

Telex

Anticensorship in the Network Infrastructure

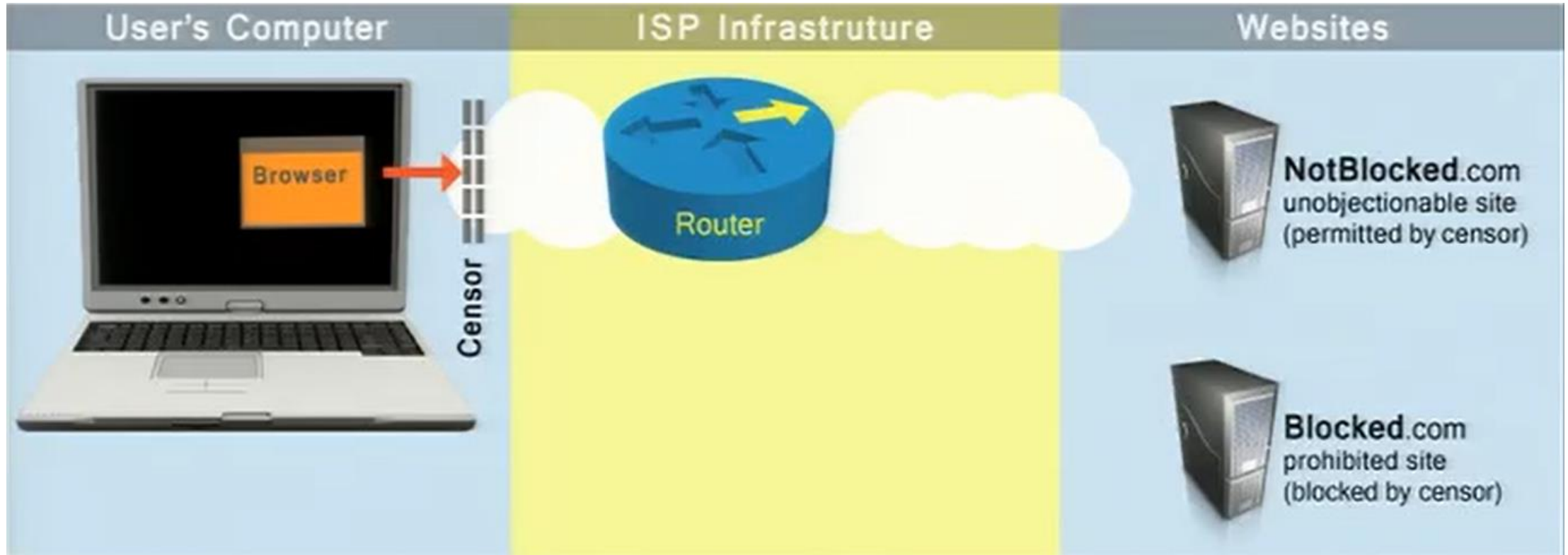
Wustrow, Wolchok, Golberg, Halderman (Aug 2011)

Overview | Network-based censorship

Denylist approach to censorship.

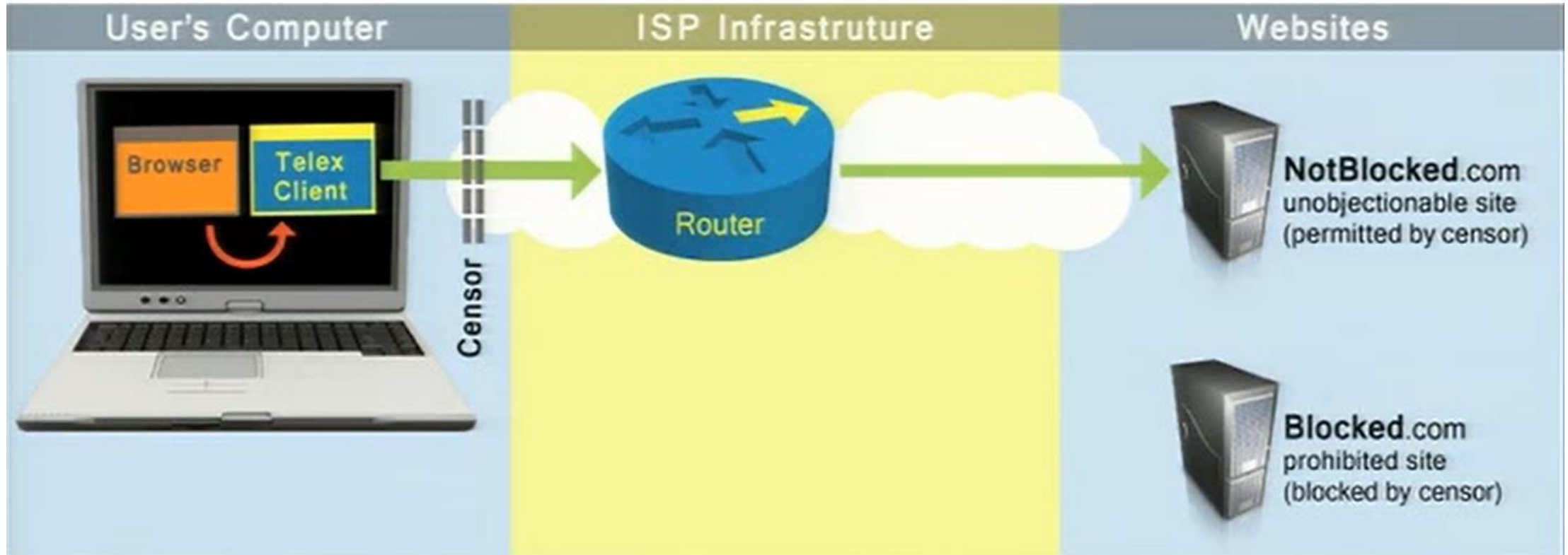
- **Techniques:** IP blocking, DNS blackholes, forged RST packets
 - Cat-and-mouse (peer-to-peer) proxy countermeasures
- **Threat model:**
 - Controls only client's network
 - Blocks according to denylist
 - Allows HTTPS connections to non-blocked sites
 - Does not weaken TLS encryption

