.ec
Programming
Information Security
Recipes
Personal
Code Snippets
eBay is port scanning visitors to their website - and they aren't the only ones
By Dan Nemec
24 May 2020
crunchbase.com
Search Crunchbase
START FREE TRIAL
ThreatMetrix
CONNECT TO CRM
SAVE
Summary
Financials
People
Technology
ThreatMetrix®, a LexisNexis® Risk Solutions Company, empowers the global economy to grow profitably and securely without compromise. With deep insight into 1.4 billion anonymized user identities, ThreatMetrix ID™ delivers the intelligence behind 100 million daily authentication and trust decisions, to differentiate legitimate customers from fraudsters in real time.
ThreatMetrix is recognized as the sole Leader in the 2017 Forrester Wave™ for risk-based authenticati
Learn more at www.threatmetrix.com.

TRUESEC

Browser-Based Port Scanning

- Privacy implication: fingerprinting visitors
  - Tracking with characteristics unique to each user, browser, hardware setup
- Security implication: uncovering intranet services
  - A foothold for XSS, CSRF

Previous Works

- <img>, <iframe>, <script>, WebRTC, WebSocket
- Browsers mitigated them to some extent



SPI Labs, “Detecting, Analyzing, and Exploiting Intranet Applications using JavaScript”
Flu1dTeam, “PortScanner”
Jacob Baines, “Using WebRTC ICE Servers for Port Scanning in Chrome”
Nikolai Tschacher, “Browser based Port Scanning with JavaScript”
Adam Rice, “WebSocket Throttling Design”

TRUESEC

Timing Measurement on Fetch

```
async function measure(ip, port, timeout, https) {
  const ctrl = new AbortController();
  const timer = setTimeout(() => ctrl.abort(), timeout / 1_000);

  let t0 = performance.now();
  try {
    await fetch(
      `http${https ? 's' : ''}://${ip}:${port}`,
      { signal: ctrl.signal }
    );
  } catch (e) {
  } finally {
    let t1 = performance.now();
    clearTimeout(timer);

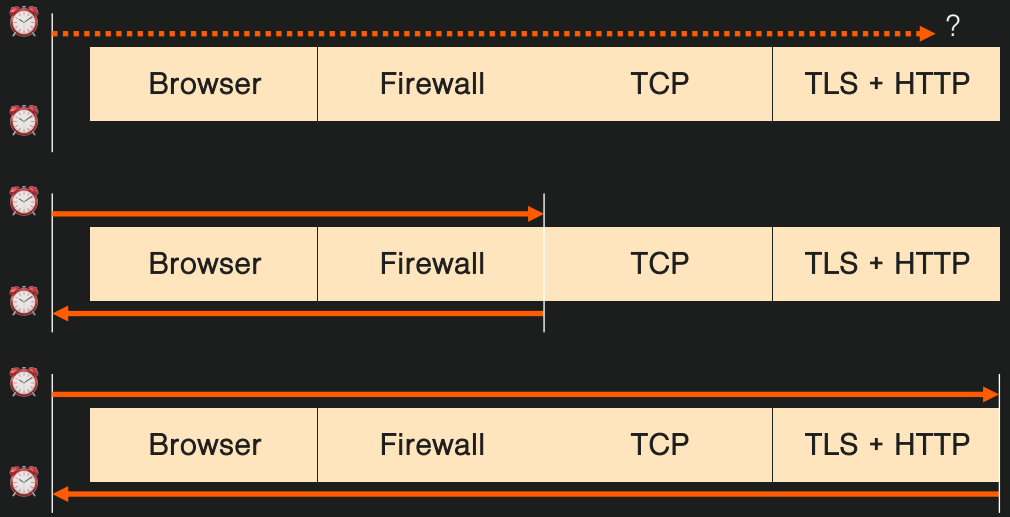
    const elapsed = (t1 - t0) * 1_000;
    return elapsed;
  }
}
```

- We can observe:
  - Elapsed time of a fetch request
- We cannot observe:
  - Response data
  - Request data
    - Other than scheme, ip, port
  - Error data
    - Other than "TypeError: Failed to fetch"

TRUESEC

States and Hypotheses

- If port is closed and firewall drops packets, or host is unreachable:
- If port is closed and firewall rejects packets:
- If port is open and a process is listening:



