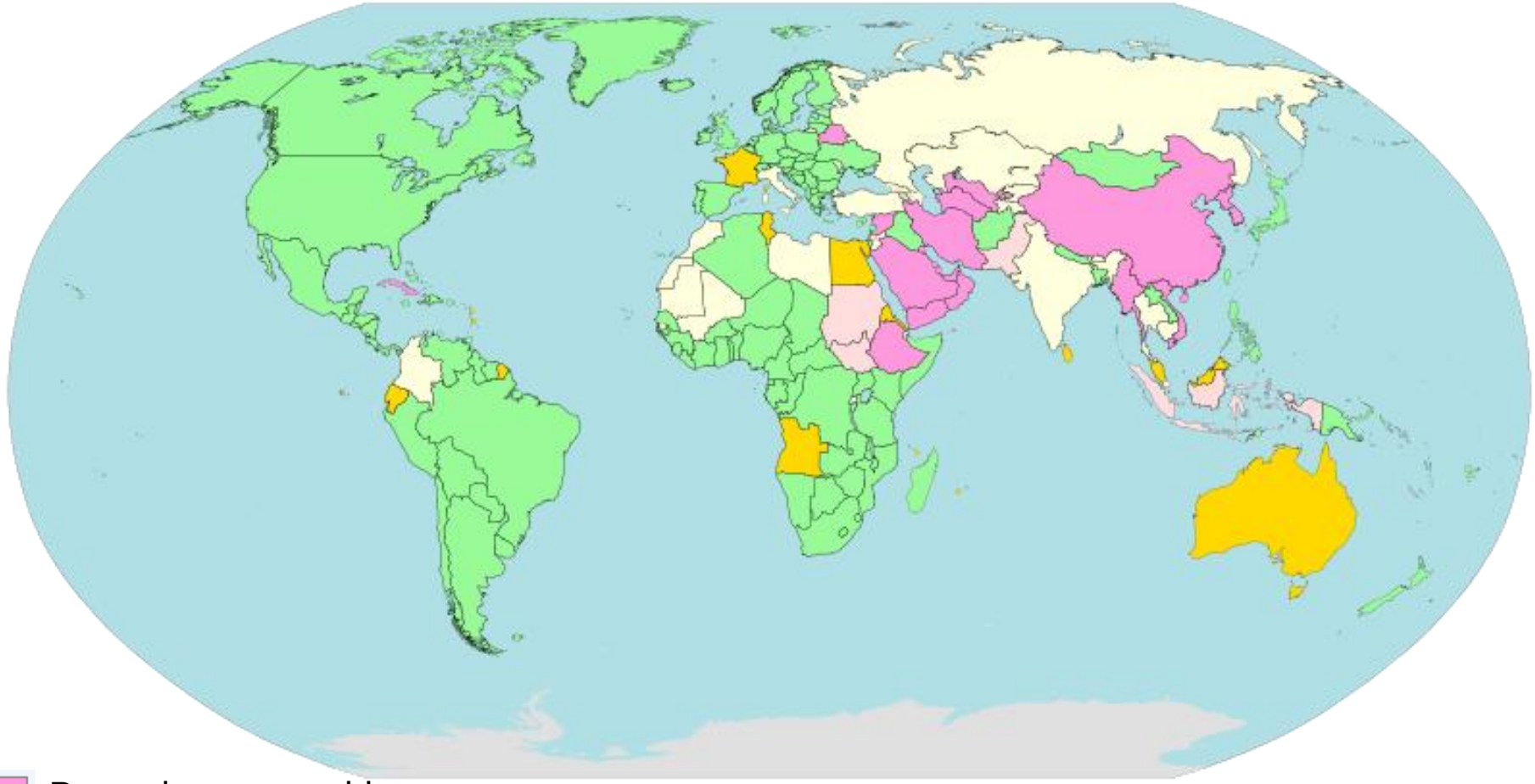
TapDance: End-to-Middle Anticensorship without Flow Blocking

Eric Wustrow
Colleen M. Swanson
J. Alex Halderman
University of Michigan

Internet Censorship



- Pervasive censorship
- Substantial censorship
- Selective censorship
- Changing situation
- Little or no censorship