Overview | Telex end-to-middle proxy



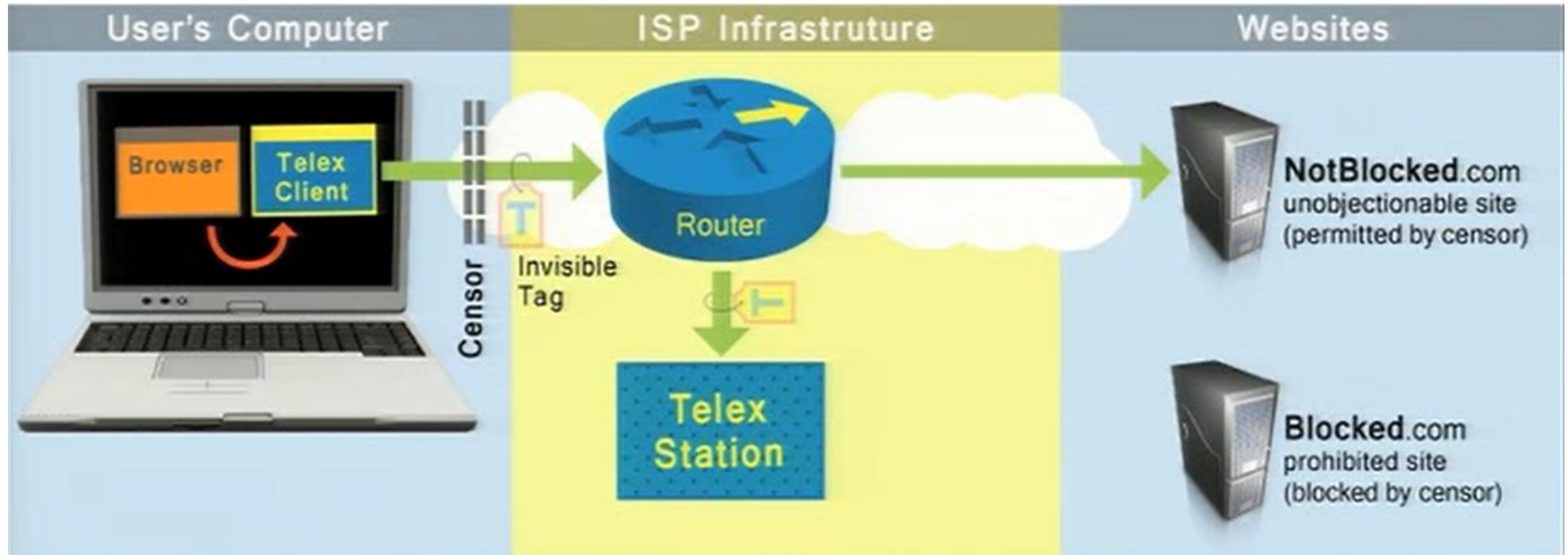
Problem: Attempted access to Blocked.com blocked by censor.

Overview | Telex end-to-middle proxy



Telex client negotiates session with NotBlocked.com, through **cooperative ISP router**.

Overview | Telex end-to-middle proxy



Router forwards requests to **Telex station**, which can identify embedded **steganographic tags**.