➥ Distinct timing differences
depending on the state of a port

TRUESEC

Three Techniques

Finding Open Ports on the Localhost

1

Finding the Router

2

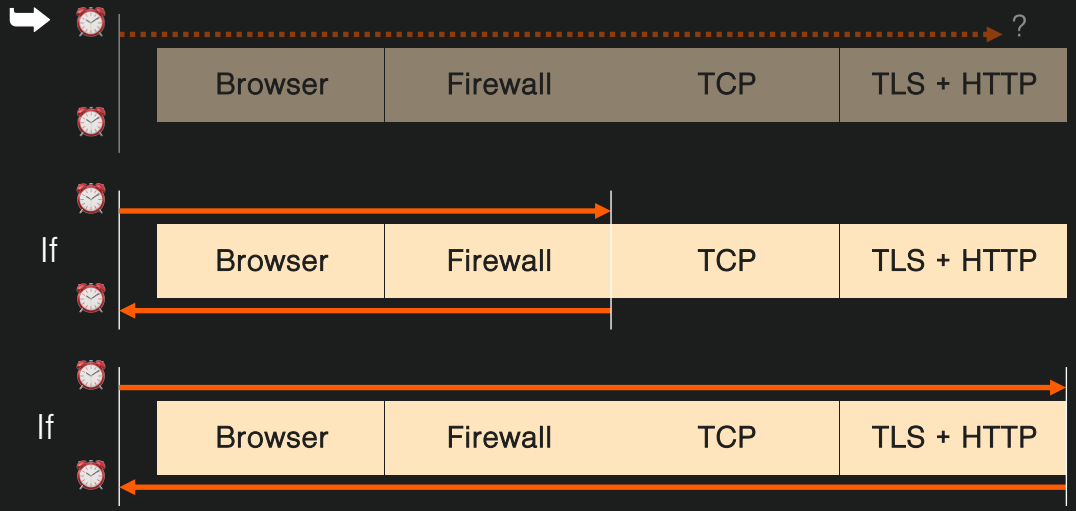
Finding Open Ports on the LAN Clients

3

TRUESEC

Observations and States

- Firewall always rejects packets when port is closed*
- Host is always reachable



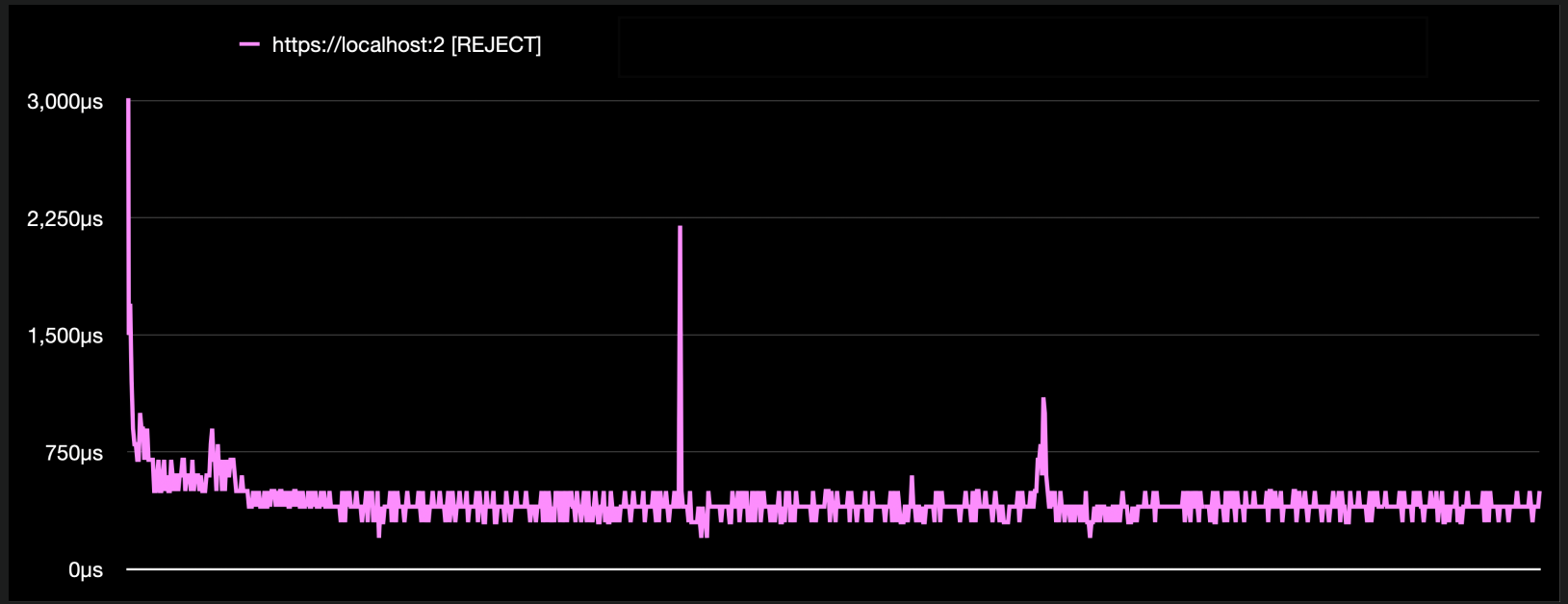
- ~~Port is closed and firewall drops packets, or host is unreachable:~~
- Port is closed and firewall rejects packets
- Port is open and a process is listening

