Minimal-latency Networking Through Better Security

W. Michael Petullo Jon A. Solworth Daniel J. Bernstein Tanja Lange Xu Zhang
http://www.ethos-os.org

UIC UNIVERSITY OF ILLINOIS AT CHICAGO COLLEGE OF ENGINEERING
Department of Computer Science

Minimal Latency Tunneling (MINIMALT)

MINIMALT is a new network protocol that provides

- **Ubiquitous encryption** for substantial confidentiality, protecting maximal amount of packet headers
- Server host and client **user authentication**
- Extensive **Denial-of-Service protections**
- **IP mobility** with protections against linking (unlinkability)

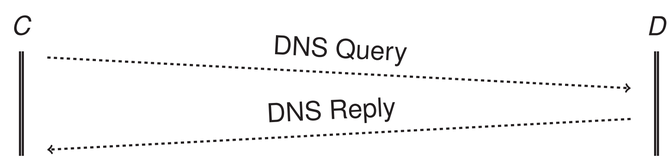
By exploiting the properties of its cryptographic protections, MINIMALT **eliminates three-way handshakes** thus creating connections **faster** than unencrypted TCP/IP.

Protocols Comparison

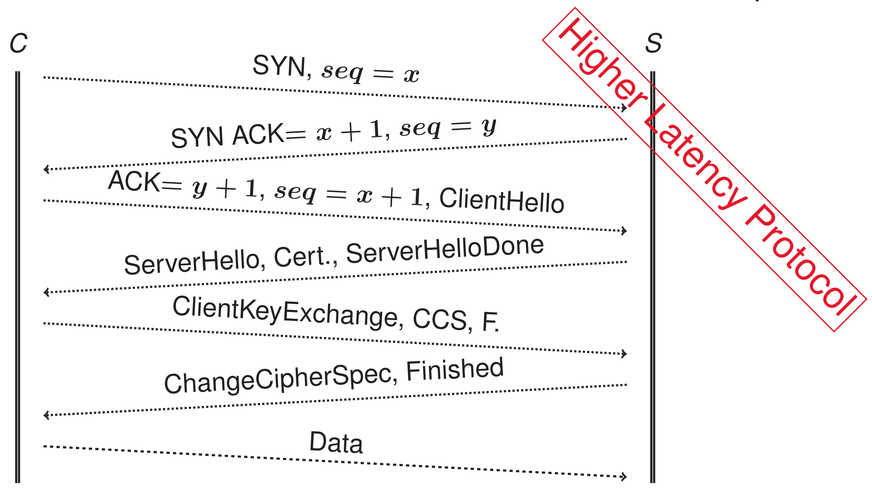
	TCP/IP	TCP Fast Open	SST	IPsec	Labeled IPsec	TLS	False Start	Snap Start	Tcpcrypt	MINIMALT
Encrypt			✓	✓	✓	✓	✓	✓	✓	✓
PFS				✓	✓	✓	✓	✓	✓	✓
User authentication					✓	✓	✓	✓	✓	✓
Robust DoS protections										✓
Round trips before client sends data*	2	2	2	≥4	≥4	4	3	2	3	1
Round trips if server is already known	1	1	1	≥3	≥3	3	2	1	2	0
Abbreviated† round trips	1	0	0	1	1	2	2	1	1	0

*Includes one round trip for DNS/directory service lookup of unknown server
†Assumes all available caching from previous connections to same server

Latency Comparison with TLS, and MINIMALT Protocol Trace (Typical Data on First Packet)

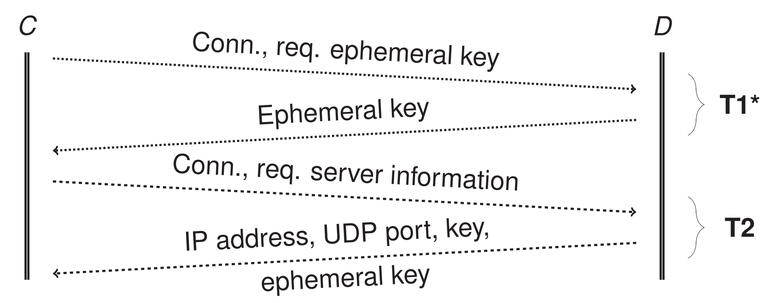


(a) Prelude to a TLS connection establishment: DNS lookup

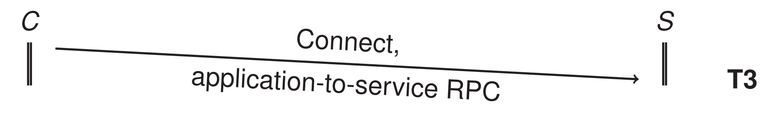


(b) Data on the first packet of a TLS full connection establishment

Three-way handshake Establish a random initial sequence number that is a
- Weak autheticator and liveness check
- Way to detect late packets