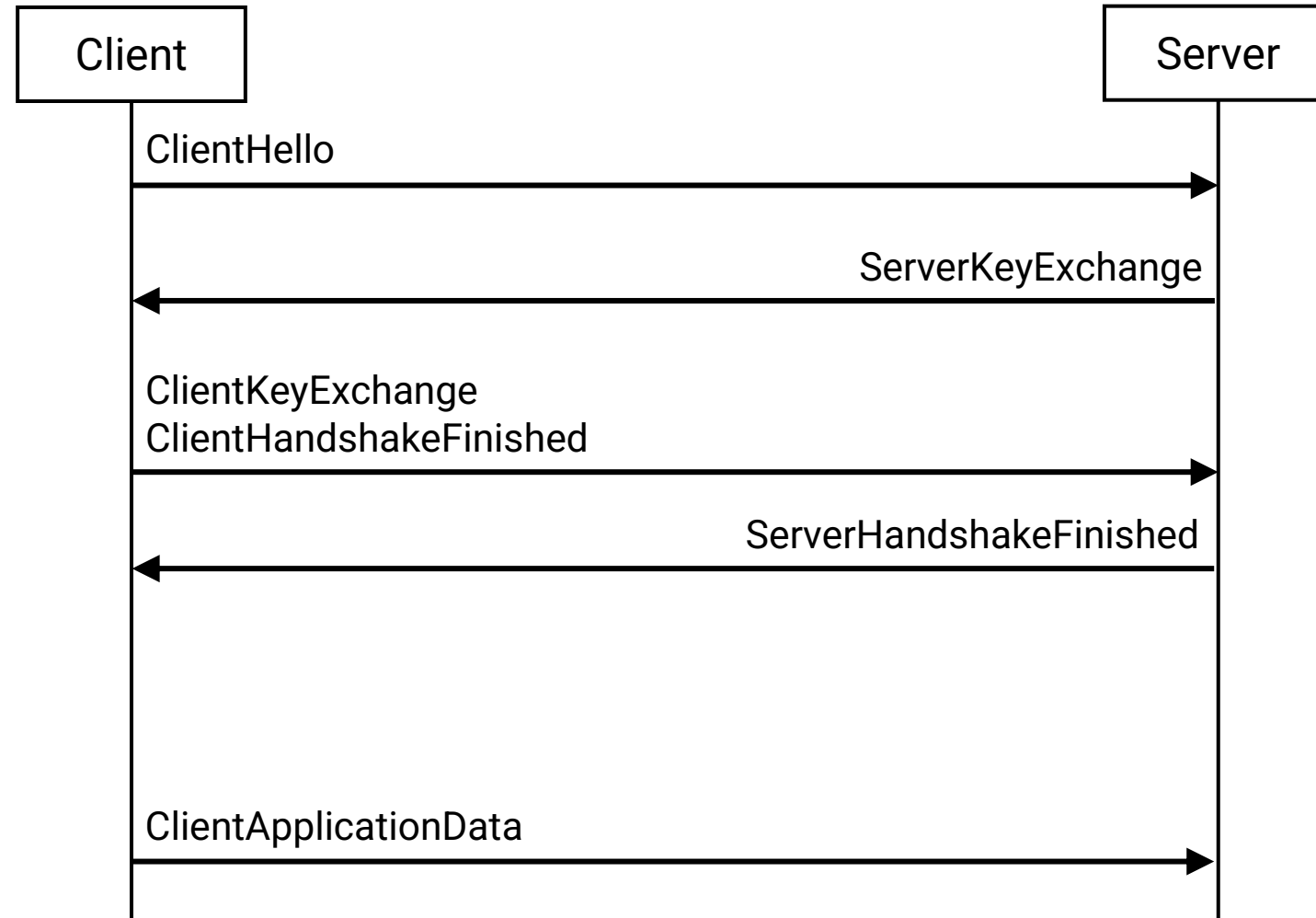
Overview | Telex end-to-middle proxy



Telex client uses tag to **leak session secrets** to station.

