CS558 Network Security

Lecture ~~16~~ 17: Tor pt2

BOSTON UNIVERSITY

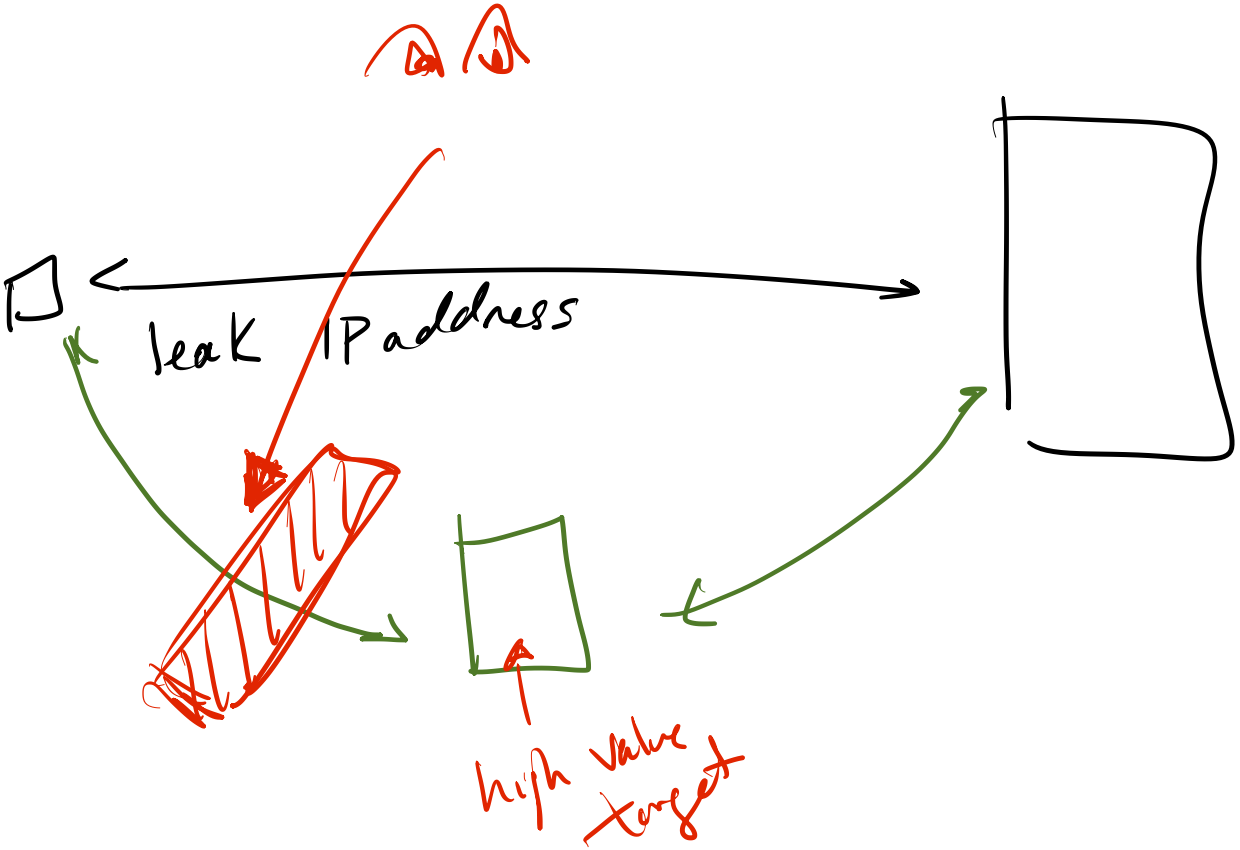
Data vs Metadata

They are actually Core about

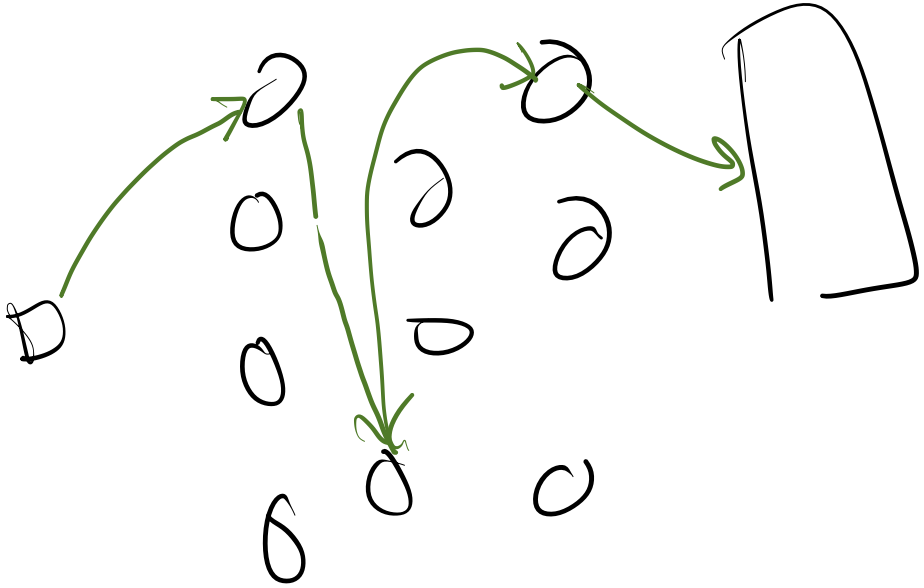
Metadata

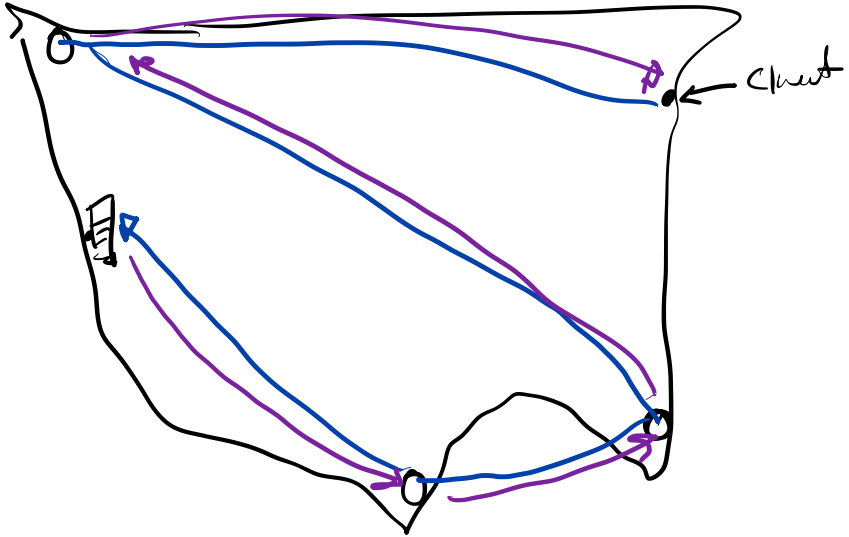
Everything Else

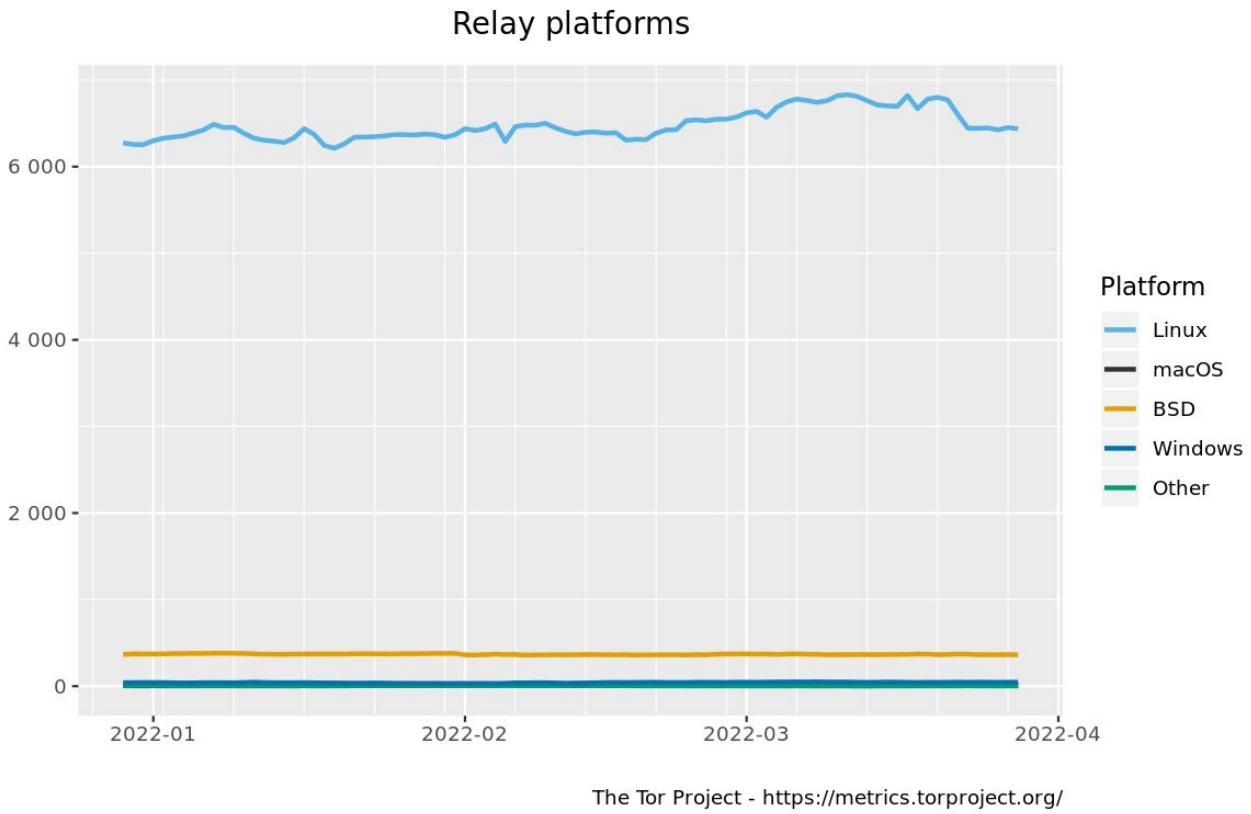
Proxies



Tor Circuit: Chaining Proxies







BOSTON UNIVERSITY

Tor Communication -- “Cells”

Layers in play:

```
The 'Command' field of a fixed-length cell holds one of the following
values:

     0 -- PADDING     (Padding)                    (See Sec 7.2)
     1 -- CREATE      (Create a circuit)           (See Sec 5.1)
     2 -- CREATED     (Acknowledge create)         (See Sec 5.1)
     3 -- RELAY       (End-to-end data)            (See Sec 5.5 and 6)
     4 -- DESTROY     (Stop using a circuit)       (See Sec 5.4)
     5 -- CREATE_FAST (Create a circuit, no PK)    (See Sec 5.1)
     6 -- CREATED_FAST (Circuit created, no PK)    (See Sec 5.1)
     8 -- NETINFO     (Time and address info)      (See Sec 4.5)
     9 -- RELAY_EARLY (End-to-end data; limited)   (See Sec 5.6)
     10 -- CREATE2    (Extended CREATE cell)       (See Sec 5.1)
     11 -- CREATED2   (Extended CREATED cell)       (See Sec 5.1)
     12 -- PADDING_NEGOTIATE   (Padding negotiation)    (See Sec 7.2)
```