(c) Prelude to a MINIMALT connection establishment: Directory Service lookup



(d) Data on the first packet of a MINIMALT full connection establishment

Directory Service Resolves queries for hostname information. This query response contains an IP address, UDP port, long-term key, and ephemeral server keys along with expiration.

T1 C establishes a tunnel, anonymously, to D in order to obtain D's ephemeral public key. *This only needs to be done once at boot time.

T2 C establishes a tunnel to D using ephemeral keys to lookup S's contact information

T3 C establishes a tunnel to S using ephemeral keys

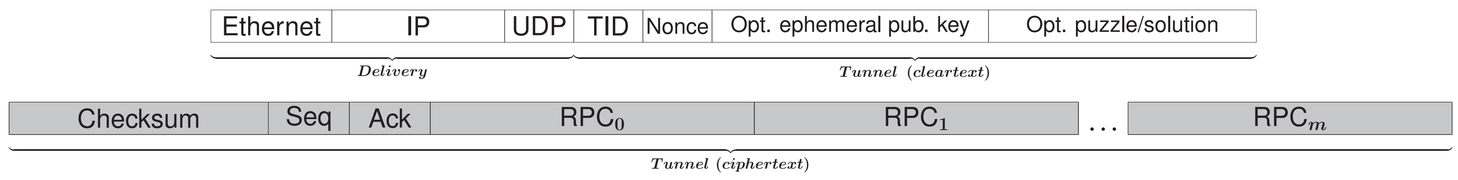
TCP: Minimal Protection

- Minimal inherent protections
  - Unencrypted due to cryptographic performance bottlenecks at the time it was designed
  - No authentication and authorization

Efforts to Secure TCP

- Cryptographic authentication:
  - TLS: discretionary user-space library per programming language
  - IPsec: operating-system-level host-to-host encryption and authentication
  - Labeled IPsec: IPsec combined with SELinux to provide user authentication; complex
- Serveral issues persist:
  - TCP based, thus suffer from **higher latency**
  - Weak **Denial-of-Service (DoS)** mitigation

Packet Format (Non-delivery Portion of Headers Are Protected)



Delivery Routing and other information necessary to deliver a packet to its destination host

Tunnel Server authentication, reliability, and encryption

Connection User authentication and application-to-service multiplexing

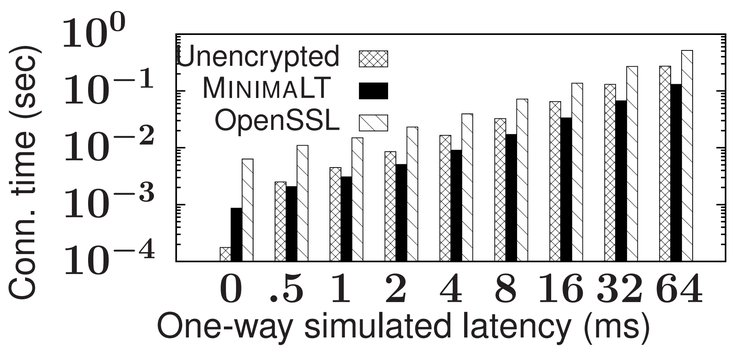
Protocol in a Nutshell

- Directory service and symmetric key establishment using Diffie-Hellman key exchange
- Rekey and perfect forward secrecy
- Crypotographic puzzles and DoS mitigation
- User authentication
- IP address mobility with protections against linking

MINIMALT and Ethos

- MINIMALT is co-designed along with **Ethos**, an experimental operating system targeted at security. For example, Ethos' system calls imply higher abstraction and more security properties
- MINIMALT serves as Ethos' native networking protocol so that the MINIMALT protocol integrates well with Ethos authentication and authorization
- MINIMALT is also ported to Linux

Connection Measurements



Throughput*

System	Bytes per second
Line speed	125,000,000
Unencrypted	117,817,528
MINIMALT	113,945,258
OpenSSL	111,448,656

* Line speed limited