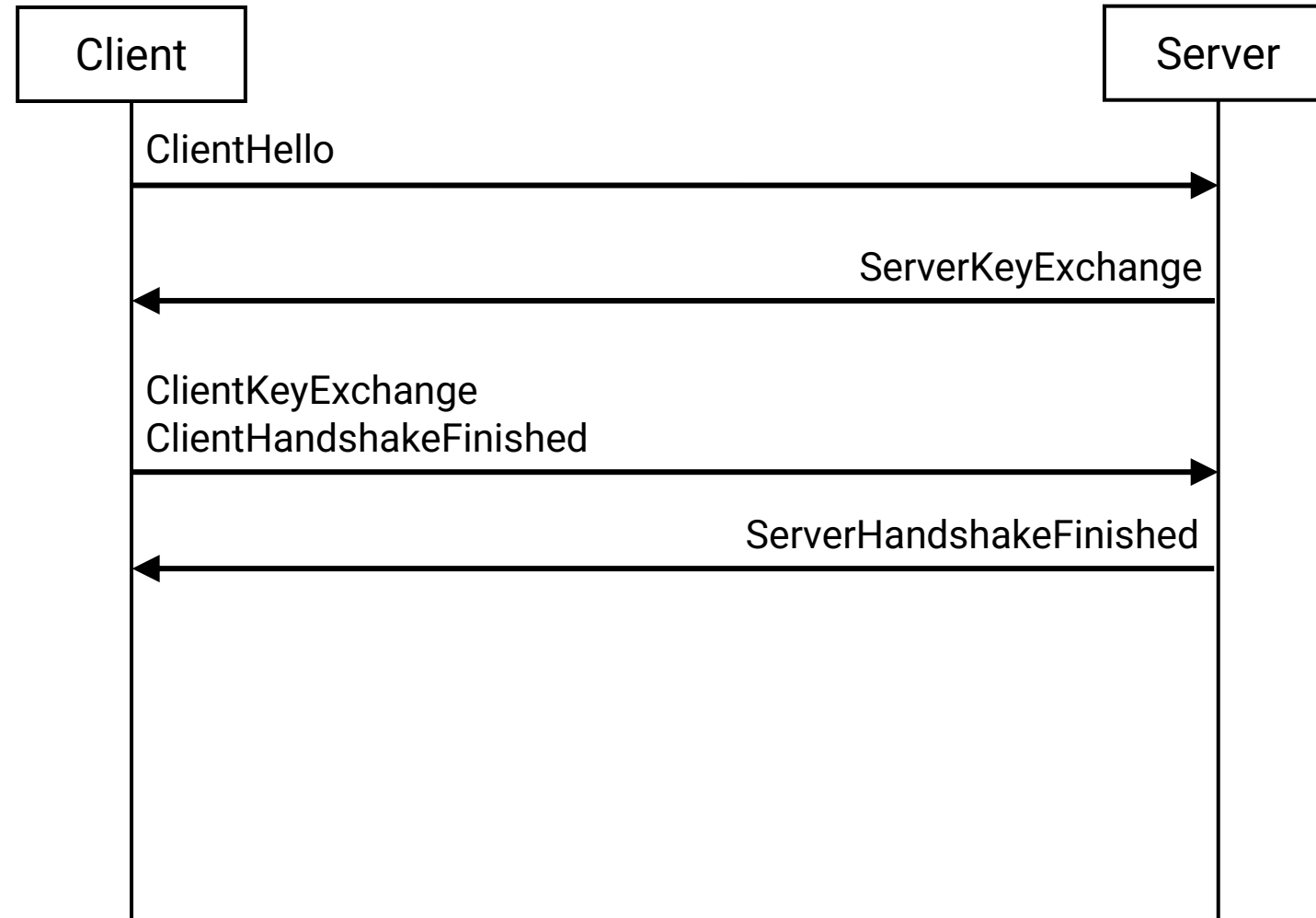
Telex station **hijacks** session to proxy requests to Blocked.com (or other services, e.g., Tor).

