Censor-Free Systems

Telex: Anticensorship in the Network Infrastructure
By Eric Wustrow, Scott Wolchok, Ian Goldberg and J. Alex Halderman

20th USENIX Security Symposium, August 2011.

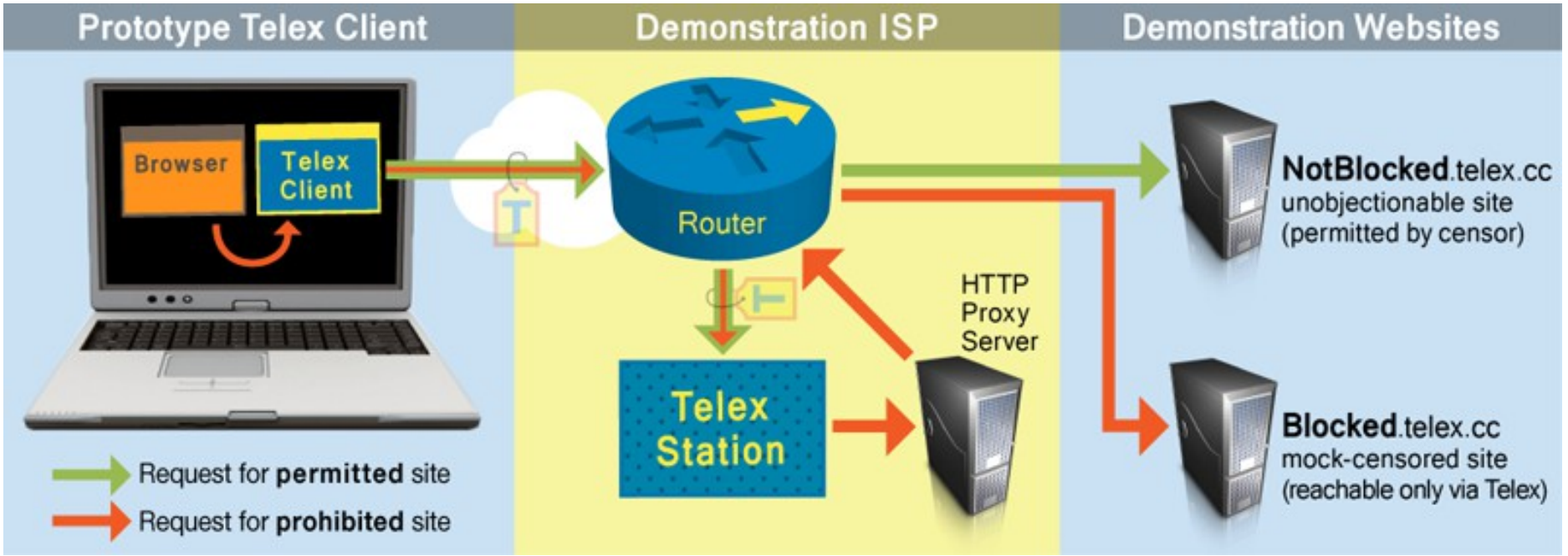
The problem

Many widely-used tools for circumventing Internet censorship don't hide the fact that you are trying to circumvent it

Telex: How it Works

- Main idea : Let backbone routers “hijack” marked network connections
- Censored users install Telex on their machines
- They seemingly surf to https://www.notcensored.org and embed a steganographic token inside their connection
- Backbone routers recognize token, decrypt HTTPS session and hijack connection
- Censor-boxes inside the country don’t know that the traffic is being hijacked
- https://telex.cc/