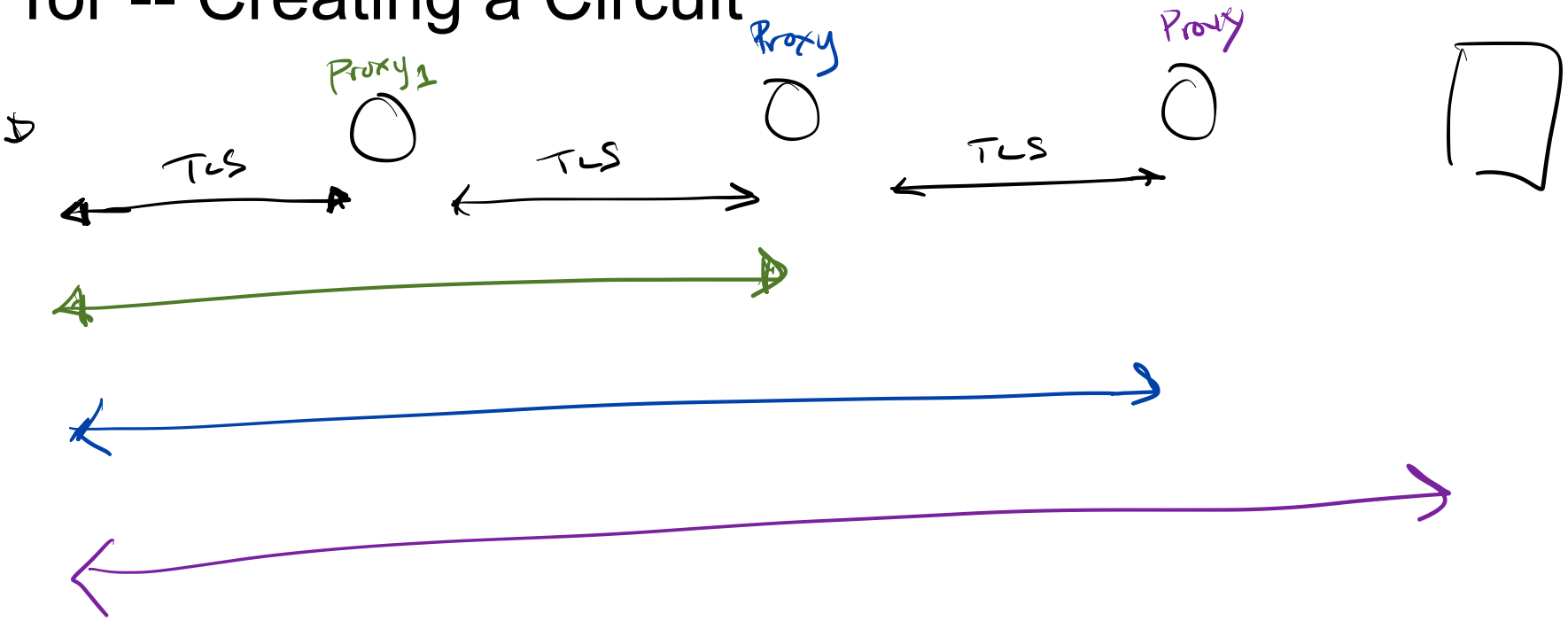
Tor Communication -- “Cells”