* On Windows: Firewall always drops packets when port is closed

TRUESEC

Algorithm

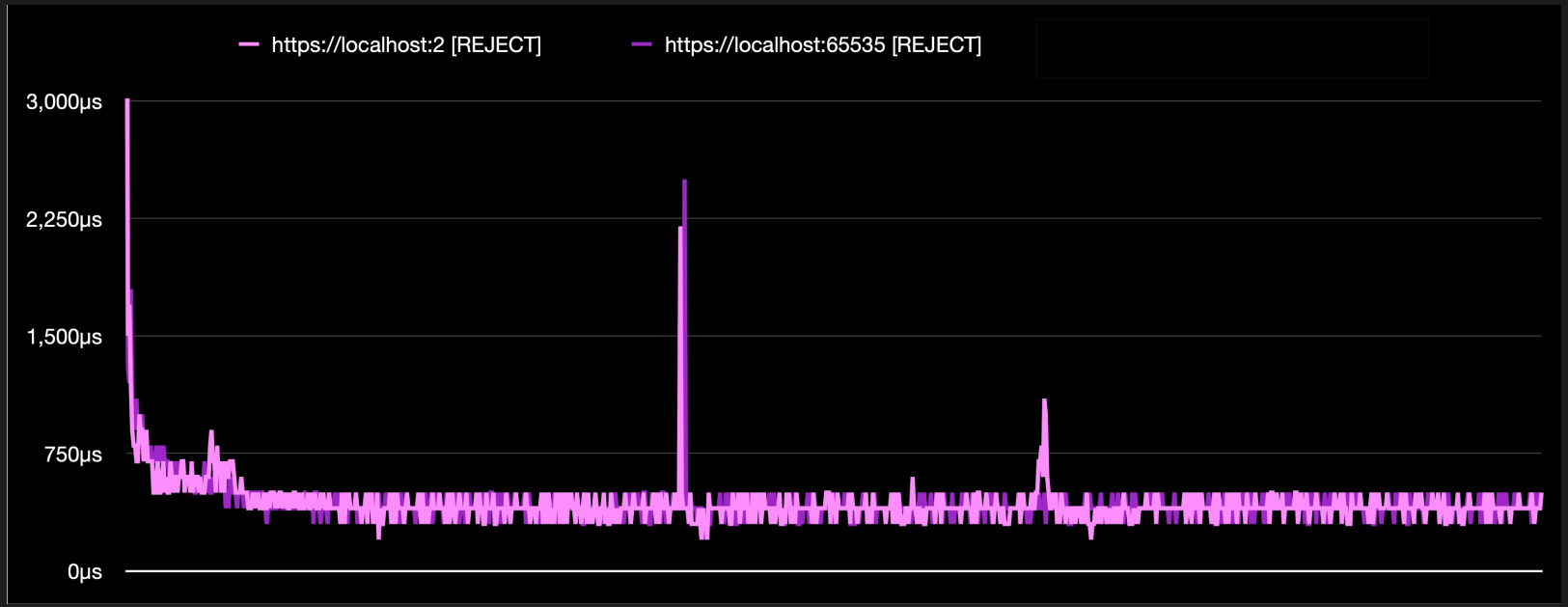
1. Make multiple fetches to localhost:2, a port that is generally closed, and calculate the average timing as a control



TRUESEC

Algorithm

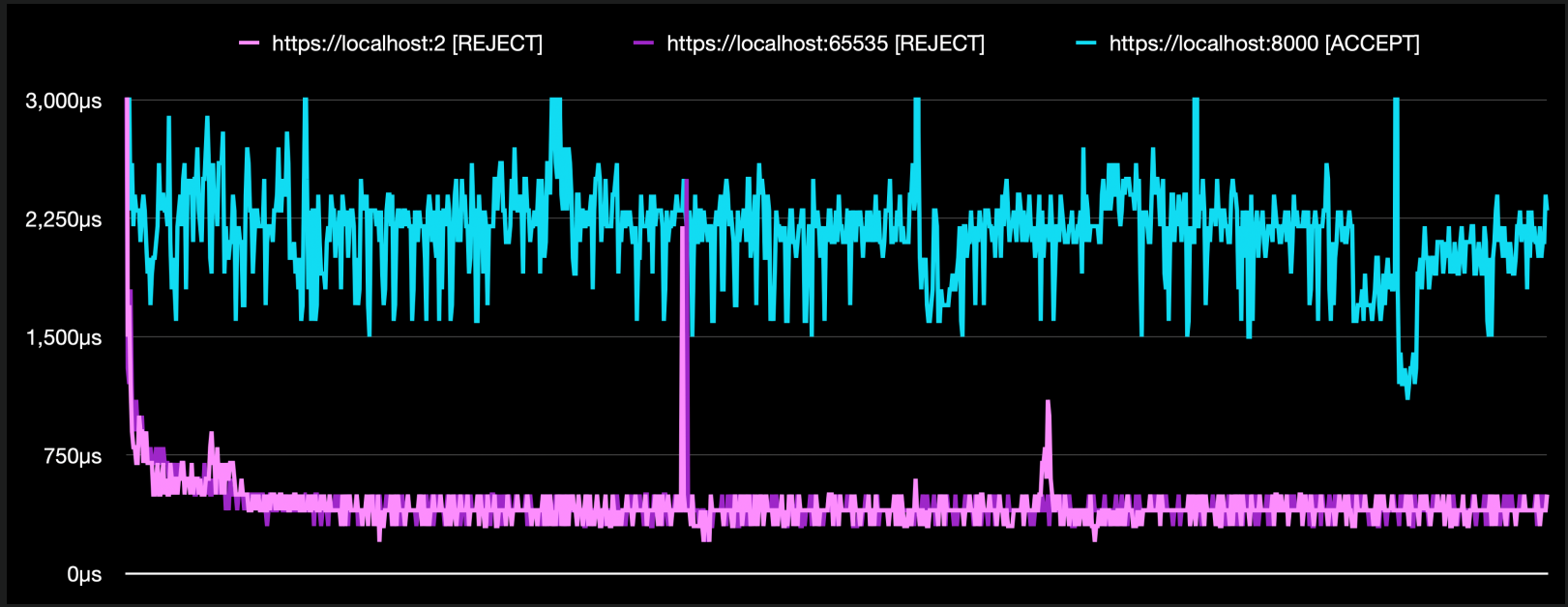
2. If a fetch takes a similar time as the control, the port is closed