End-to-Middle Proxies

Telex: Anticensorship in the Network Infrastructure

Eric Wustrow, Scott Wolchok, Ian Goldberg, J. Alex Halderman

USENIX SEC 2011

Decoy Routing: Toward Unblockable Internet Communication

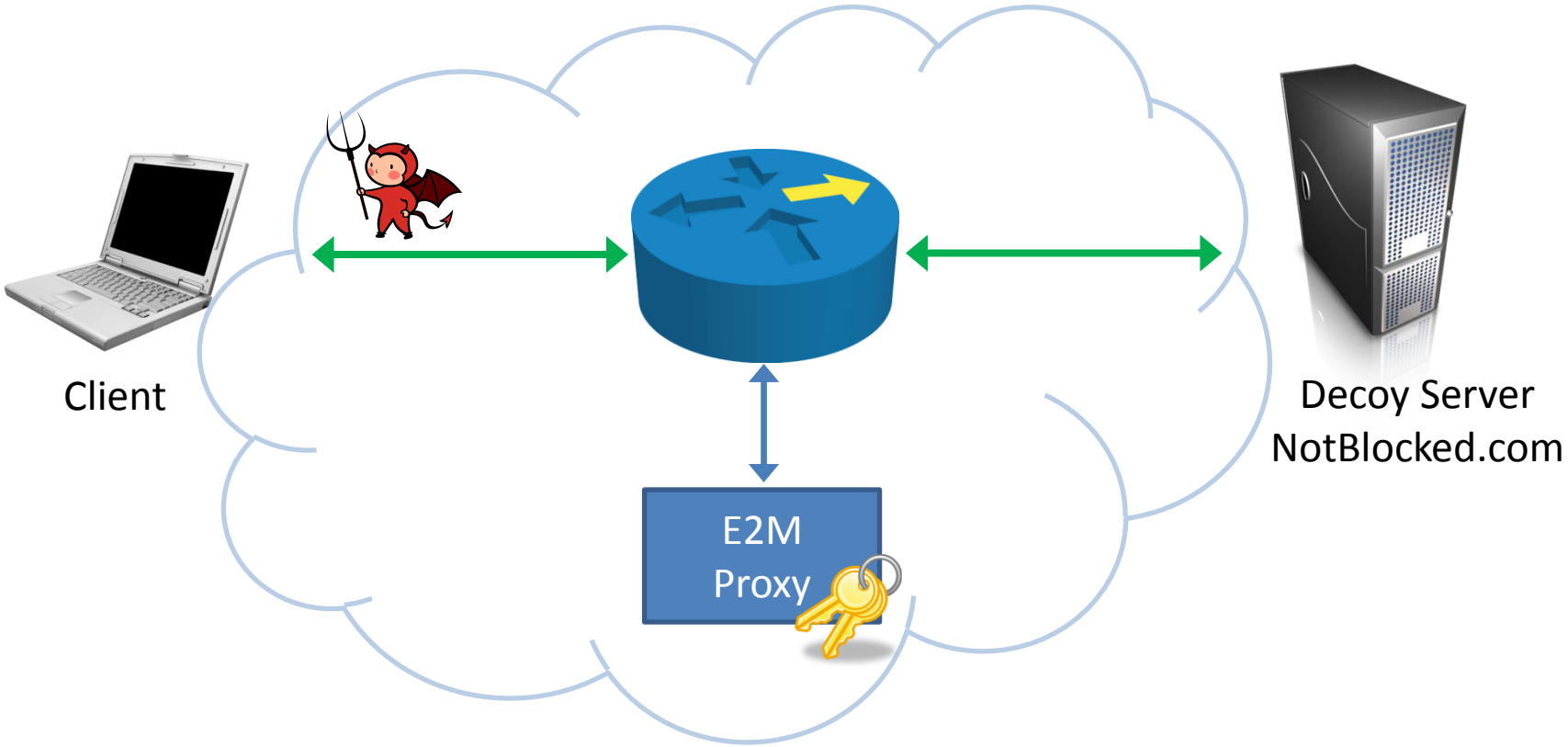
Josh Karlin, Daniel Ellard, Alden W. Jackson, Christine E. Jones,
Greg Lauer, David P. Mankins, W. Timothy Strayer
FOCI 2011

Cirripede: Circumvention Infrastructure using Router Redirection with Plausible Deniability

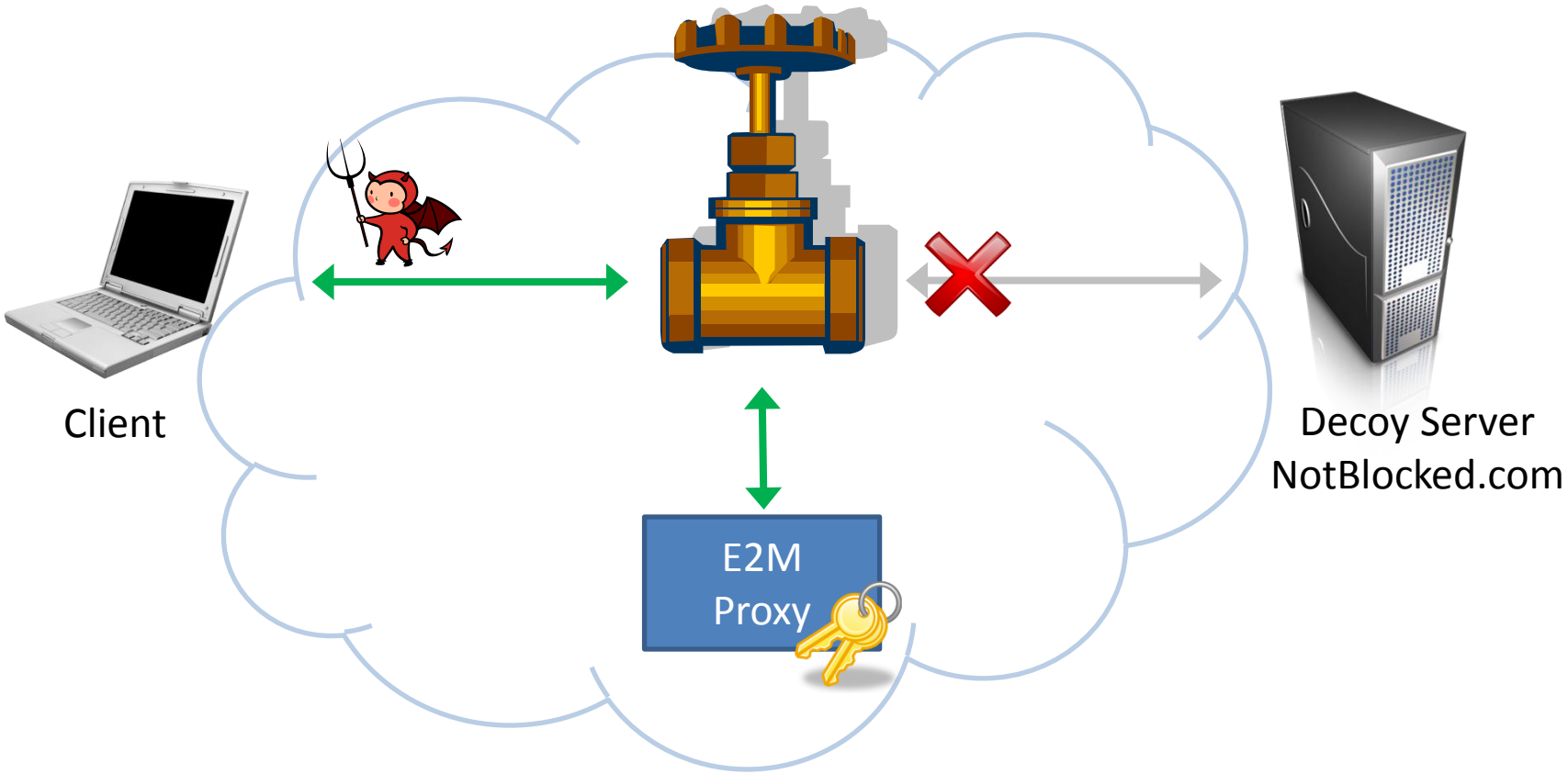
Amir Houmansadr, Giang T. K. Nguyen, Matthew Caesar, Nikita Borisov

