Cloaked Network

July 3, 2023 (20230703)

EXECUTIVE SUMMARY

Objective

A new generation of privacy enhanced networking providing better privacy protections, stronger censorship resistance and improved resilience against attacks making it the preferred replacement for incumbent solutions such as VPNs and Tor.

Issues with status quo

Virtual Private Networks (VPNs) have seldom lived up to the promises they made to users. Despite promising safety from the prying eyes of their ISPs and other parties, they have largely been shown to provide a false sense of security to users. From No-log VPN providers who turn out to store logs[1] to the many wholesale compromises of various VPN companies the issues have been severe. There are also companies like Team Cymru[2][3] that offer tracing services[4] that use NetFlow data to provide source attribution by following VPN connections to their source, thus negating any efforts a diligent VPN host may have made.

Tor suffers[5]from several limitations[6][7], some of which are baked into the design and hard to overcome incrementally. From attacks on the TCP protocol that simplify tracing to the simple fact that Tor handles packet on a first in first out basis laying bear the network to any observer with a sufficiently complete overview of the participants. The above list is not exhaustive, but the general sentiment regarding Tor has been that it isn't effective against well funded attackers and that conclusion has been reached by many people and organizations independently. The German BND[8] identified the obvious attacks as early as 2007 and worked with other agencies on attacks.

Solution

[1] https://www.comparitech.com/vpn/vpn-logging-policies/

[2] https://forum.torproject.net/t/why-is-torproject-org-hosted-on-team-cyru-servers/3452

[3] https://www.vice.com/en/article/y3pnkw/us-military-bought-mass-monitoring-augury-team-cymru-browsing-email-data

[4] https://www.vice.com/en/article/jg84yy/data-brokers-netflow-data-team-cymru

[5] https://arstechnica.com/tech-policy/2014/07/report-rare-leaked-nsa-source-code-reveals-tor-servers-targeted/

[6] https://github.com/Attacks-on-Tor/Attacks-on-Tor

[7] https://www.ndss-symposium.org/wp-content/uploads/2017/09/raptor-routing-attacks-on-privacy-in-tor.pdf

https://netzpolitik.org/2017/secret-documents-reveal-german-foreign-spy-agency-bnd-attacks-the-anonymity-network-tor-and-advises-not-to-use-it/

CLOAKED SERVICES

We are building a mixnet that ensures continued high performance by compensating node operators for their services. The mixnet will use HTTP/3 for both client-server and server-server communications via layered tunnels to ensure fully end to end encrypted communications. By offering bitcoin payments to node operators, we ensure a robust network of high bandwidth and low latency routing nodes with a large diverse set of IP addresses.

