The Tor Project
Anonymity Online

Erinn Clark & Linus Nordberg
erinn@torproject.org
linus@torproject.org
Heard about Tor?
What's the problem?
What's the solution?

Alice

R1

R2

R3

R4

R5

Bob
What's the problem?
What's the solution?
What's the problem?
What's Tor?

```c
/* Tor main loop. */
/* static */ int
do_main_loop(void)
{
    int loop_result;
    time_t now;

    /* initialize dns resolve map, spawn workers if needed */
    if (dns_init() < 0) {
        if (get_option()->ServerDNSAllowBrokenConf)
            log_warn(LD_GENERAL, "Could not set up any working nameservers. "
            "Network not up yet? Will try again soon.");
        else {
            log_err(LD_GENERAL, "Error initializing dns subsystem; exiting. To "
            "retry instead, set the ServerDNSAllowBrokenConf option.");
        }
    }
    handle_signals(1);

    /* load the private keys, if we're supposed to have them, and set up the
     * TLS context. */
    if (!identity_key_is_set()) {
        if (init_keys() < 0) {
            log_err(LD_BUG, "Error initializing keys; exiting");
            return -1;
        }
    }

    /* Set up the packed_cell_t memory pool. */
    init_cell_pool();

    /* Set up our buckets */
    connection_bucket_init();
    stats_prev.global_read_bucket = global_read_bucket;
    stats_prev.global_write_bucket = global_write_bucket;

    /* Initialize the bootstrap status events to know we're starting up */
    control_event_bootstrap(BOOTSTRAP_STATUS_STARTING, 0);

    if (!trusted_dirs.reload_certs()) {
        log_warn(LD_DIR,
                "Could not load all cached v3 certificates. Starting anyway.");
    }
    if (!router_reload_v2_networkstatus()) {
        return -1;
    }
```
What's Tor?
What's Tor?

Tor Protocol Specification
Roger Dingledine
Nick Mathewson

1. Preliminaries

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

1.1. Notation and encoding

PK — a public key,
SK — a private key,
K — a key for a symmetric cipher,
\( a \| b \) — concatenation of 'a' and 'b'.

[00, 01, C2] — a three-byte sequence, containing the bytes with hexadecimal values 00, 01, and C2, in that order.

All numeric values are encoded in network (big-endian) order.

\( H(m) \) — a cryptographic hash of \( m \).

1.2. Security parameters

Tor uses a stream cipher, a public-key cipher, the Diffie-Hellman protocol, and a hash function.

KEY_LEN — the length of the stream cipher's key, in bytes,

PK_ENC_LEN — the length of a public-key encrypted message, in bytes,

PK_PAD_LEN — the number of bytes added in padding for public-key encryption, in bytes. (The largest number of bytes that can be encrypted in a single public-key operation is therefore PK_ENC_LEN-PK_PAD_LEN.)

DH_LEN — the number of bytes used to represent a member of the Diffie-Hellman group,

DH_SEC_LEN — the number of bytes used in a Diffie-Hellman private key (x).

HASH_LEN — the length of the hash function's output, in bytes,

PAYLOAD_LEN — The longest allowable cell payload, in bytes, (509)

CELL_LEN -- The length of a Tor cell, in bytes,
The Tor Project
Available software
Available software
Who uses Tor?
How to help Tor
How to help Tor

Alice → R1 → R2 → R3 → R4 → R5 → Bob
How to help Tor
How to help Tor
Where to find us

- IRC: #tor and #tor-dev @ OFTC
- Email: or-talk and or-dev