Overview | TLS 1.2

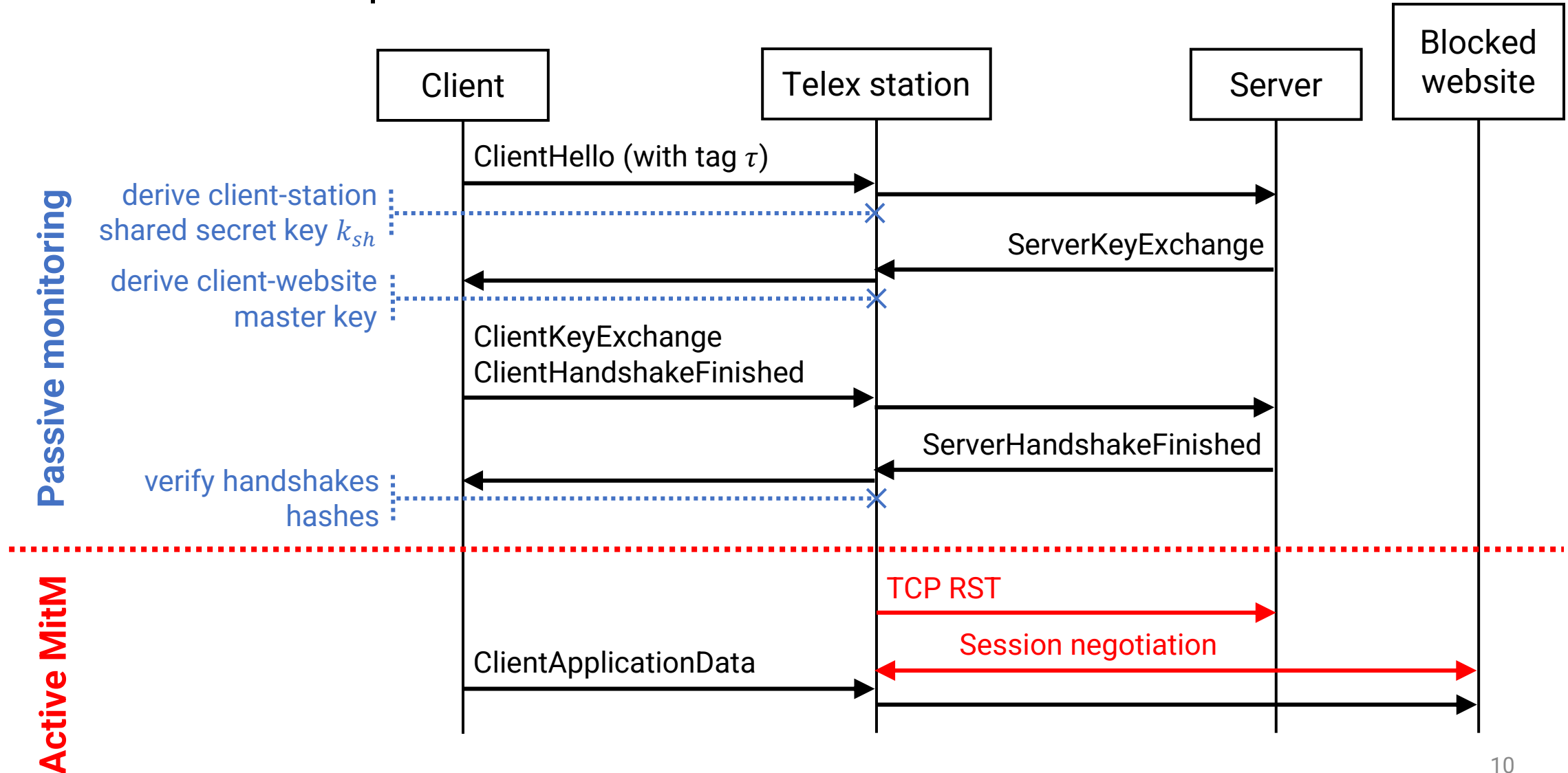


Category	byte + 0	byte + 1	byte + 2	byte + 3	byte + 4
Record header (byte 0)	Record type (handshake)	Protocol version (TLS 1.0)		Message length (165 bytes)				
	16	03	01	00	a5			
Handshake header (byte 5)	Type (ClientHello)	Message length (161 bytes)						
	01	00	00	a1				
Handshake message (byte 9)	Client version (TLS 1.2)		Client random nonce [4 byte UNIX timestamp + 28 byte random]				Session id (none)	
	03	03	xx	xx	xx	...	00	
Cipher suites (byte 44)	Message length (32 bytes)		Cipher suite list [2 bytes per cipher suite]					
	00	20	xx	xx	xx	...		
Compression, extensions header (byte 78)	Length (1 byte)	Method (none)	Extensions length (88 bytes)					
	01	00	00	58				
Extensions message (byte 82)	Extension type (Server Name Indication)		Total length (24 bytes)		Entry length (22 bytes)		Type (DNS name)	...
	00	00	00	18	00	16	00	...

Overview | TLS 1.2



Overview | TLS 1.2 with Telex



Telex | Tag requirements

1. Fast recognition only if private key known
 - Diffie-Hellman key agreement with hashing
2. Convey shared secret in 224-bits
 - Elliptic-Curve DH over 168-bit prime field (~84-bit security)
 - Hash output 56-bit
3. Indistinguishable from random
 - Two mutually exclusive elliptic curve groups

Telex | Tag τ

- Telex station
 - Choose ECDH generators g_0, g_1 and private key r
 - Distribute public key $P \equiv (\alpha_0, \alpha_1) = (g_0^r, g_1^r)$ to clients
- Telex client initiates connection
 - Choose random $b \in \{0,1\}$ and private key s
 - Generate:
 - Public key $\beta = g_b^s$
 - Shared secret hash $h = H_{tag}(\alpha_b^s \parallel \chi)$
 - Tag $\tau \equiv \beta \parallel h$

Context string:
 $\chi \equiv ServerIp \parallel UnixTimestamp \parallel TlsSessionId$

Verification by station:
 $H_{tag}(\beta^r \parallel \chi) = h$

Telex | Shared secret key k_{sh}

- Telex station
 - Calculates 128-bit $H_{key}(\beta^r \parallel \chi)$
- Telex client
 - Calculates 128-bit $H_{key}(\alpha^s \parallel \chi)$

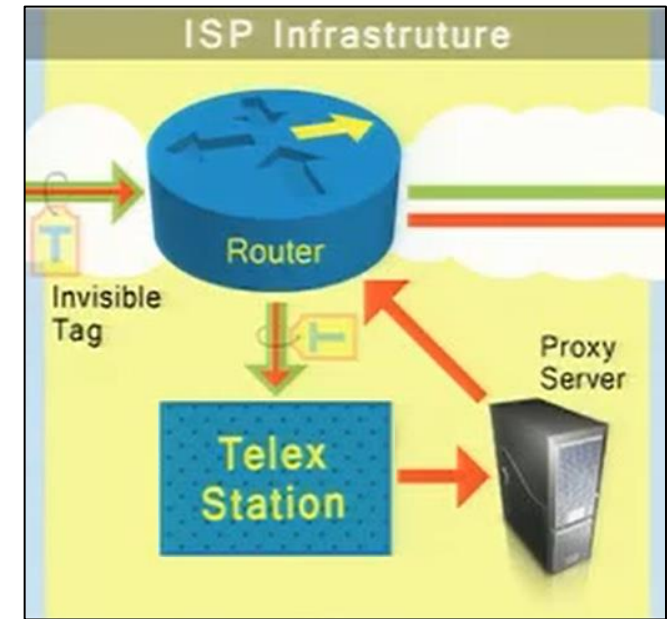
DH parameters:

- Station public, private key: α, r
- Client public, private key: β, s

Used as seed to PRNG for generating key exchange parameters, so that Telex station can hijack session.