CCS 2011

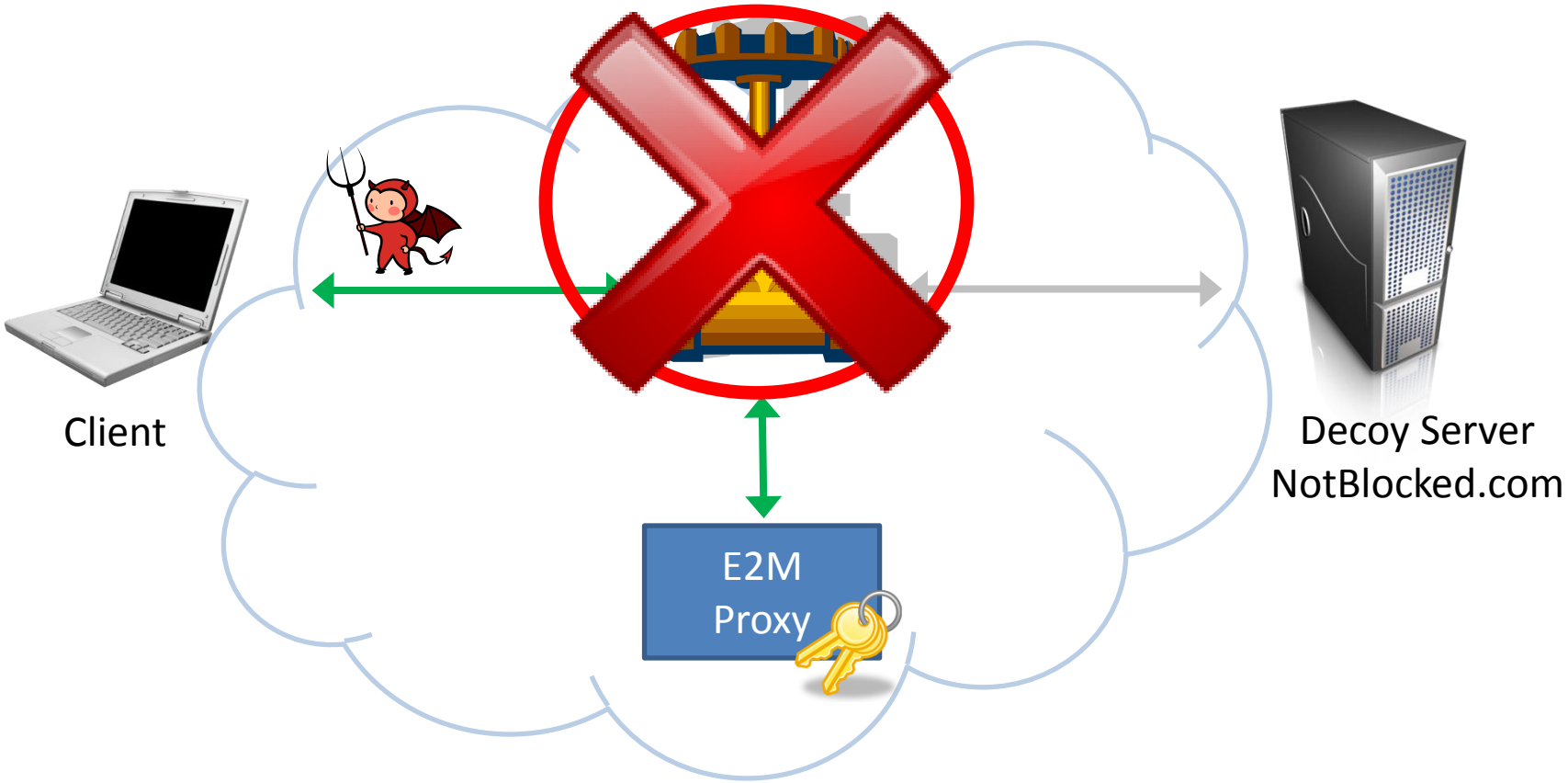
End-to-Middle Proxies



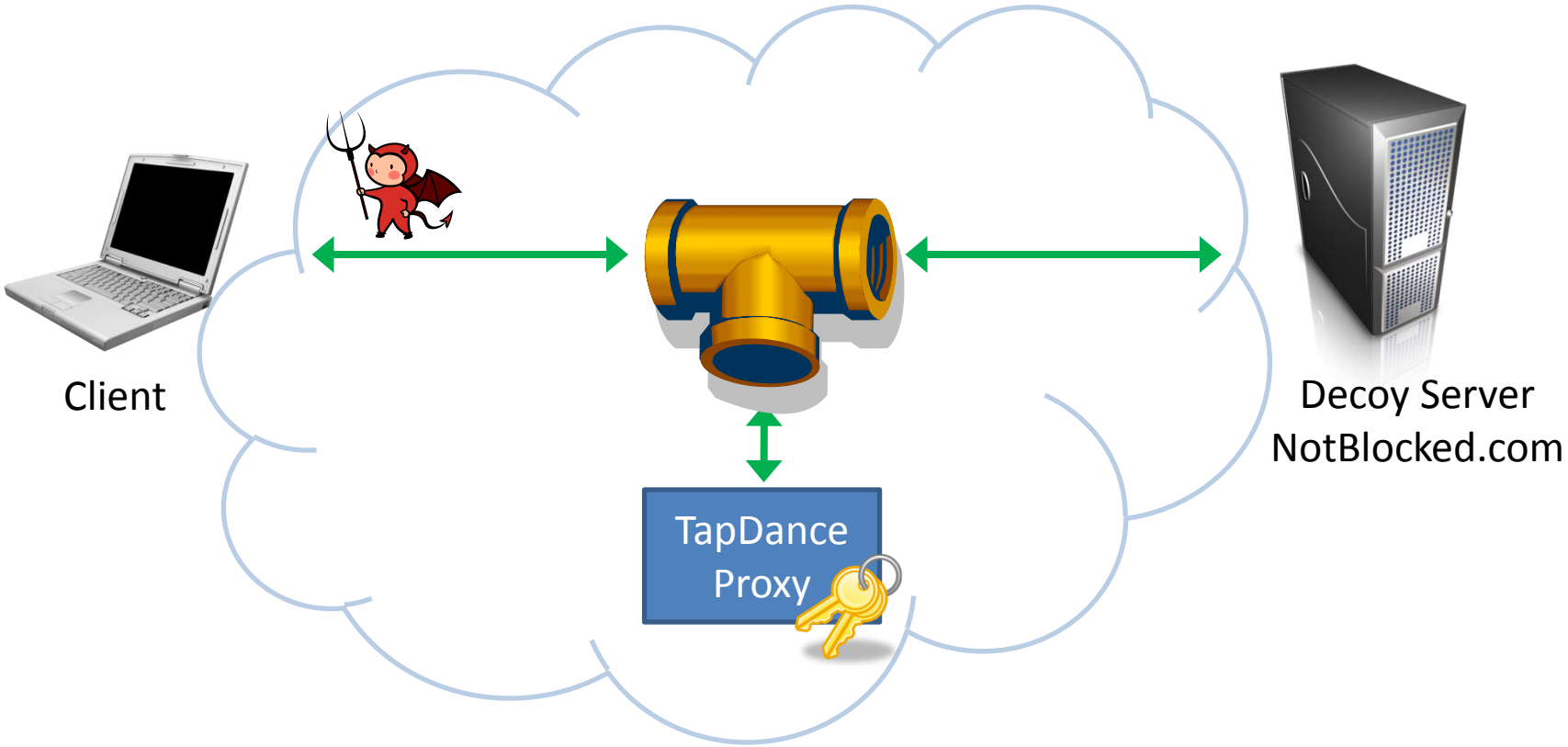
End-to-Middle Proxies