Hostile nodes

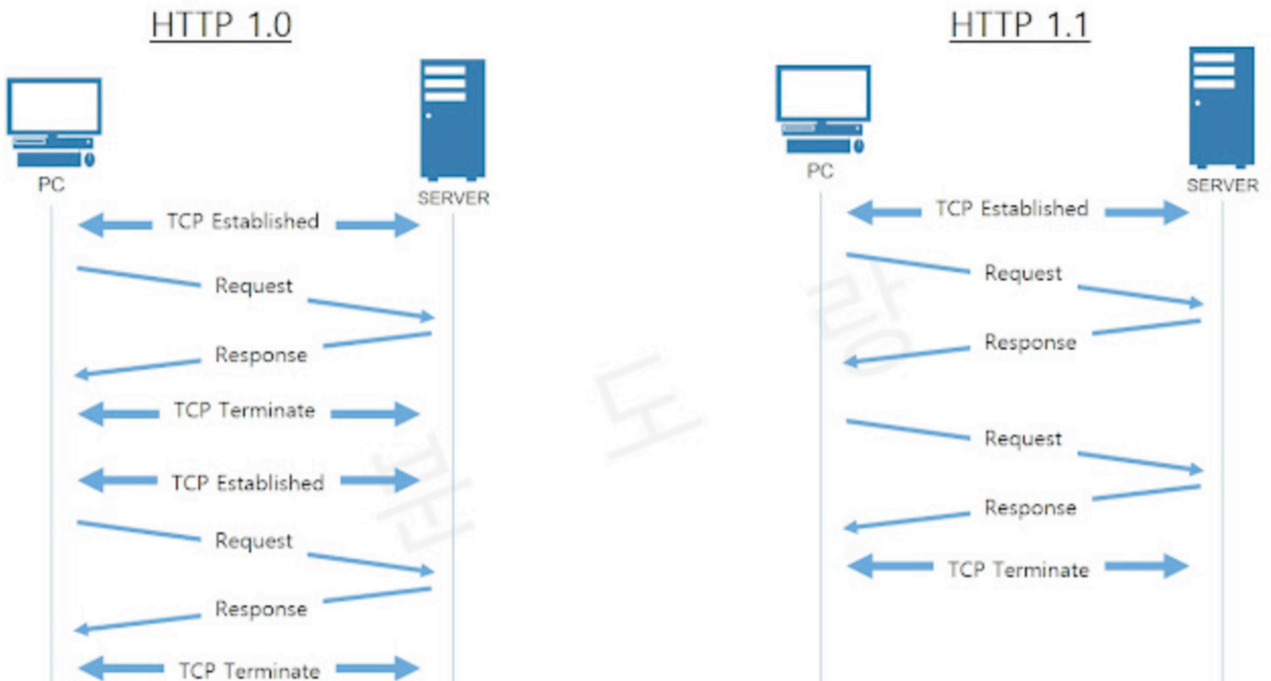
This s one of the simplest avenues of attack on existing anonymity networks. By introducing delays and disruptions and observing the network, it is simple to perform correlation attacks. For certain well resourced attacker, it is even possible to watch the entire network and simply trace packets as they traverse the network. With control of some major backbone points, performing segmentation attacks and watching the TCP level disruption is another simple way to narrow the set of possible endpoints. HTTP/3 can defeat this via its native support of multipath and its connectionless protocol. Network roaming can allow users to continue their communication transparently.

Censorship resistance

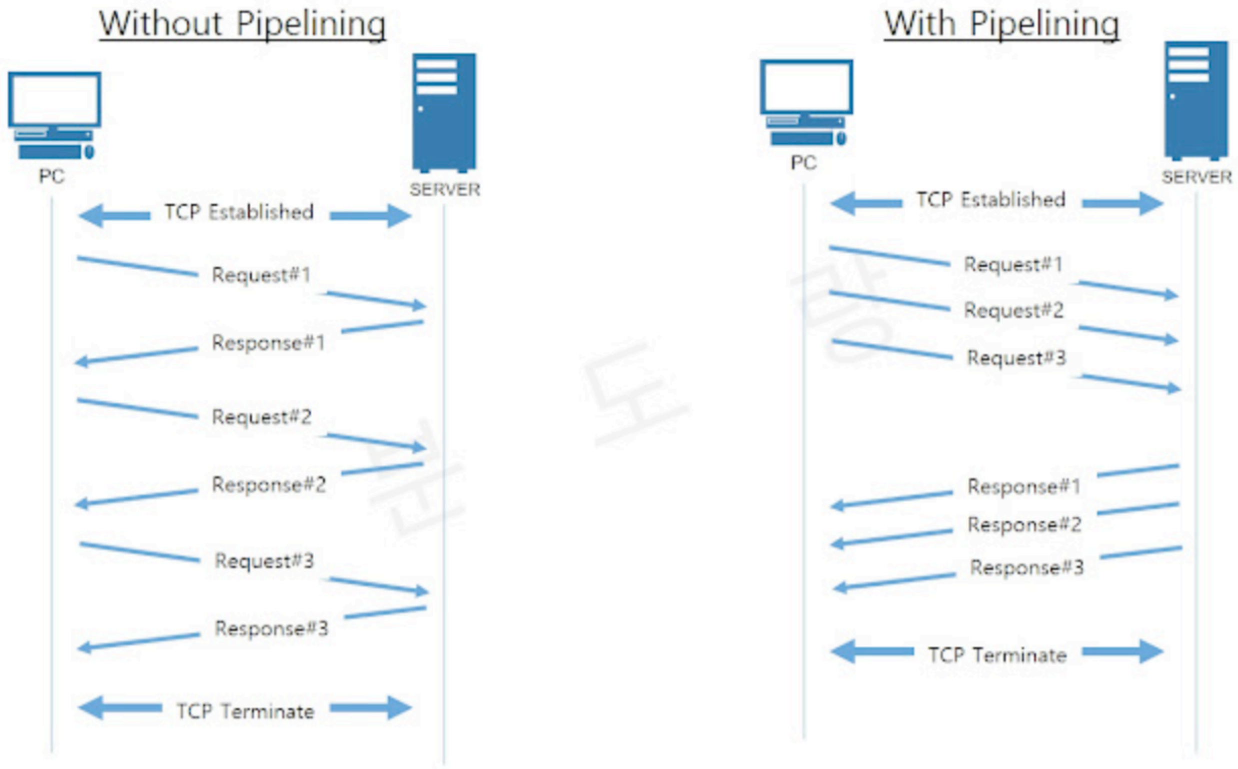
The Cloaked Network will hide in plain sight. By leveraging HTTP/3, we provide a censorship resistant infrastructure that anyone can use to protect their services, be it a web site or the Bitcoin network itself. Recent changes to the underlying technology stack used for web browsing have opened up avenues for massive improvements in the level of privacy afforded by a web browser.