TRUESEC

Algorithm

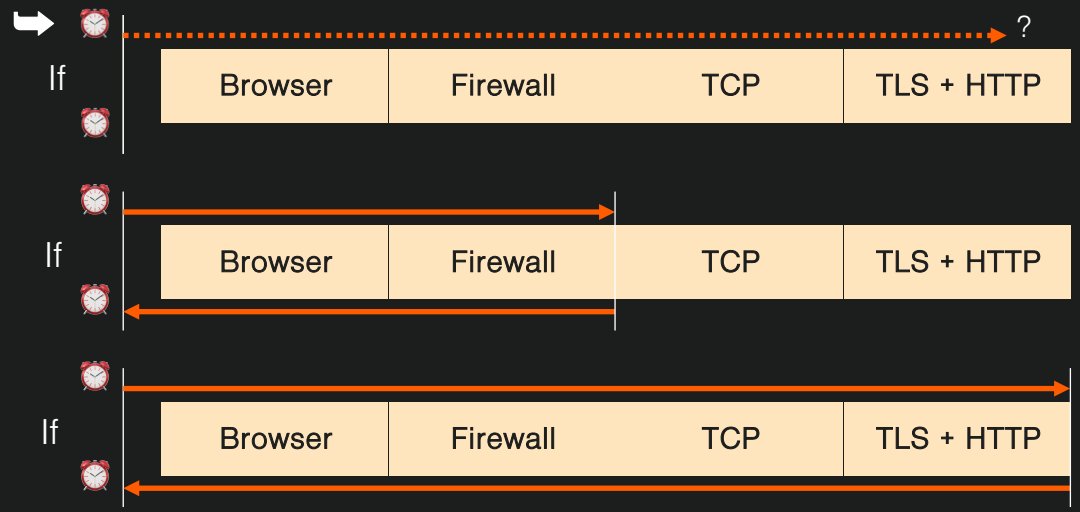
2. If a fetch takes a similar time as the control, the port is closed
3. If a fetch takes significantly more time than the control, the port is open