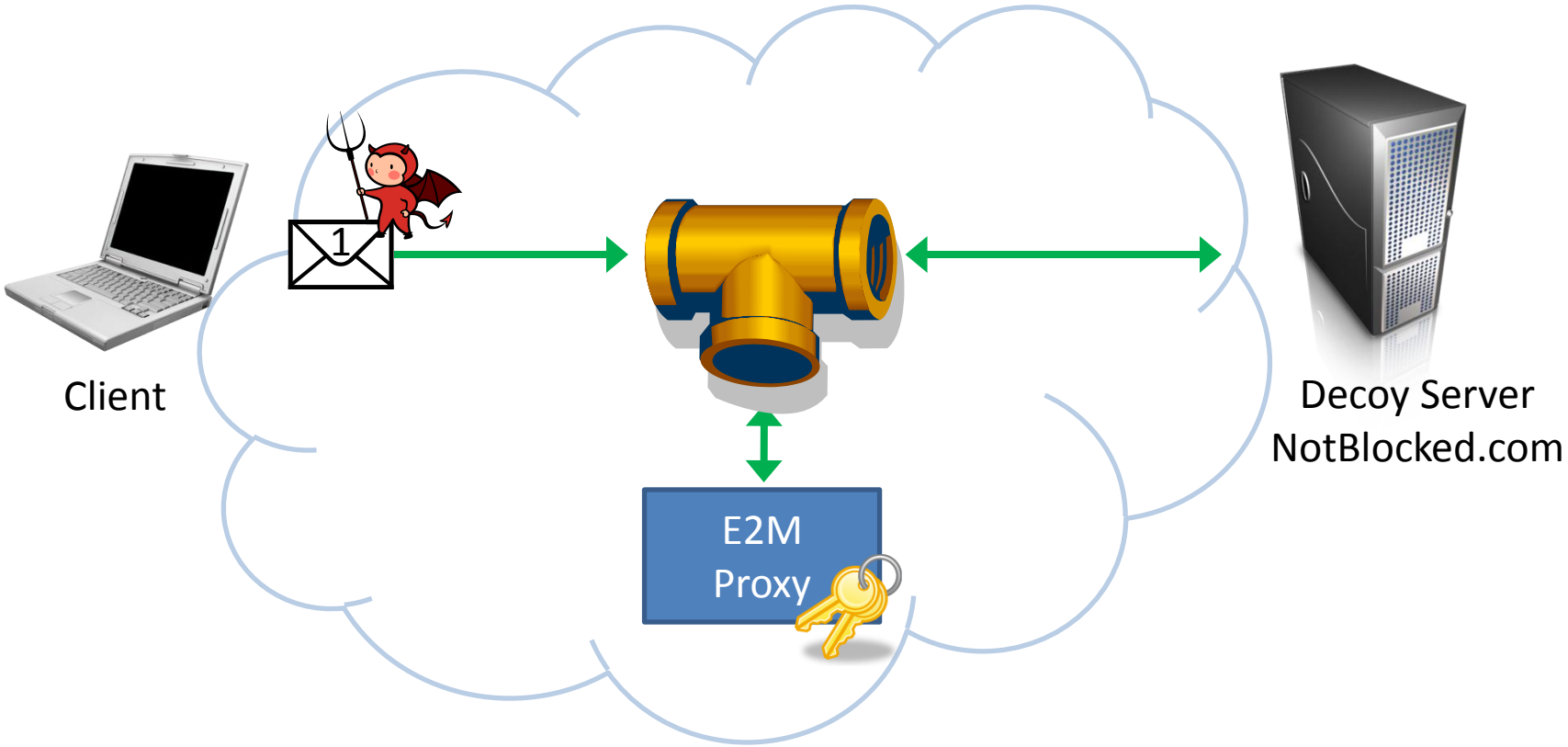
End-to-Middle Proxies



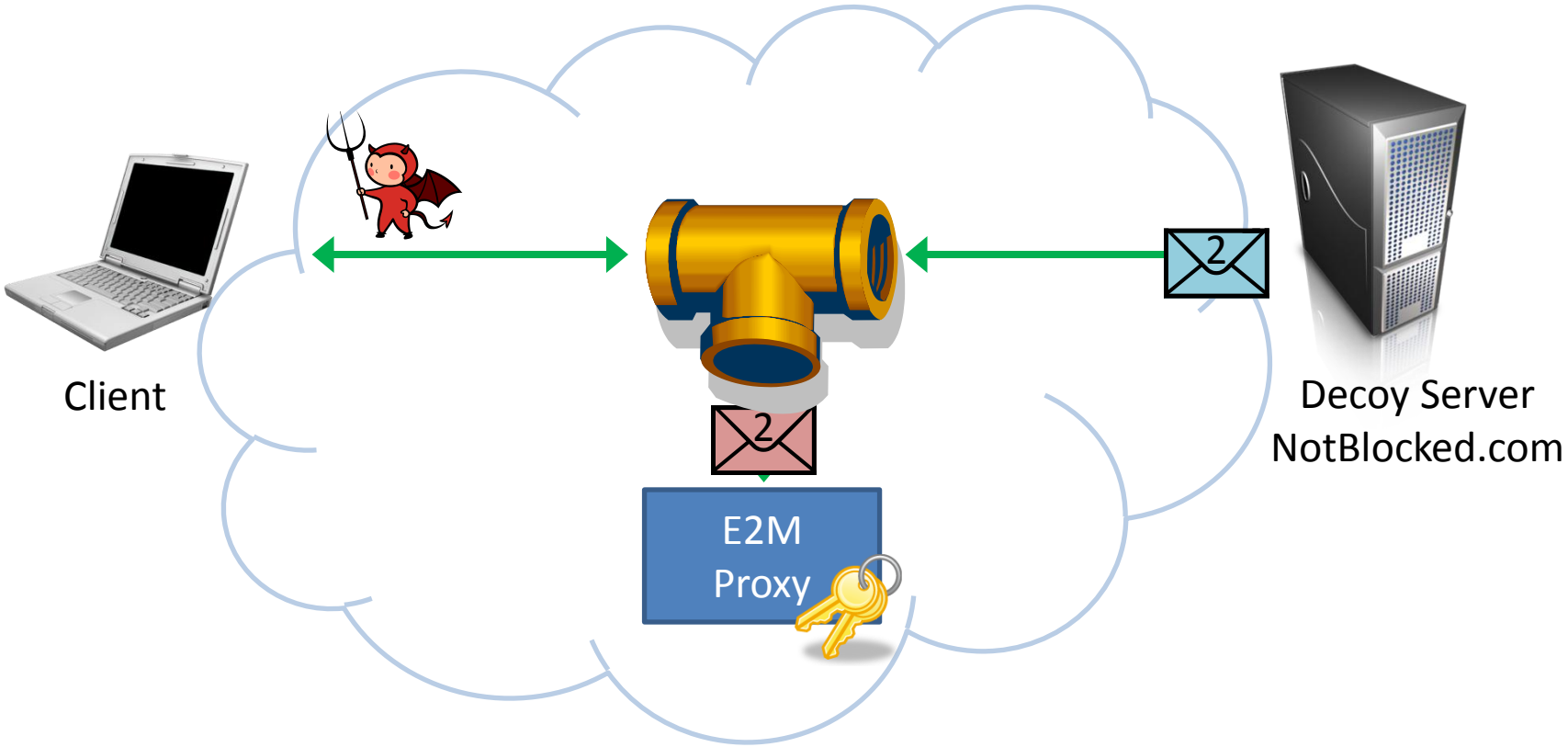
TapDance: End-to-Middle Anticensorship without Flow Blocking