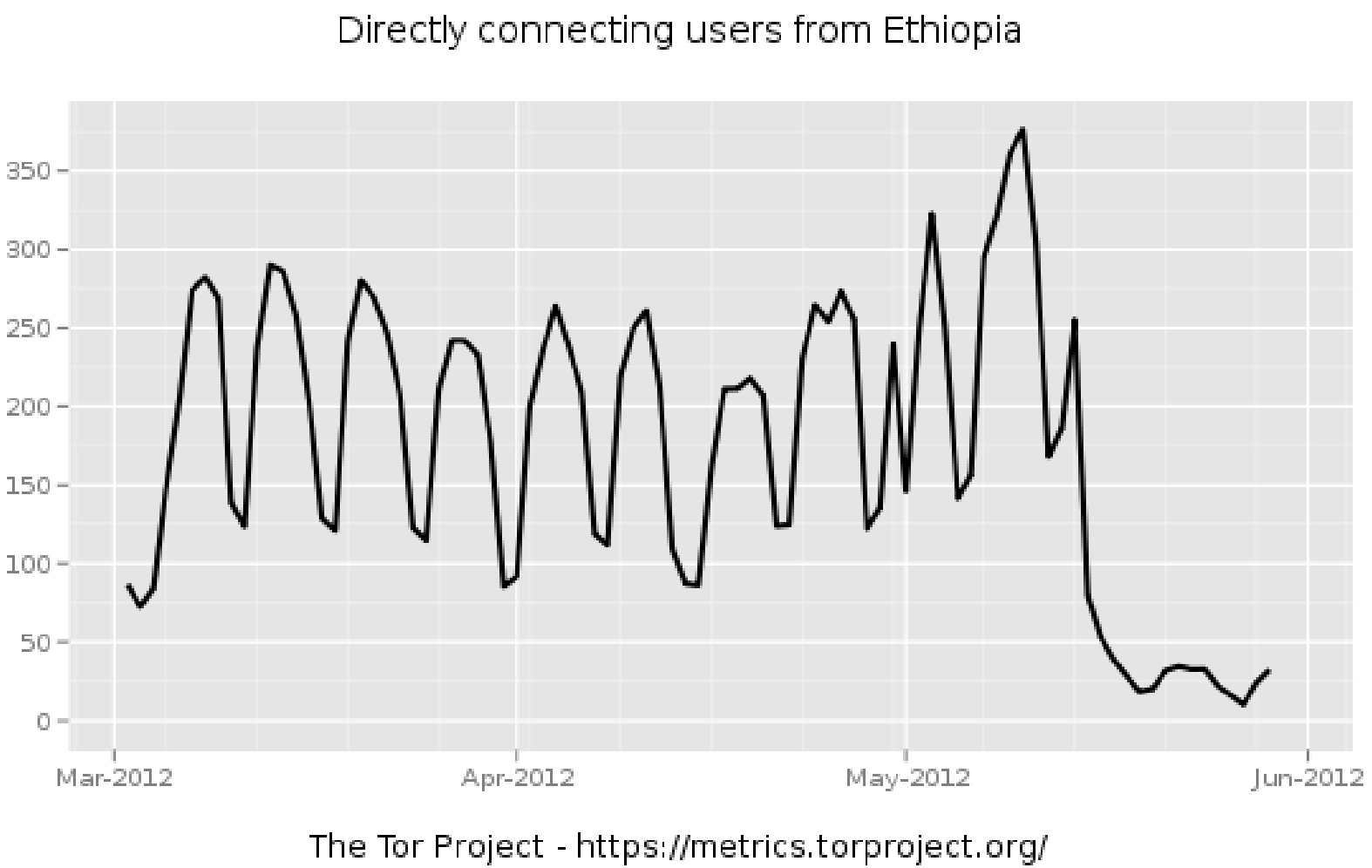
Overview


Prototype Telex Client
Demonstration ISP
Demonstration Websites
Browser
Telex Client
Router
HTTP Proxy Server
Telex Station
NotBlocked.telex.cc
unobjectionable site
(permitted by censor)
Blocked.telex.cc
mock-censored site
(reachable only via Telex)
Request for permitted site
Request for prohibited site

Telex: summary

- Very messy (breaks with end-to-end principle), yet effective concept
- The censor should not be able to distinguish the Telex handshake from a normal TLS handshake
- Telex stations' are selected from a client's database
- So far : In early alpha state
- Very similar concepts proposed at the same time: Cirripede (CCS’11) and decoy routing (FOCI’11)
- Requires cooperation with backbone network providers :-(
- It's deeply based on the fact that you will find a telex station in your way
- http://cyber.law.harvard.edu/netmaps/geo_map_home.php

Ethiopia Introduces DPI



Obfsproxy

- The censor will see innocent-looking transformed traffic instead of the actual Tor traffic.