TRUESEC

Observations and States

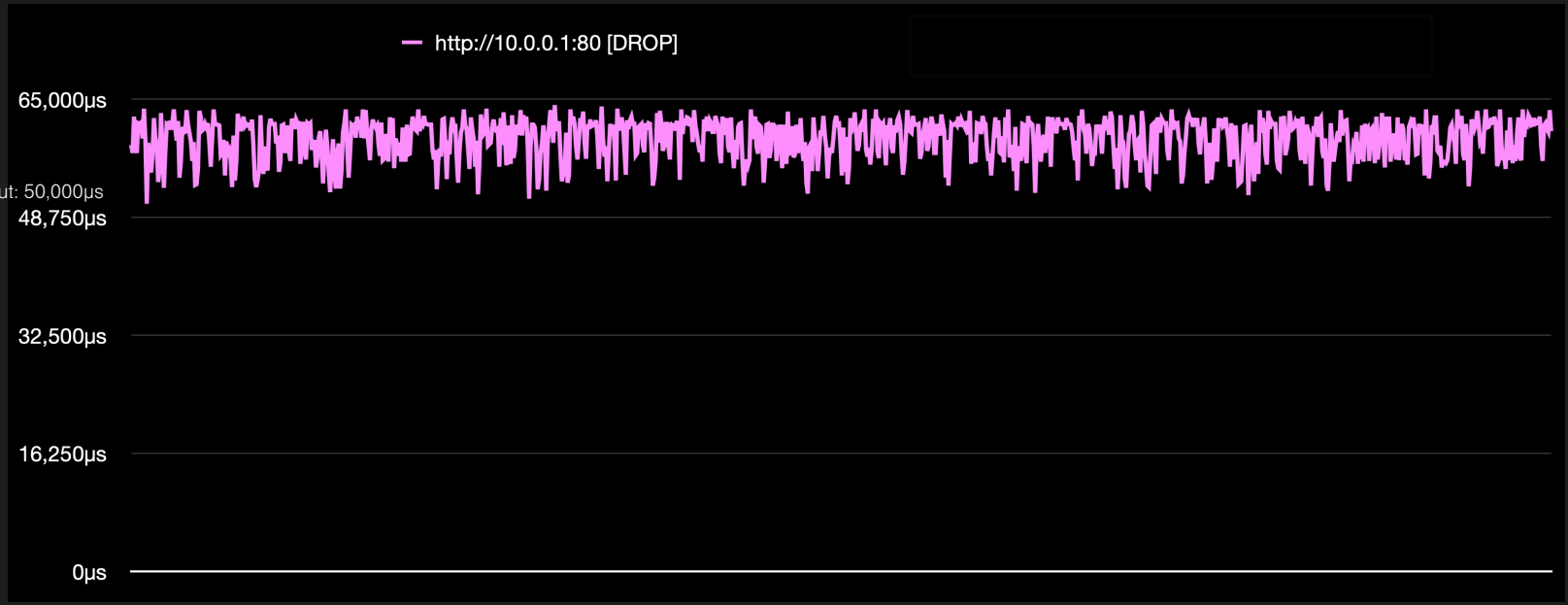
- We only care if host is responsive or not



- Port is closed
  and firewall drops packets,
  or host is unreachable
  ➥ Host is unresponsive
- Port is closed
  and firewall rejects packets
  ➥ Host is responsive
- Port is open
  and a process is listening
  ➥ Host is responsive