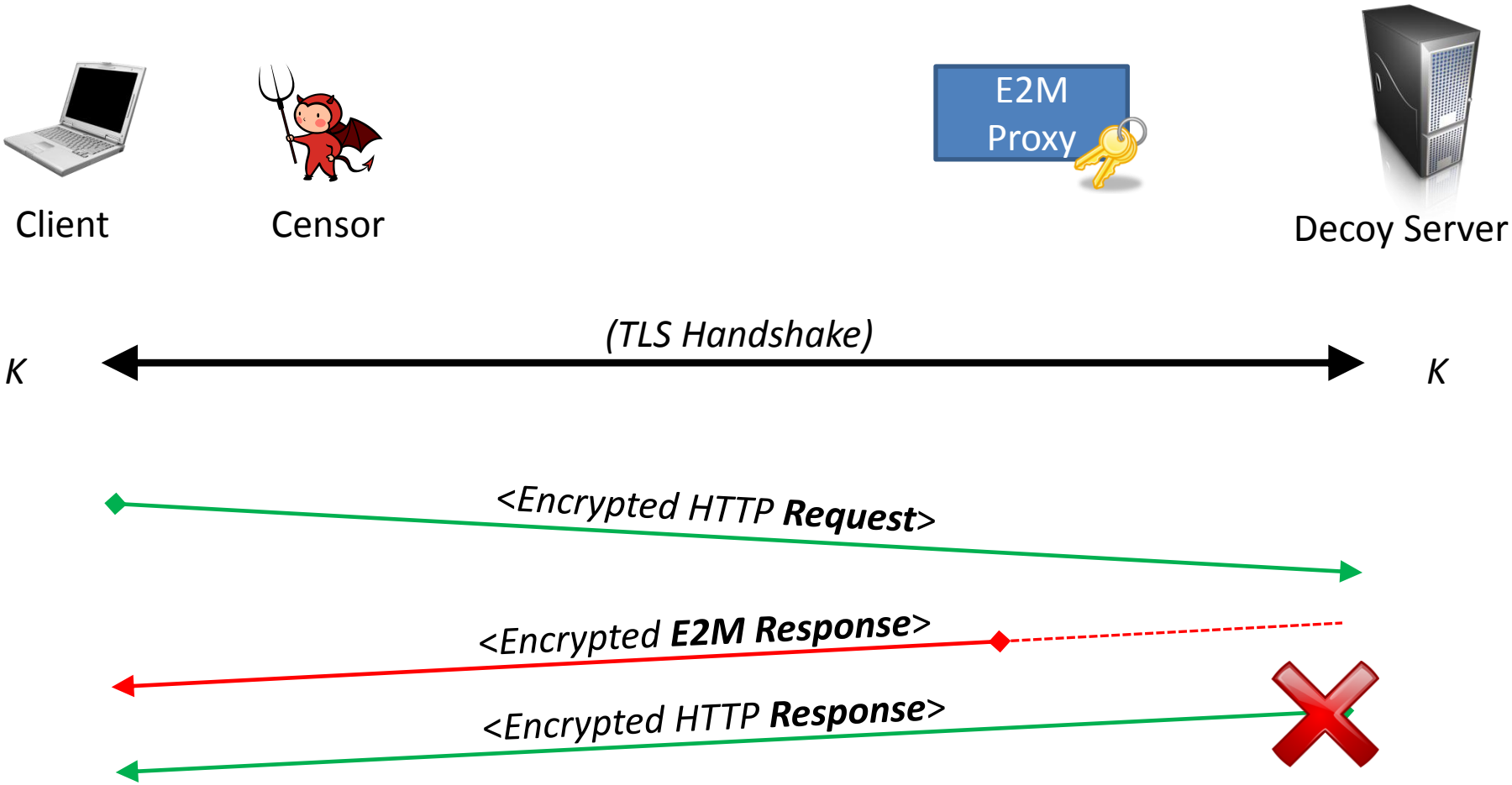
Passive Tap Challenges



Passive Tap Challenges



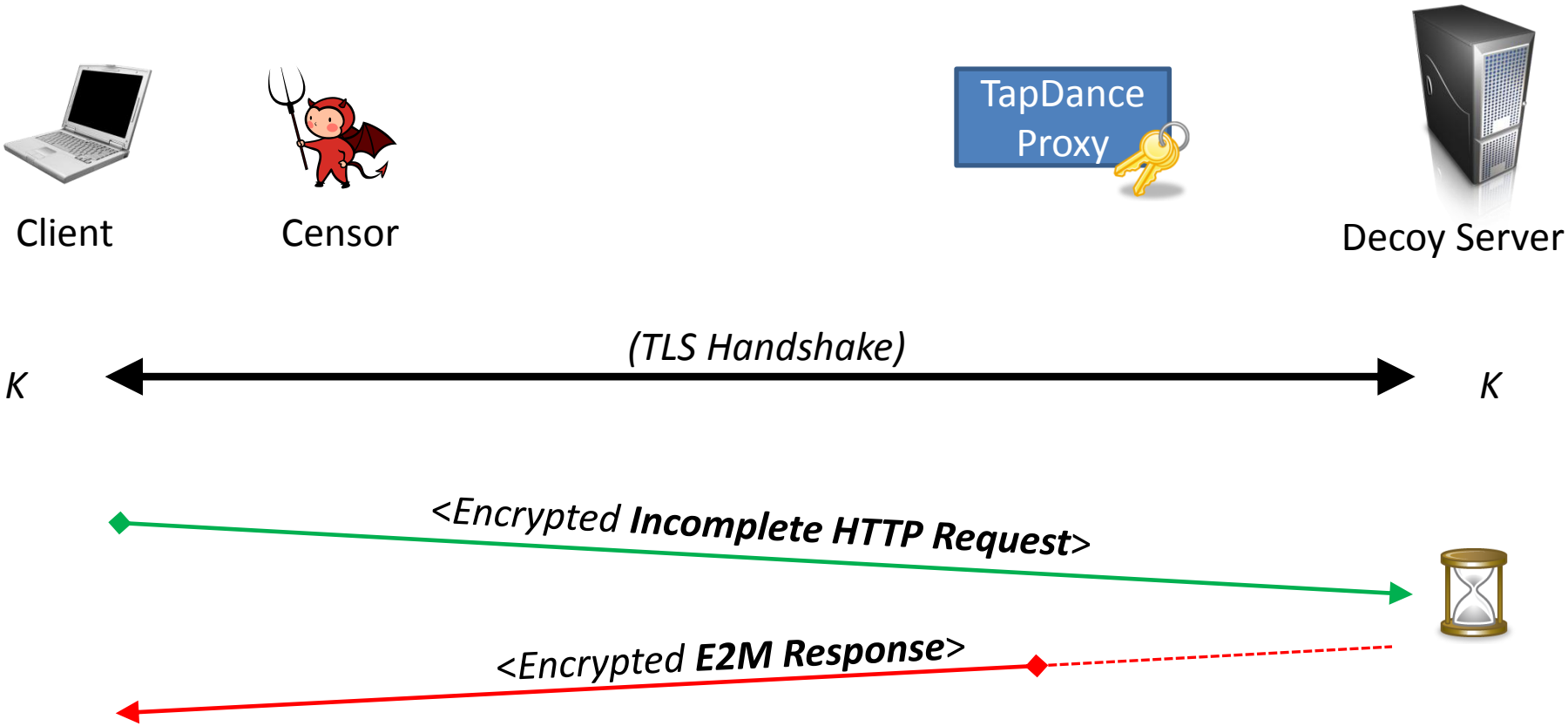
Passive Tap Challenge: **Duplicate Data**



Incomplete HTTP request example

```
GET / HTTP/1.1\r\n
Host: www.site.com\r\n
X-Ignore: AAAAAAAAAAA…\r\n
```