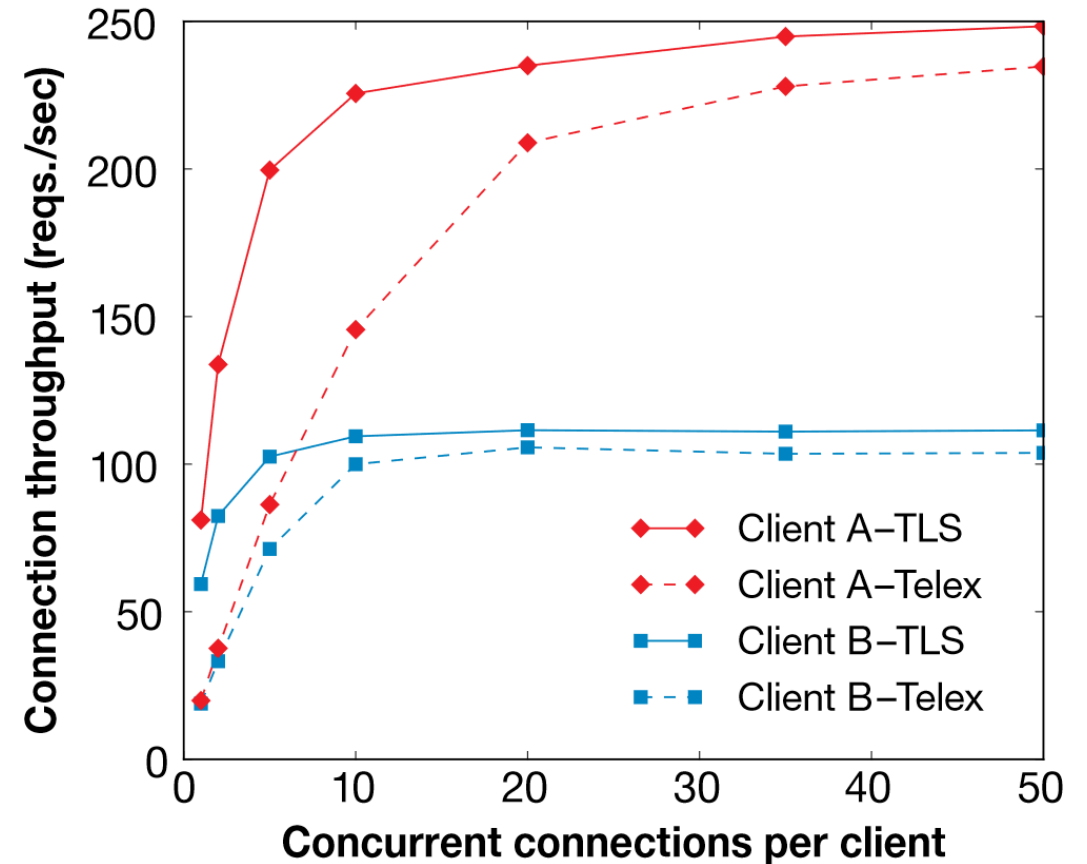
Telex | Implementation

- Router: Flow diversion
 - Linux iptables
- Telex station: TCP flow reconstruction + tag recognition
 - Bro IDS, with addition of ECDH code
 - Checks 11k tags/s/core on 3GHz Intel Core 2 Duo
- Proxy server: Shunt data from client TLS connection
 - Kernel module



Evaluation | Performance

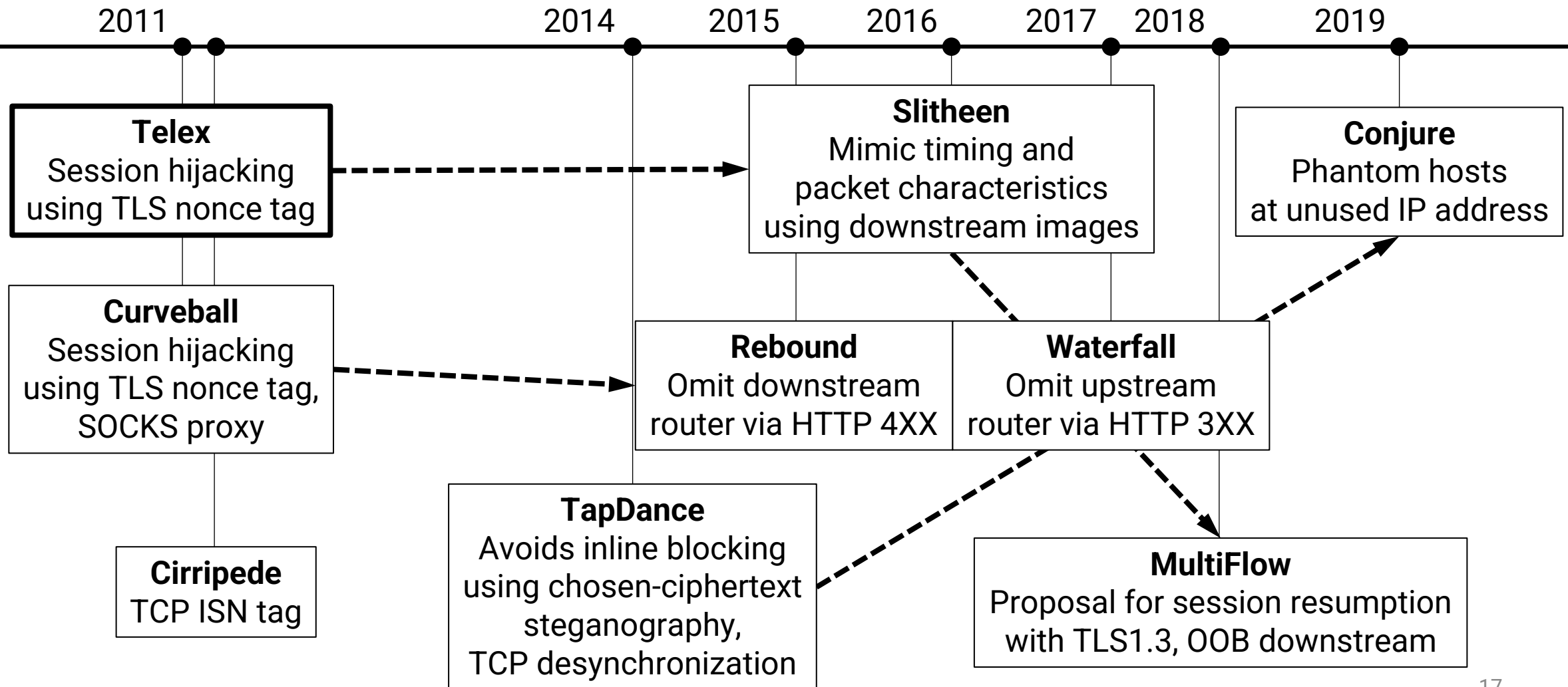
- Lab testing:
 - CPU-bound at high concurrency
 - Network-bound at low concurrency
 - HTTP used by proxy instead of HTTPS
- Beta testing:
 - PlanetLab node in Beijing
 - Median latency overhead of 60% for Alexa top 100 websites