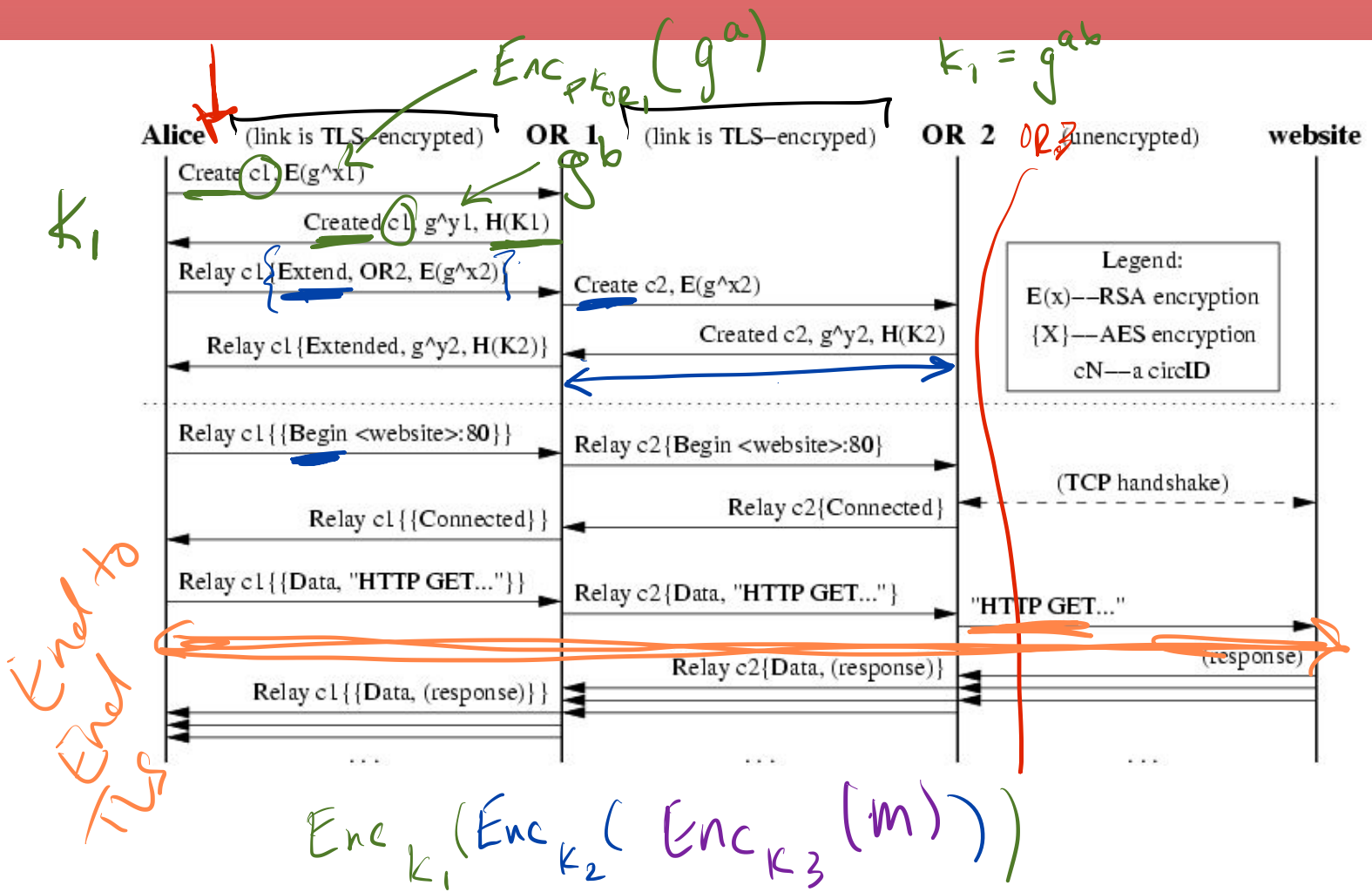
The relay commands are:

```
 1 -- RELAY_BEGIN     [forward]
 2 -- RELAY_DATA      [forward or backward]
 3 -- RELAY_END       [forward or backward]
 4 -- RELAY_CONNECTED [backward]
 5 -- RELAY_SENDME    [forward or backward] [sometimes control]
 6 -- RELAY_EXTEND    [forward]             [control]
 7 -- RELAY_EXTENDED  [backward]            [control]
 8 -- RELAY_TRUNCATE  [forward]             [control]
 9 -- RELAY_TRUNCATED [backward]            [control]
10 -- RELAY_DROP      [forward or backward] [control]
11 -- RELAY_RESOLVE   [forward]
12 -- RELAY_RESOLVED  [backward]
13 -- RELAY_BEGIN_DIR [forward]
14 -- RELAY_EXTEND2   [forward]             [control]
15 -- RELAY_EXTENDED2 [backward]            [control]

32..40 -- Used for hidden services; see rend-spec-{v2,v3}.txt.

41..42 -- Used for circuit padding; see Section 3 of padding-spec.txt.
```