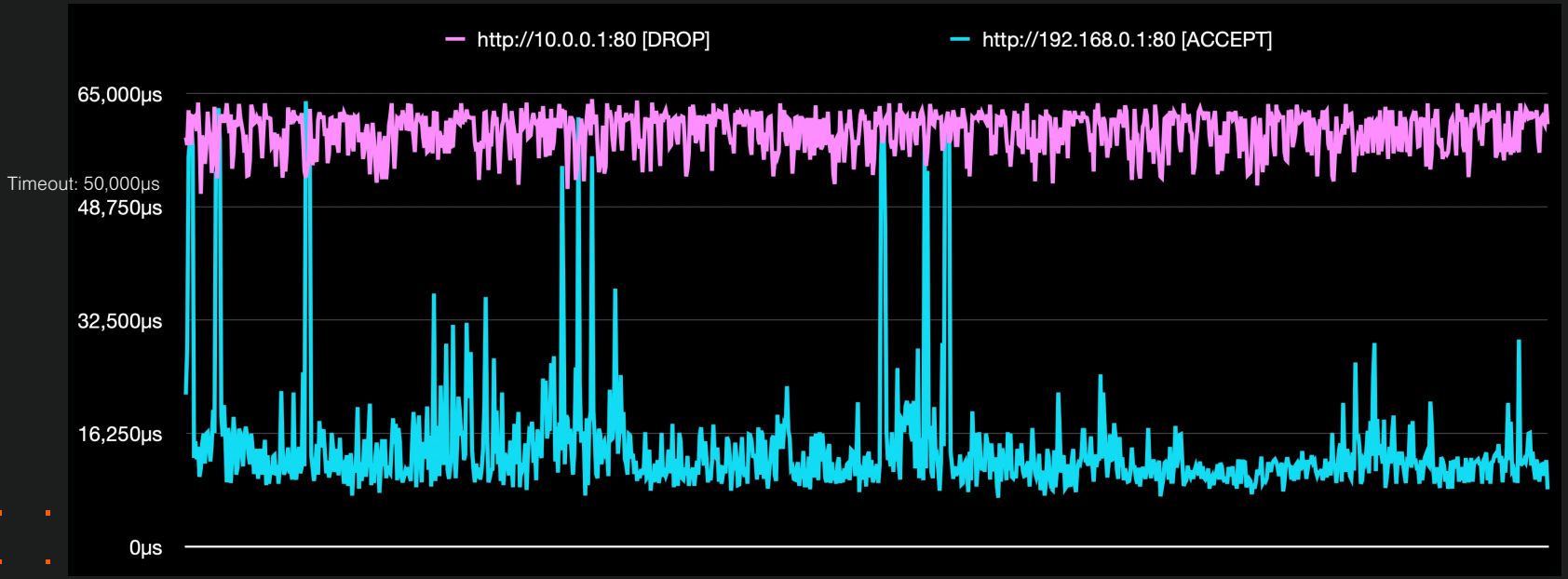
Algorithm

1. If a fetch times out, the host is unresponsive



Algorithm

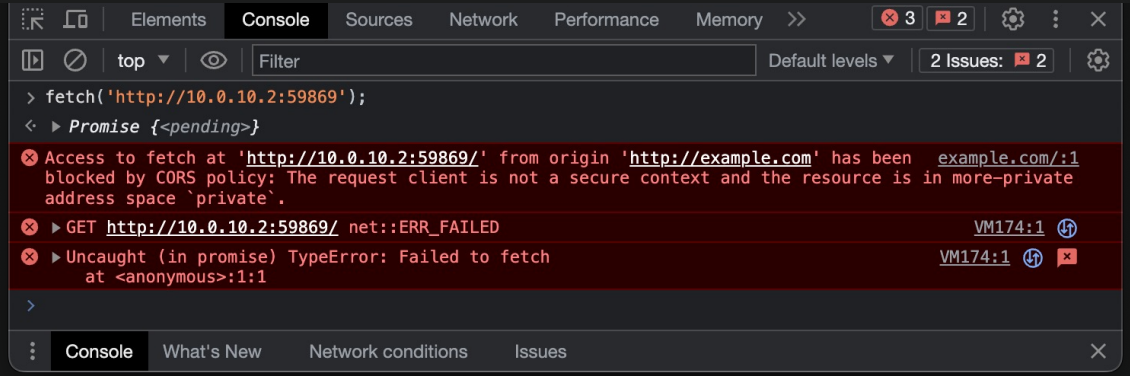
1. If a fetch times out, the host is unresponsive
2. If a fetch ends before the timeout, the host is responsive

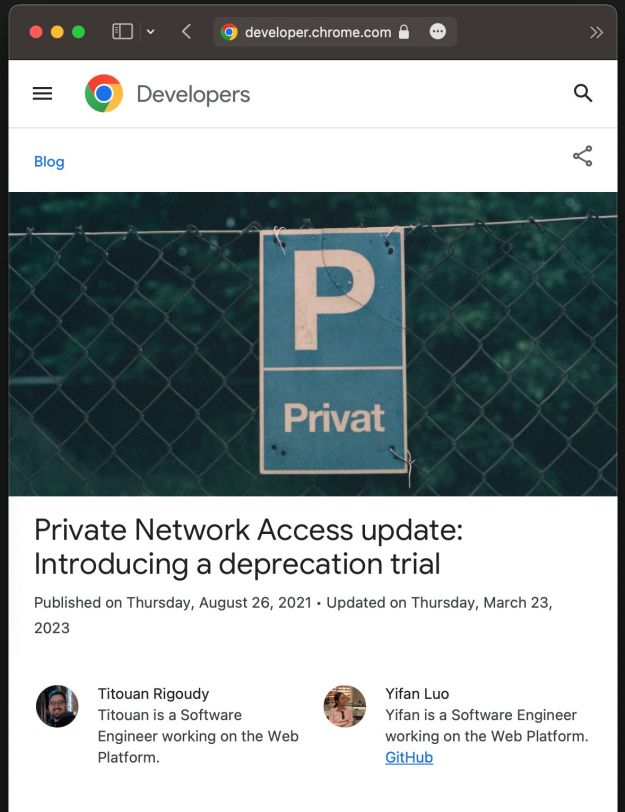


TRUESEC

Observation: Private Network Access

- On Chrome by default, requests to private network resources are allowed only from HTTPS web pages
- HTTP requests to a client on the LAN from an HTTP web page would return a CORS error





TRUESEC

Observation: Private Network Access

- How the CORS error gets returned:

W3C “Private Network Access”

3.1.1. Secure context restriction

5. The HTTP-network fetch algorithm is amended to add 3 new steps right after checking that the newly-obtained *connection* is not failure:
    1. Set *response*’s IP address space to *connection*’s IP address space.
    2. Let *privateNetworkAccessCheckResult* be the result of running Private Network Access check for *fetchParams*’ request and *connection*.
    3. If *privateNetworkAccessCheckResult* is a network error, return *privateNetworkAccessCheckResult*.