Incomplete HTTP Request



Passive Tap Challenge: **Inconsistent TCP**

Client

Censor

Decoy Server

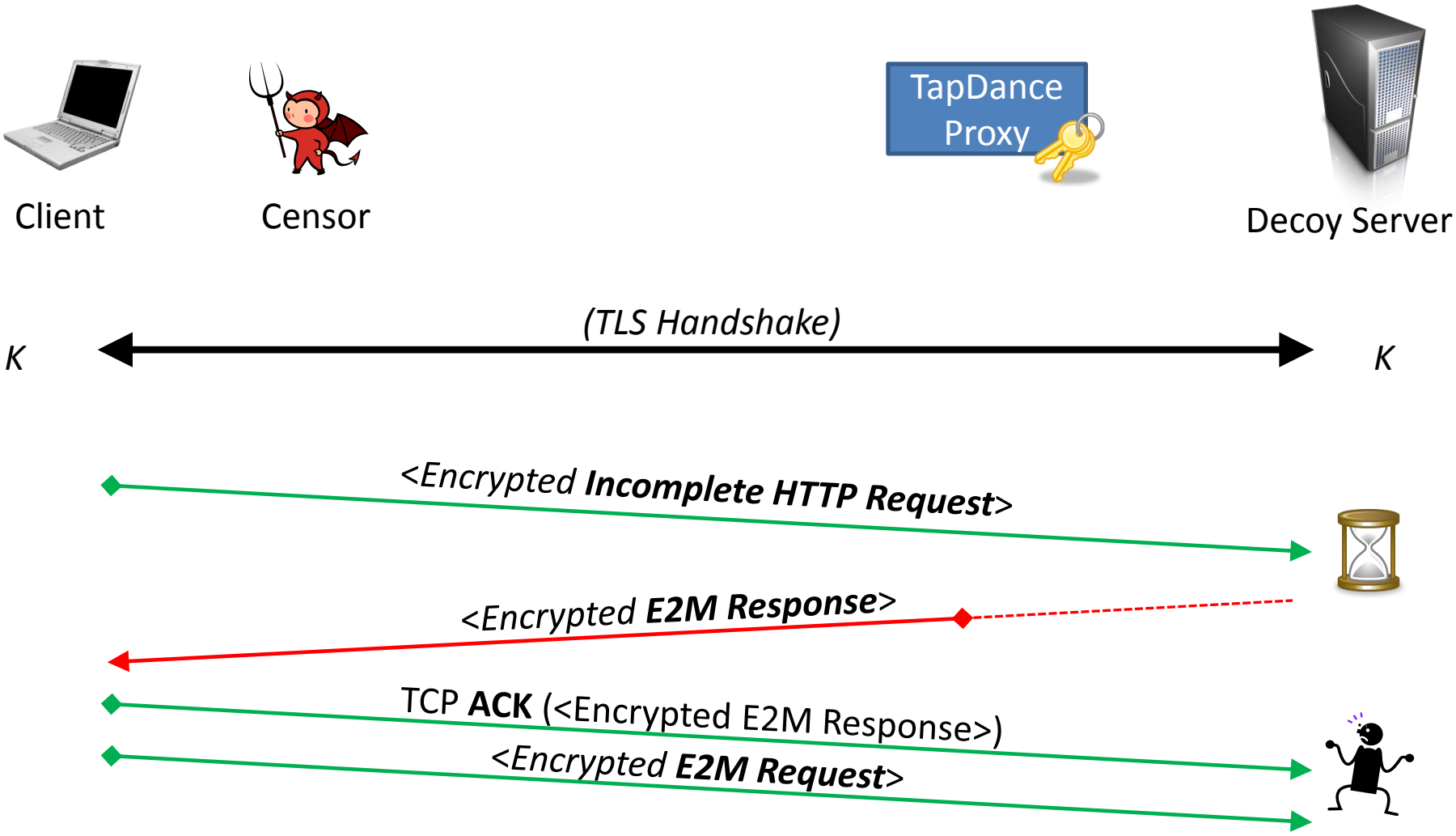
K ← *(TLS Handshake)* → *K*

*<Encrypted **Incomplete HTTP Request**>*

*<Encrypted **E2M Response**>*

TCP **ACK** (<Encrypted E2M Response>)