BOSTON UNIVERSITY

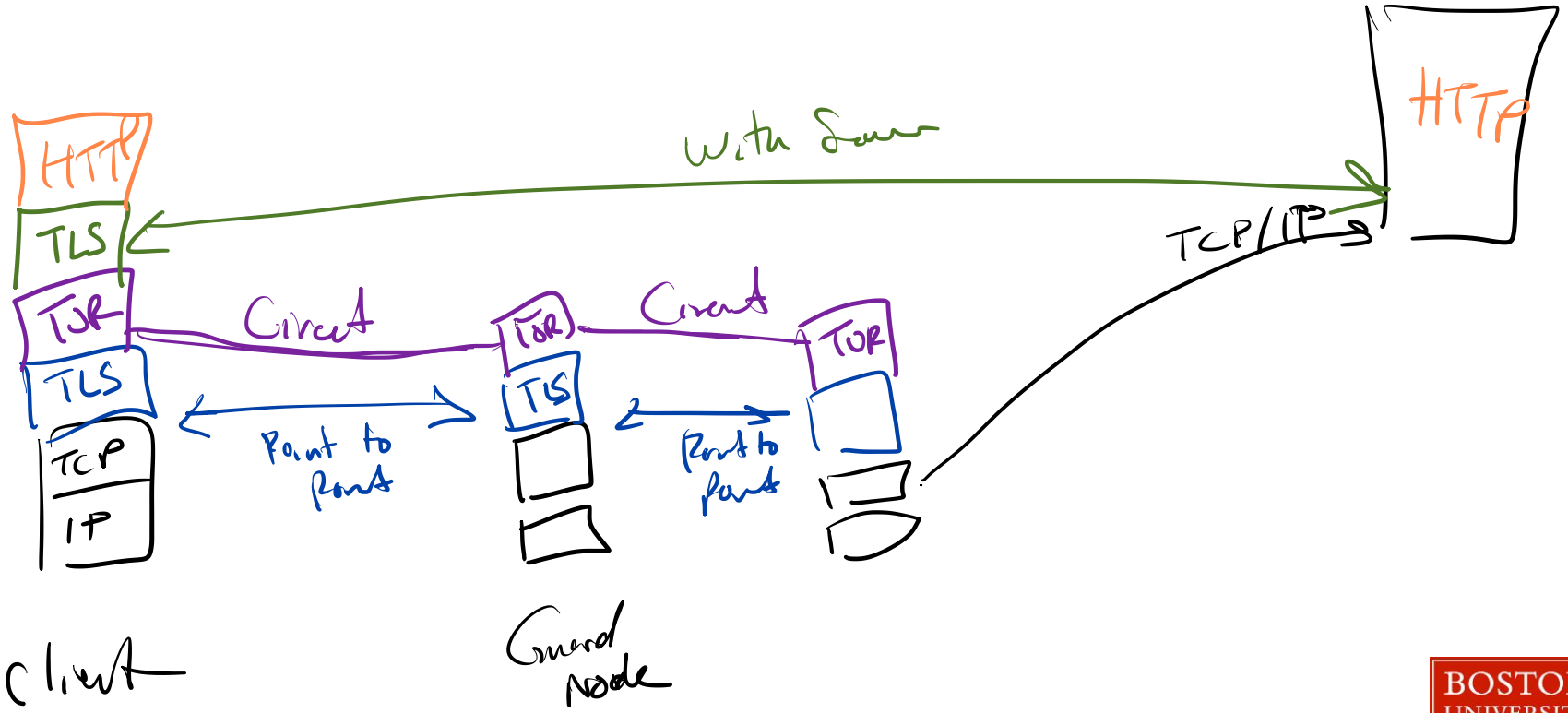
Tor -- Creating a Circuit





BOSTON UNIVERSITY

Tor Circuit: A Stack of Protocols



Tor Traffic: Tracing the protocols

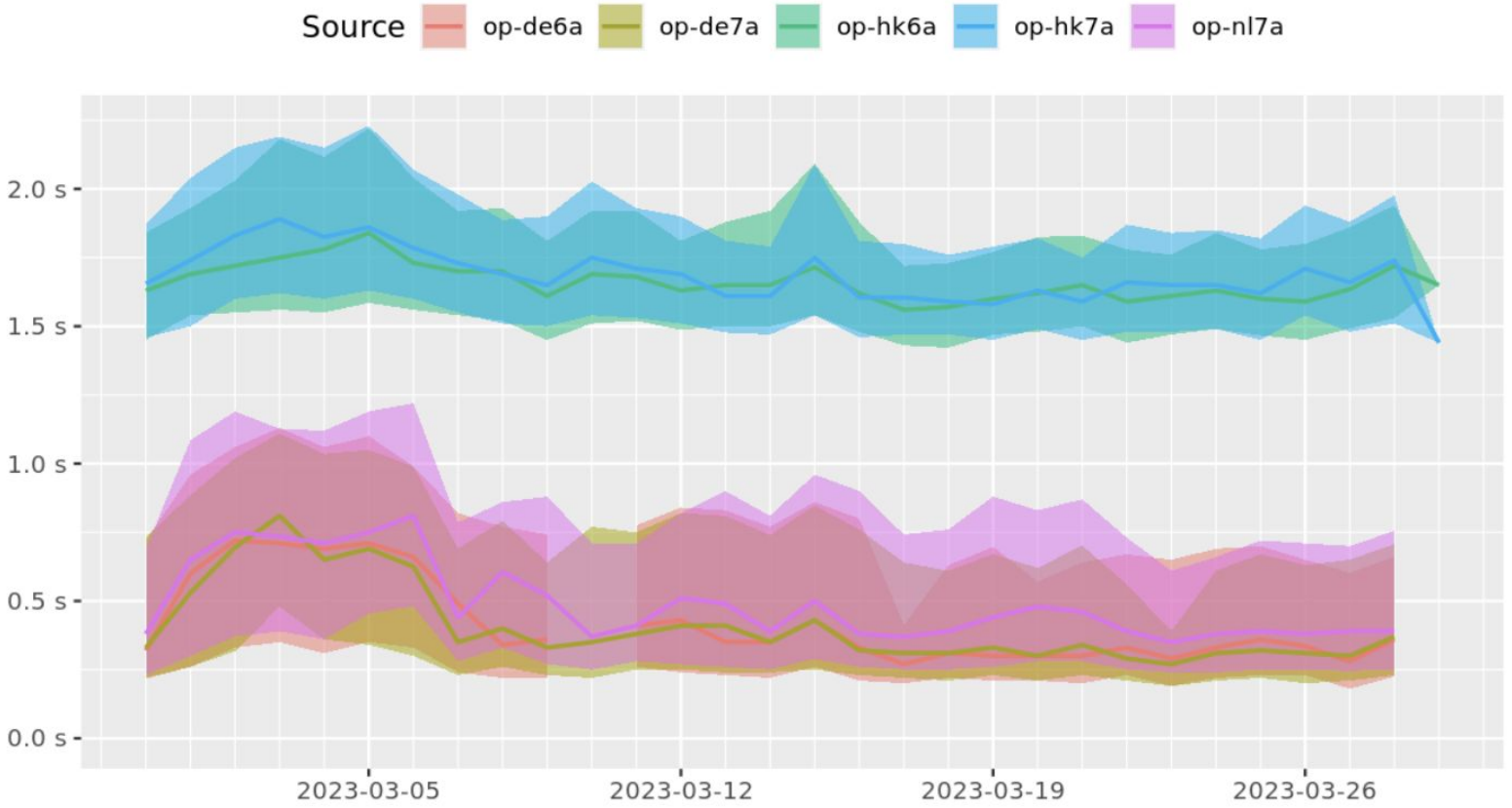
protocol fuzzy → further degrade performance

Website specific metadata fuzzy

Attacking Tor

- Timing Attacks
- Traffic Analysis

Time to complete 50 KiB request to public server



The Tor Project - https://metrics.torproject.org/