Traffic analysis

The first version of HTTP (HTTP/1.0) made a new connection for each request. The client would request a given file and the server would respond with status and, barring error, the file content.



This made traffic analysis very simple. If an attacker could connect to the site themselves and spider it, it was trivial to later observe user connections and predict which files they were accessing. Even after HTTP/1.1 allowed multiple requests over a single connection, these still followed predictable patterns of traffic and it was still simple to discern the individual requests and responses in an encrypted connection. Later Pipelining was added, which finally added some noise to these patterns.



HTTP/3, includes many improvements which make traffic analysis harder. Firstly it uses UDP instead of TCP for connections. This has improved page load times significantly and also affords better protection against protocol level attacks than TCP does. Instead of being able to cause TCP connections to fail and observe the protocol level effects as they spread through the other layers of a Tor circuit, UDP doesn't force similar side effects. HTTP/3 also allows multiplexing (which allows multiple parallel requests, even to different endpoints). In a multiplexed connection, an observer can't make assumptions about packet size and response patterns. A given packet can correspond to any number of individual streams within the connection. We can also use these streams to ensure that traffic is as homogenous as possible. If an attacker can observe that a given session has a very even number of bytes going each direction, they can infer that the use is not passive streaming of content. This is relatively simple to address as we can deploy cover traffic (aka chaffing) to shift the ratio as needed to mimic appropriately innocuous traffic patterns[9].

Project outline

A privacy system is generally composed of several components, a Directory Service (DS), Mix Nodes (MN) and Clients. Clients get a list of available nodes from the DS and establish circuits through a series of these (which may have specialized roles for entry and exit nodes). Clients will negotiate fees with the Nodes for network services (including cover traffic) and will use Chaumian notes (Cashu/Fedimint style) to make regular micropayments. Lightning will generally be used to purchase the satoshi denominated chaumian notes so as to not cause the user to wait on blockchain confirmation and for the privacy benefits that off-chain transactions provide, but we will also support traditional bitcoin transactions with the mint as we have much confidence in the chaumian mint technology.

Directory Service: Directory servers maintain the list of nodes available for building routes[10]. When nodes register with the DS they indicate the fees they charge for traffic and any relevant metadata such as ownership and jurisdiction. Clients are able to specify connection policies. For example circuits must have 3 different jurisdictions and never use the same organization twice; or can be more specific and indicate all circuit nodes by IP. They can also use specific country choices eg, China->USA->Russia).

Early versions will simply use signed messages at predefined network locations to update the directory, but ensuring that the directory service is robust against censorship and other attacks is essential[11]. Clients will learn IP addresses from querying DNS and will be able to confirm that information received is the latest available by

[9] We can potentially use HTTP/3's multiplexing to make traffic extremely uniform. If there is a request for a file that is 61,536 bytes, we can also request a make another request for a section of the same file in another stream for padding Eg request a Range of 4000 bytes of the file and discard, making the request total 64k). It is also simple to have each node have a chargen-like service that will send random bytes on request.