Passive Tap Challenge: **Inconsistent TCP**



Tagging Methods

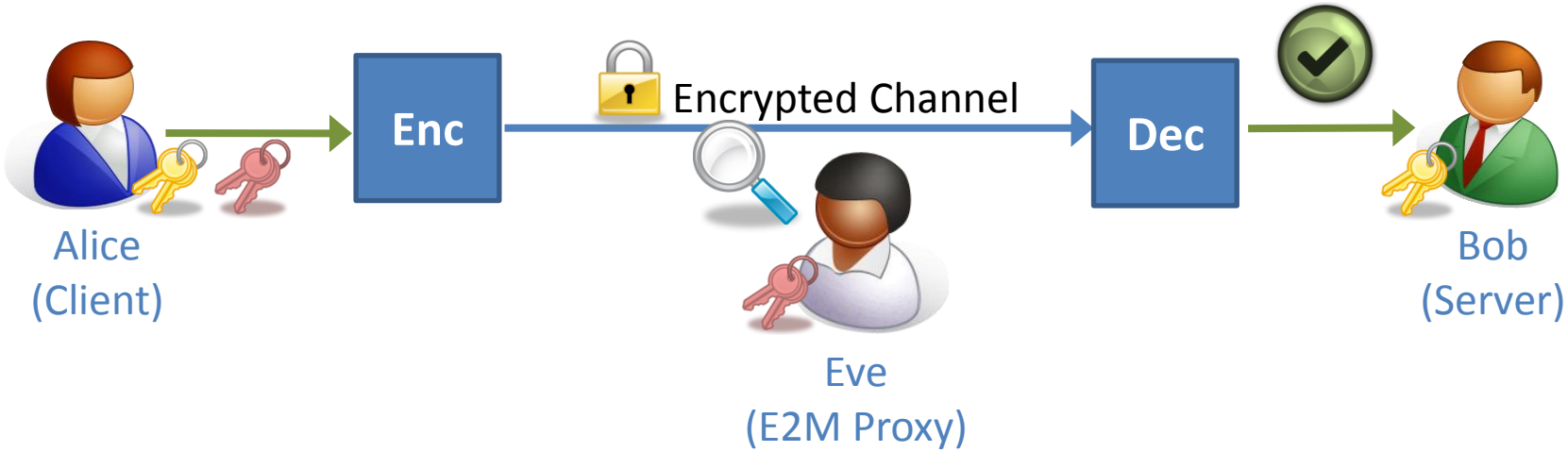
Telex: 28-byte *TLS ClientRandom*

Decoy Routing: 28-byte *TLS ClientRandom*