TRUESEC

Observation: Private Network Access

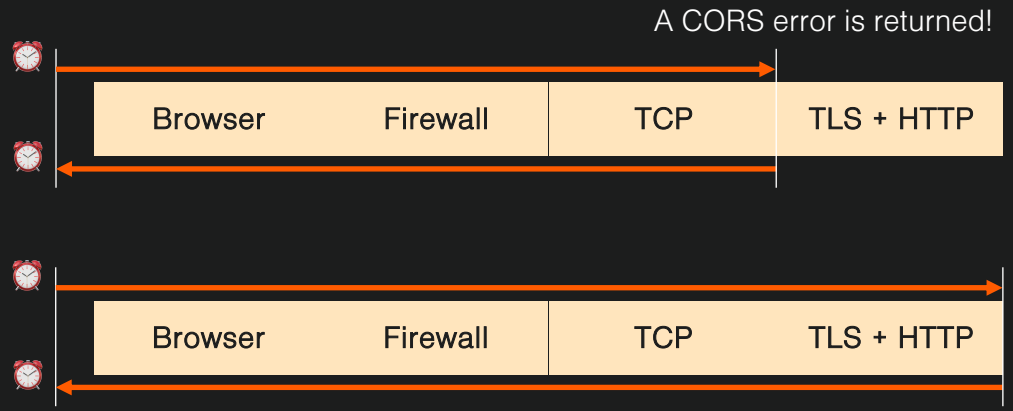
- How the CORS error gets returned:

W3C “Private Network Access”

3.1.1. Secure context restriction

5. The HTTP-network fetch algorithm is amended to add 3 new steps right after checking that the newly-obtained *connection* is not failure:

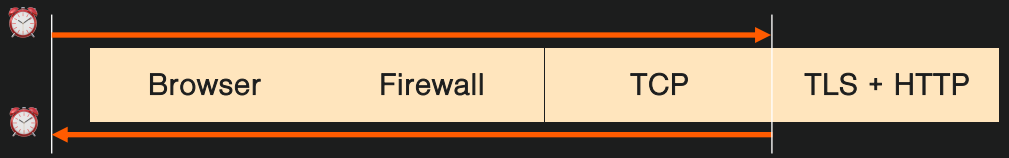
- New states and hypotheses
  - When fetching HTTP local IP from an HTTP web page, if port is open and a process is listening:
  - When fetching HTTPS local IP from an HTTP web page, if port is open and a process is listening:



TRUESEC

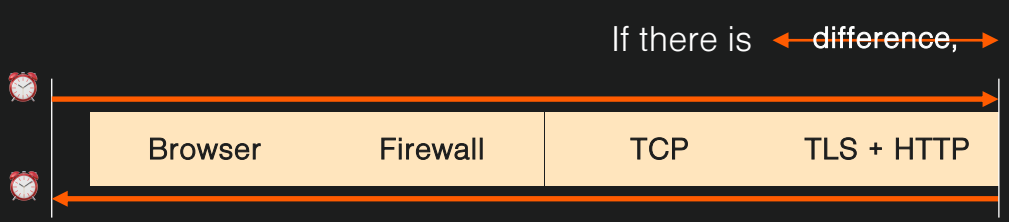
Observations and States

- When fetching HTTP local IP from an HTTP web page



A CORS error is returned!