Evaluation | Problems

- Susceptible to DoS of Telex stations
 - Flooding of ClientHello requests
 - Routing Around Decoy (RAD) attack: discard upstream BGP routes through known decoy AS
- Susceptible to traffic analysis
 - Detection of anomalous connections, e.g., censor-controlled decoys
 - Deviations from server behaviour (e.g. IP/TCP/TLS)
- Only symmetric routes supported

Follow-up | Protocol zoo



Follow-up | ISP-scale deployment

- TapDance over Psiphon network 
 - Reasonable performance: 100 Kbps/user, total 500 Mbps
 - Low decoy impact: ~10 MB/day per site, up to 160k connections/day
 - High costs: \$30k per deployment site, \$37k/year deployment costs
- Biggest bottleneck is ISP onboarding
 - Possible retaliation attacks
 - Lack of direct customer-ISP relationships
- Routing optimization: Half of clients fail to pass through station

Suppl. | Security argument

$$\tau = \beta \parallel h$$

1. Adv. cannot distinguish β from uniform distribution of l_p bits
 - β represents an x -coordinate, which can only fall under one category:
(1) E over \mathbb{F}_p , (2) E' over \mathbb{F}_p , (3) invalid $> p$ (small %)
2. Adv. cannot distinguish correct $H_{tag}(\beta^r \parallel \chi)$ from β
 - Essentially decisional DDH assumption
 - Requires minimum of 2^{l_p} computations

Suppl. | Only x-coordinate needed in ECC

Law of quadratic reciprocity: If z is a quadratic residue, i.e.,

$\exists y$ s.t. $y^2 = z \bmod p$, then

$$z^{\left(\frac{p-1}{2}\right)} = 1 \bmod p$$

Let $z = (x^3 - 3x + b) \bmod p$, and $p = 3 \bmod 4$, then using Euler's criterion. We can verify

$$y = \pm z^{\left(\frac{p+1}{4}\right)}$$

$$y^2 = z^{\left(\frac{p+1}{2}\right)} = z \cdot z^{\left(\frac{p-1}{2}\right)} = z \bmod p$$

Standard ECC implementation to use point compression.

Suppl. | ECC domain parameter constraints

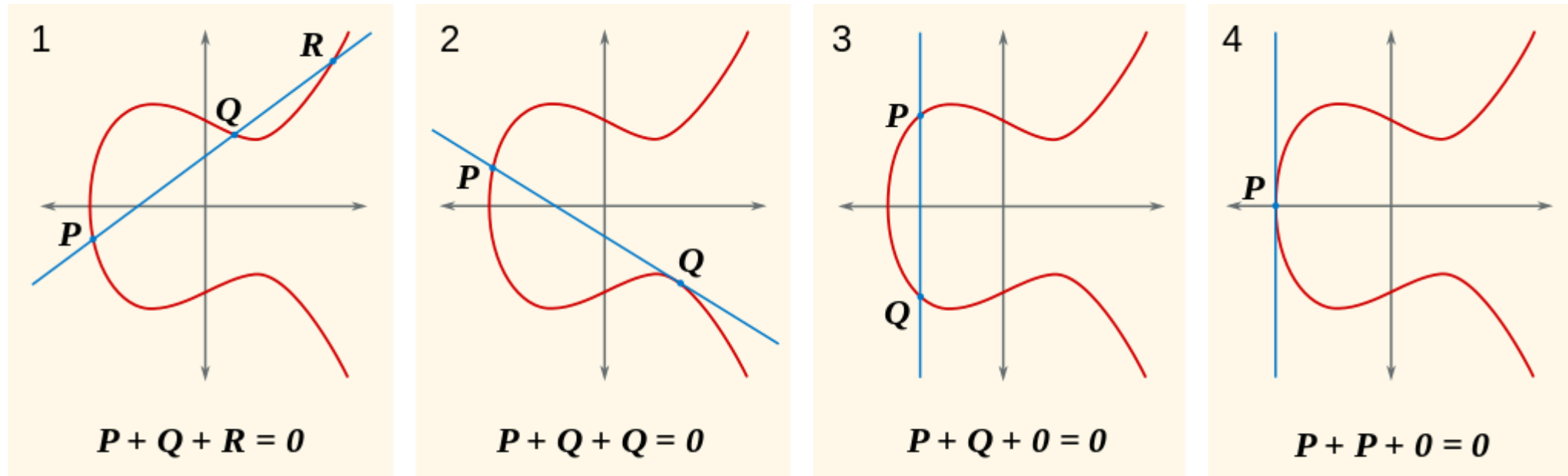
- Elliptic curve E over field of prime order p
 - Define such points with equation $y^2 = x^3 - 3x + b \bmod p$
 - IEEE-P1363 suggests this curve shape may provide the fastest arithmetic
 - Special choice of p :
 - **Choose odd prime p** \Rightarrow exactly half of non-zero elements are quadratic residues, i.e., solutions lie on E (Euler's criterion)
 - **Choose $p \equiv 3 \bmod 4$** \Rightarrow negative of all quadratic non-residues are quadratic residues, i.e., solutions that do not lie on E instead lie on E' : $-y^2 = x^3 - 3x + b \bmod p$ (Law of Quadratic Reciprocity, first supplement)
 - **Choose p near power of 2** \Rightarrow small number of invalid tags with $(x \bmod p)$
 - b selected such that both curves E and E' have prime orders

