APRICOT 2023, MANILA

QUIC Transport Protocol

Performance and Security Implications

Paul Vixie *(he/him)*

VP & Distinguished Engineer
AWS Security

Abstract

The Internet has long served as the Web's communications substrate, and historically that has meant TCP/IP. TCP is a clear text reliable stream protocol which predates the Web by about two decades and is usually implemented in the operating system's kernel. Starting in 2013, the Web community has reconsidered the use of clear text protocols and kernel resident protocols. The result is QUIC, a fully encrypted protocol intended to be implementable at the application layer. Adoption of QUIC will radically alter the security profile and performance characteristics of managed private edge networks including home and enterprise, for both Web servers and Web clients. Let's discuss.

QUIC Itself

Crafted in the ~decade following E. Snowden’s disclosures of 2013

- Primary motive is complete end to end communications secrecy by default

Where TCP/IP is usually kernel resident, QUIC layers atop UDP

- Can be in user mode, and revised with greater freedom by app developers

Implications:

- Kernel no longer sees a “connect()” or “accept()” system calls
- All data sent or received is completely opaque to the kernel
- So, traditional endpoint detection/response (EDR) systems will not work

Managed Private Networks

Endpoints are fundamentally unsecurable

- IoT; abandonware; supply chain poisoning; 0-days; intruders

So, operators permit some kinds of traffic, and deny others

- Firewalls: IP, web, DNS

Economics of scale force an anomaly detection posture

- Bad actors must therefore try to “blend in”

Nation-state and ISP networks are not private

- But they want some of the privileges of MPN’s (observation; filtering)

Effective Modern Site Security

- Near oxymoronic – effective ≠ modern, for site security
- What there is, is behavioural, not pattern or privilege based
- Behavioural means we evaluate the signals (packets and flows) sourced or sunk by local and remote actors
- Rule or law breaking is a local matter yet the Internet is global
- “Behavioural” is simultaneously too little and too much security

How Did Site Security Become Ineffective?

Unbounded complexity

- Most know little, few know much, nobody knows all

Hardware, software, protocols, configurations, in a virtual blender

- Extreme churn in vendors, versions, patches, personnel, policies

Confidence in safety is probabilistic

- Backups, logging, verification, assurance – all expensive to do “well enough”
- Many sites assume, and some sites know, that they are already breached

Asymmetry of incentives

- Attacks are a profit center whereas defense is a cost center

Defense Now Requires Rule Breakage

An endpoint operating system that does not trust its apps or its users has to allowlist, or denylist, or pervasively monitor

- Same for a site security administrator
- Same for an authoritarian government

A passionate defender of human freedom in the face of wide spread abuse of end-user privacy by ISPs and governments must seek to disintermediate same

These requirements are in conflict

What’s Happening Now (2013—2023)

In 2013, E. Snowden famously traveled to Hong Kong and made some important disclosures, before traveling onward to Moscow

The IETF invited E. Snowden to give a plenary speech, which resulted in two Requests for Comment (RFCs)

RFC 7258 – Pervasive Monitoring Is An Attack
RFC 8890 – The Internet Is For End Users

No carve outs were made for:

- Monitoring in the service of site security
- Intruders or insiders attackers
- Defense against surveillance capitalism or malware

RFC 9312 – Manageability of QUIC Protocol

3.1. Identifying QUIC Traffic

The QUIC wire image is ***not specifically designed to be*** *distinguishable from other UDP traffic by a passive observer in the network. While certain QUIC applications may be heuristically identifiable on a per-application basis, there is no general method for distinguishing QUIC traffic from otherwise unclassifiable UDP traffic on a given link. Therefore, any unrecognized UDP traffic may be QUIC traffic.*

What Can A Load Balancer See in TCP/IP?

```
00:20:49.818784 IP6 2001:559:8000:ca::41.12684 > 2001:559:8000:cd::5.22:
       Flags [S], seq 901949512, win 65535,
       options [mss 1440,nop,wscale 6,sackOK,TS val 3799452908 ecr 0],
       length 0

00:20:49.819094 IP6 2001:559:8000:cd::5.22 > 2001:559:8000:ca::41.12684:
       Flags [S.], seq 1775462878, ack 901949513, win 65535,
       options [mss 1440,nop,wscale 6,sackOK,TS val 4233103442 ecr 3799452908],
       length 0
```

See Also Encrypted Client Hello (ECH)

Transport Layer Security (TLS) is at the heart of HTTPS and similar

- TLS 1.2 is in near universal use, and works with next-gen firewalls
- TLS 1.3 is now in final clearing stages, and won’t

The specific feature of interest is Encrypted Client Hello (ECH)

- Was Encrypted Server Name Indicator (ESNI) but grew

A next-gen firewall will know the destinations’ IP but not its name

Most destination IP’s serve more than one (“many”) names

It is the name that is of interest to a firewall operator

Ugly Choices for Site Security Administrators

Network traffic is “going dark” due to political and economic forces

- There will be no good way to detect intrusion, exfiltration, malware, spam, DDoS, predacious grooming, or insider corruption

Many sites cannot afford this fight, and will let the floodgates open

Some sites cannot afford not to fight, and will take expensive action

- For example, enforce the use of ALG (proxy) for all trans-gateway flows
- Or perhaps, block all trans-gateway UDP, block TLS 1.3

Innovation (and chaos) can be expected here

Impact on Malware Reversing / Analysis

Malware, as an endpoint, now has rights

- Can forbid monitoring, tracking, and interference (don’t fall back)
- Defenders will have difficulty learning (or using) signalprints

On the bright side, firewalls who block this stuff receive a boon

- Managed private network looks to malware like a reverse engineer
- Malware may not be willing to take that chance

Cooperation Is Alignment

Users, Apps

Clients

Operator

Near ISP

Far ISP

Servers

Cooperation ~~Is~~ Was Alignment

Users, Apps

Clients

Operat or

Near ISP

Far ISP

Server

Age of Surveillance Capitalism (Shoshana Zuboff)

«The challenges of epistemic justice and epistemic rights in this new era are summarized in three essential questions about knowledge, authority and power: Who knows? Who decides who knows? Who decides who decides who knows?»

Thank you!

Paul Vixie

upavixie@amazon.com