- When fetching HTTPS local IP from an HTTP web page

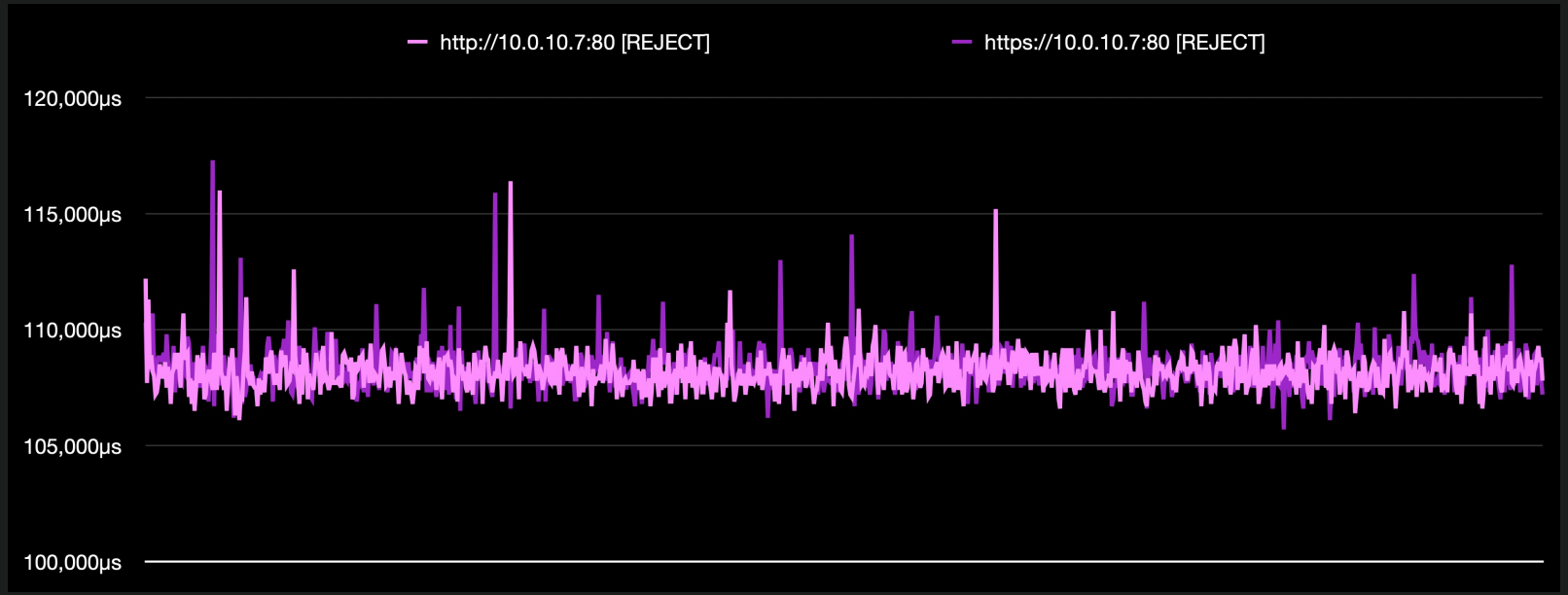


- Port is open
  and a process is listening

TRUESEC

Algorithm

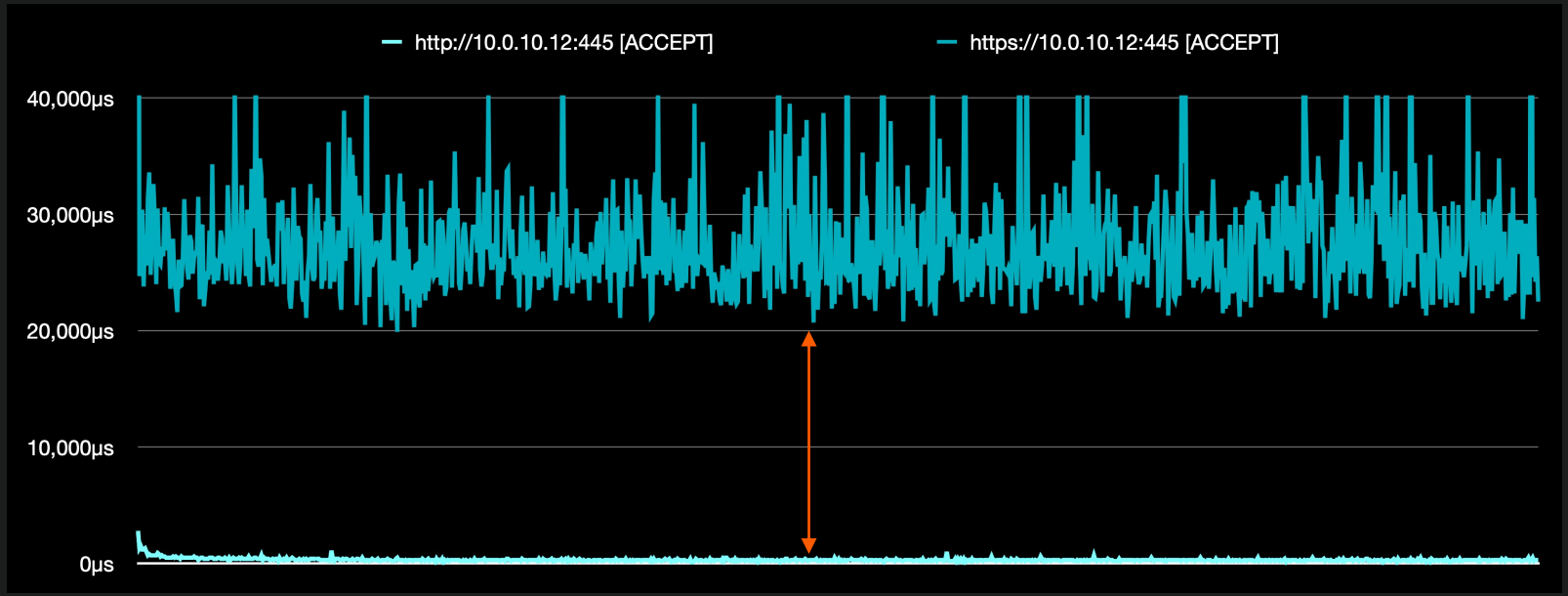
1. If an HTTPS fetch takes a similar time as an HTTP fetch, port is closed and firewall rejects packets



TRUESEC

Algorithm

2. If an HTTPS fetch is significantly slower than an HTTP fetch, port is open and a process is listening



TRUESEC

Demo



your-lan.js

http://lan.kidi.ng

macOS recommended
Chrome required

TRUESEC

Conclusion

- A website can scan your local network

Limitations

- False positives and false negatives
- Needs optimization

Takeaways

- Use Tor browser for privacy & security
- Use ad blockers to avoid malicious tracking scripts
- VPNs can’t be a mitigation



TRUESEC

Thank you!


www.truesec.com / www.security-office.co.kr


twitter.com/truesec


linkedin.com/company/truesec