[10] Ensuring that it is not easy to get a full list of the nodes in the system is important. Both entry and exit nodes need this protection. Entry nodes because it shouldn't be easy for eg China to find a list of IPs within their country that are hosting gateways or IPs outside that can be blocked at the firewall. Using QUIC here is very powerful as any node may be an entry node merely by allowing connections to port 443/UDP.

[11] Future versions will begin to use the Bitcoin blockchain to advertise updates to the DS IPs. Nodes will need to connect to the bitcoin network to ensure reception of these updates, but this too can be done over the Cloaked Network. This is extremely robust. Even if we were to encounter a hostile miner environment, we could broadcast transactions in an encrypted form followed by a second transaction that broadcasts the key for the first TX and indicates the block height and txid for the encrypted data. Even if miners suppress these secondary messages, any Bitcoin node listening for new transactions will receive them in their mempool and can process the new data.

validating information from the DS upon connection. Bitcoin's robust multisig support will be used to validate these messages.

Nodes

Each circuit is constructed by layering. First the client negotiates with the first hop, then extends the path to the next host. This can be done for a single hop or as many as can be fit in our UDP packet (subject to latency and encryption overhead with the path MTU being a hard ceiling so this isn't without limit). 3 hops is the equivalent of a standard Tor circuit (6 for a circuit to a hidden service).

Once the Client has established at least one circuit, it can begin browsing. DNS lookups are done via DNS over HTTP (DoH) to avoid leakage (see RFC9230 for additional privacy improvements) or DNS over QUIC (DoQ RFC9250).

10.0.0.1 = client
10.1.0.1 = first hop
10.2.0.1 = second hop
10.3.0.1 = third hop

HTTP/3 tunnel is created from 10.0.0.1 to 10.1.0.1 (gives 192.168.0.2 to client and 192.168.0.1 as gateway)
HTTP/3 tunnel is extended from 192.168.0.2 to 10.2.0.1 (gives 192.168.1.2 to client and 192.168.1.1 as gateway)
HTTP/3 tunnel is extended from 192.168.1.2 to 10.3.0.1 (gives 192.168.2.2 to client and 192.168.2.1 as gateway)

Later this will be replaced with a better protocol (native HTTP/3 proxying using the MASQUE[12] protocol). MASQUE already has a facility for encapsulating TCP and other protocols in the QUIC stream. MASQUE is used by Apple and Cloudflare to create Apple's iCloud Private Relay.
In the demo, netfilter is used to duplicate the UDP traffic across multiple circuits. This helps protect against packet dropping/network segmentation attacks.

Payments/Incentives

It is undesirable to link a given circuit to a lightning transaction flow since those have explicit identities associated. For this reason, CashU (Chaumian Mint / Token) will be used in the production system. This allows for batch payments and redemptions that preserve user privacy through the use of anonymous Chaumian tokens. Bitcoin main chain and Lightning will be used to purchase Cloaked Sats (Chaumian token/notes, always denominated in satoshis) with lightning being preferred to provide fast settlement.

[12] https://datatracker.ietf.org/wg/masque/about/

All nodes will be randomly chosen as either an entry gateway (entry node), a node that proxies request to the regular internet (exit node), or a node that acts as an internal mixer (internal node). Over time nodes should expect an equal distribution across these three node types.

Clients will receive a time stamp which will provide access to the network for a block of time. The time stamp will be honored by all nodes in the network during that block of time. For initial connections that are not free, the payment from the client will be rewarded to the entry node. The initial entry node will provide the time stamp to the client. Clients will automatically procure additional time stamps in advance of their current time stamps expiration in order to provide a seamless connection as they use the network. Each time block will be 30 mins.