Suppl. | ECC domain parameter selection

- Domain parameters:
 - $p = 2^{168} - 2^8 - 1$
 - $E: y^2 = x^3 - 3x + b$
 - $b = 114301813541519167821195403070898020343878856329174$
 - $g_0 = 2, \quad g_1 = 0$
 - $H_{tag}(x) = \text{SHA-256}(x)[55:0]$
 - $H_{key}(x) = \text{SHA-256}(x)[255:128]$

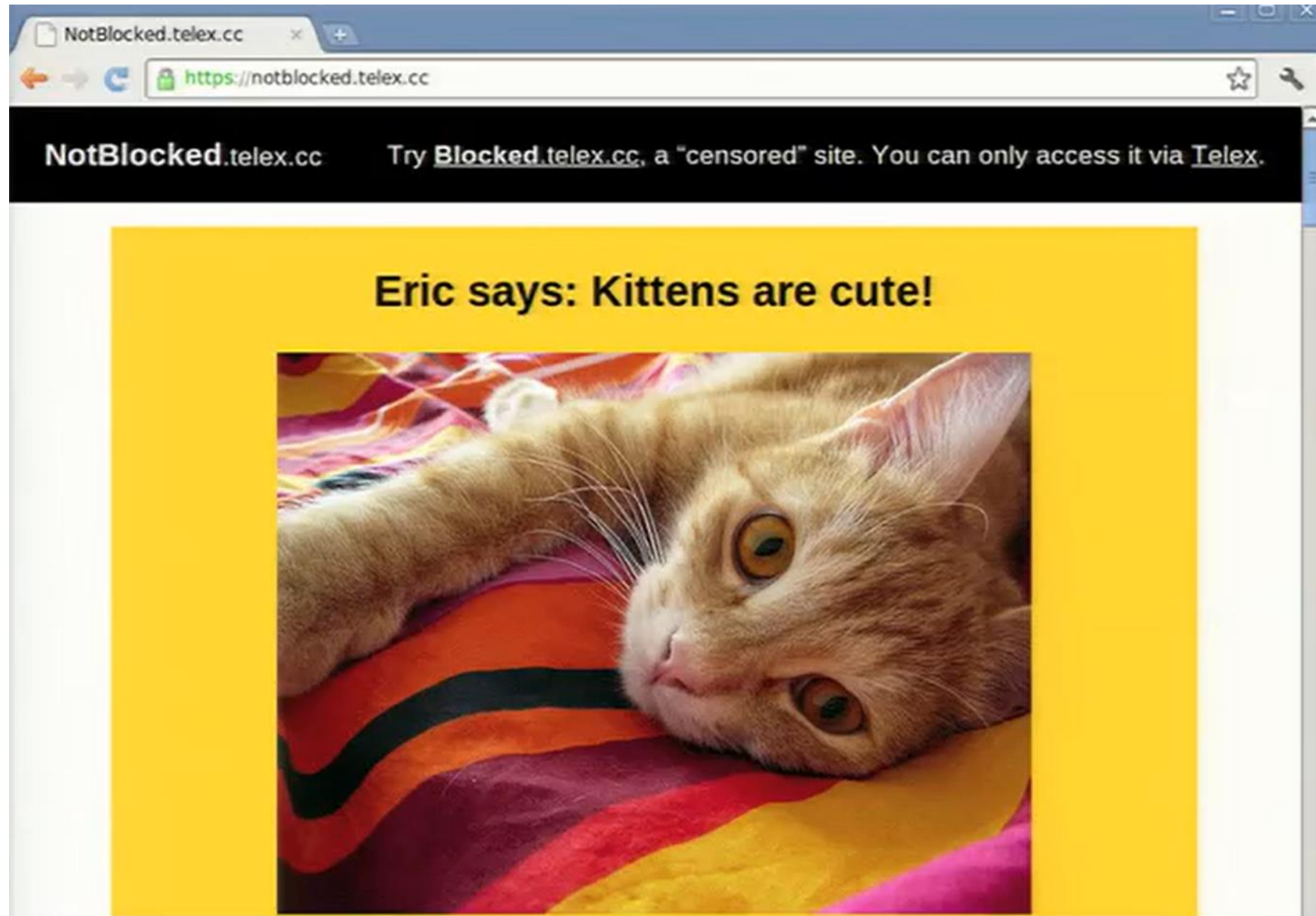
Fraction of nonces known to *not* be tags: $\left(\frac{2^8+1}{2^{168}}\right) \approx 2^{-160} = 10^{-48}$

Suppl. | Elliptic-curve addition



Suppl. | Vulnerability of $p \sim 2^k$?

- Can be exploited by index calculus algorithm, in the context of DLP
 - Relies on choice of an efficient “factor base” related to the primitive element of multiplicative groups
- Since all non-identity elements in an elliptic curve group are generators, there is no such notion of primitive elements
 - i.e., not necessarily exploitable for ECDLP



Evaluation | Client accesses



Evaluation | Bandwidth