The system will occasionally verify the node's utility by constructing routes and verifying speed and integrity (ie, not modifying http-based sites). Part of this verification will be to determine the capacity of the node and the directory service will only issue a certain number of tokens to the node for each time period. This prevents a node from claiming performance beyond what it can support. Any misbehaving or unreliable nodes can be identified and blocked from future use. In order to discourage malicious nodes, it may become necessary to have providers of nodes stake a certain number of Satoshi's as a deterrent to bad behavior, and make running a large number of nodes in order to perform a Sybil attack infeasible or very expensive.

Prices

Both the client and the node will be able to set their own price. Both will be presented with the average rate paid during the last cycle. Clients will choose a max price they are willing to pay. The client will then look for the least expensive entry node and payment will be made from the client to the first entry node that is used during that time block. All middle and exit nodes will honor traffic from any client with a valid time stamp.

Clients that choose free connections, will only be able to access available entry gateway nodes offering free services. Clients that choose to pay will have access to entry gateway nodes that are charging = or < than the max price the Client user is willing to pay.

Appendix A - HTTP/3 Features: Multiplexing

One of the main features of HTTP/3 is its use of the QUIC (Quick UDP Internet Connections) protocol, which provides multiplexing capabilities. Multiplexing is a technique that allows multiple independent streams of data to be transmitted over a single network connection. This can improve the performance and efficiency of network communication, by reducing the overhead associated with establishing and maintaining multiple connections.

In the context of the Cloaked Network, multiplexing can be used to provide cover traffic, which is a means of disguising the true content and purpose of network communication. By transmitting cover traffic over a single QUIC connection, HTTP/3 can reduce the visibility and distinguishability of the underlying data streams. It can be used to shape the overall nature of the link, making a node appear to be streaming when it is mostly transmitting data (the downstream is all garbage and discarded). This can make it more difficult for attackers or surveillance agents to identify and target specific streams of data, helping to protect the privacy and security of internet users.

Multiplexing can also be used to improve the performance and reliability of cover traffic. By transmitting multiple streams of data over a single connection, HTTP/3 can reduce the overhead and latency associated with establishing and maintaining multiple connections. This can improve the performance of cover traffic, making it more practical and useful for a wider range of applications. For example, where CDNs are available for a given resource, we could allow the Cloaked Network to gossip the hashes of specific common files and the nodes could obtain the file at an alternative source where it makes sense to do so. This can blunt the effectiveness of some Google tracking (eg Font resource and similar tracking).

Overall, the use of multiplexing in HTTP/3 can provide a valuable tool for implementing cover traffic that provides privacy and anonymity for internet users. By leveraging the performance and security features of the QUIC protocol, HTTP/3 can enable the efficient and secure transmission of multiple streams of data over a single connection, helping to protect the privacy and security of users on the internet.

Appendix B - HTTP/3 Features: IP Address Migration[13]

HTTP/3 is full of features that benefit builders of privacy enhancing systems. One of these is Address Migration. Because the protocol is connectionless, relying only on a session key for identification, it is relatively simple to have sessions survive interruptions in the network thus removing one major confirmation attack that is endemic to TCP based onion routing protocols. If a given connection is interrupted, even via minor packet delays, it will elicit traffic from the TCP protocol as extra ACK packets are sent or data is retransmitted. An observer need not decrypt the session, they can simply confirm that extra packets are sent in response to the delay or interruption.

HTTP/3 can avoid these attacks by migrating between networks in the case of any interruptions, or, taken to an extreme, there is the MIMIQ protocol which initiates frequent IP changes without disrupting transfers.

> *MIMIQ is one approach to privacy enhancement via connection migration. The authors describe it as a privacy-enhancing system that enables flexible IP address mixing. MIMIQ only relies on a single trusted network for deployment [...]. Using MIMIQ, a client frequently changes its IP address (i.e., IP hopping) within the trusted network's address space, without changing locations or disrupting ongoing connections. Leveraging IP hopping and QUIC, MIMIQ prevents an adversary from discovering the client originating a flow or associating multiple flows with the same client. By changing the IP address in the middle of a connection, MIMIQ can split a connection into multiple smaller flows to reduce the amount of information the adversary can learn from a single connection, further mitigating traffic-analysis attacks.*

[13] https://www.usenix.org/system/files/foci20-paper-govil.pdf