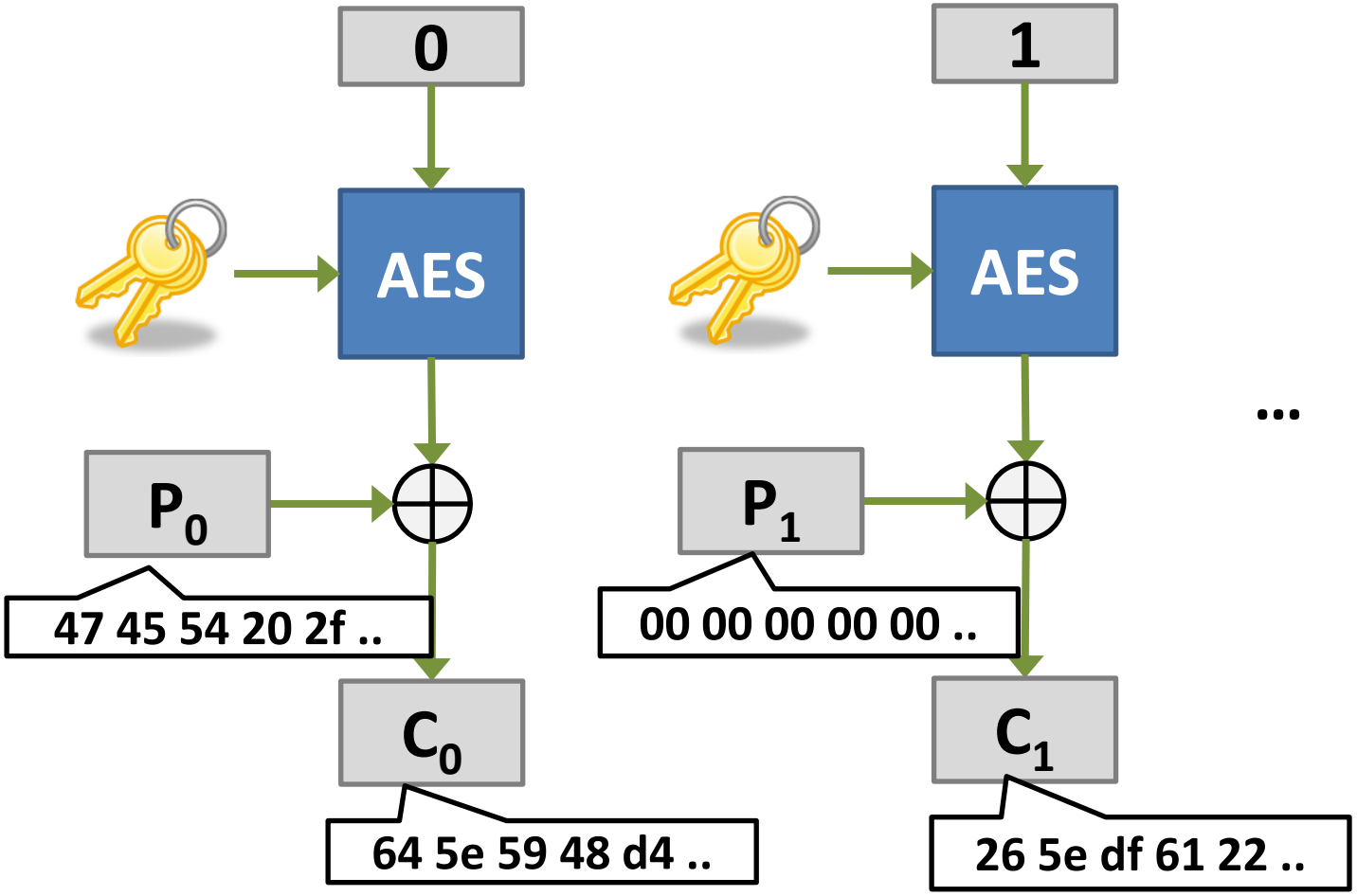
Cirripede: Successive (3-byte) *TCP ISN*s

TapDance: Arbitrary-length *TLS* ***Ciphertext***

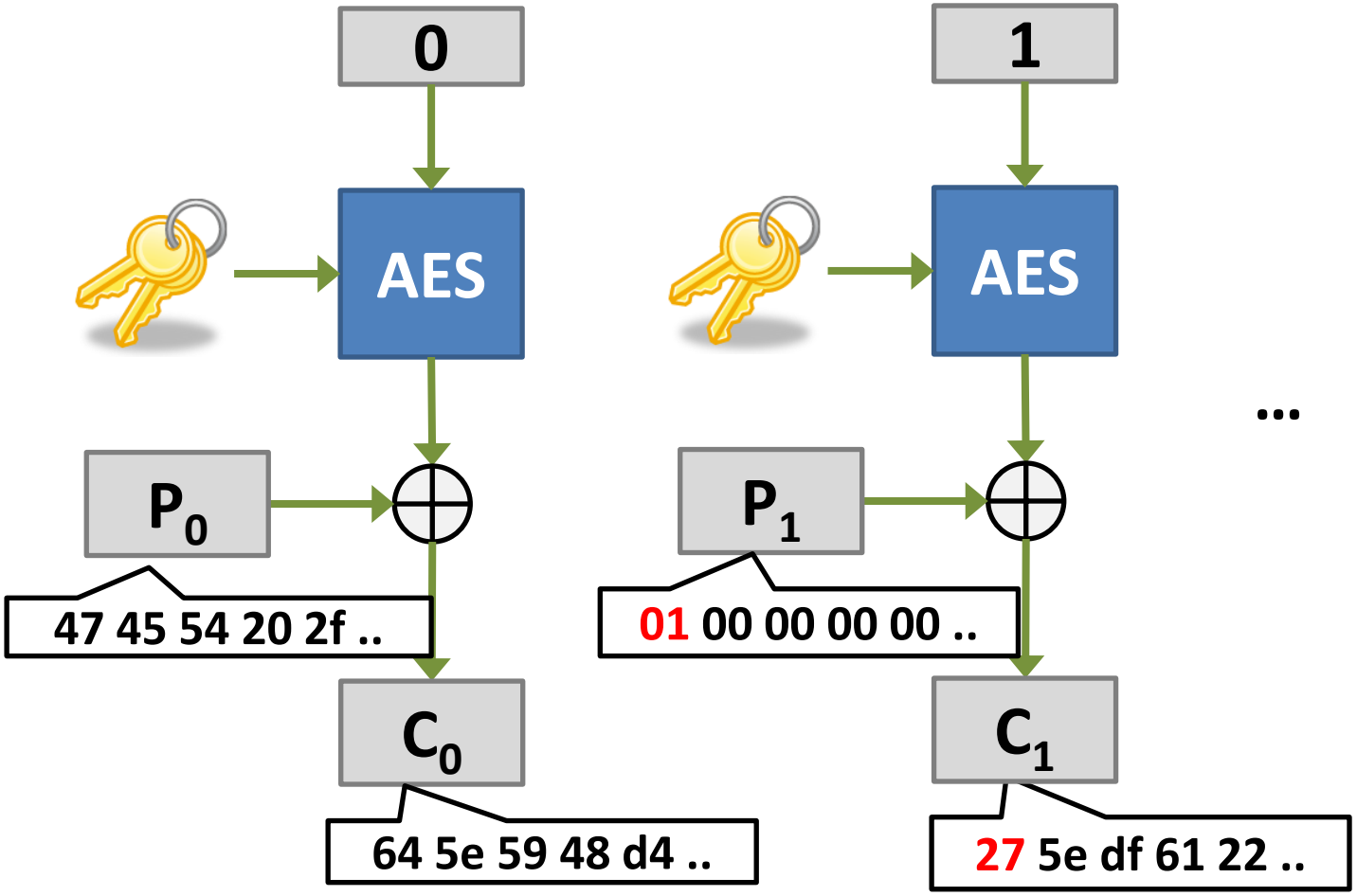
Chosen-Ciphertext Covert Channel



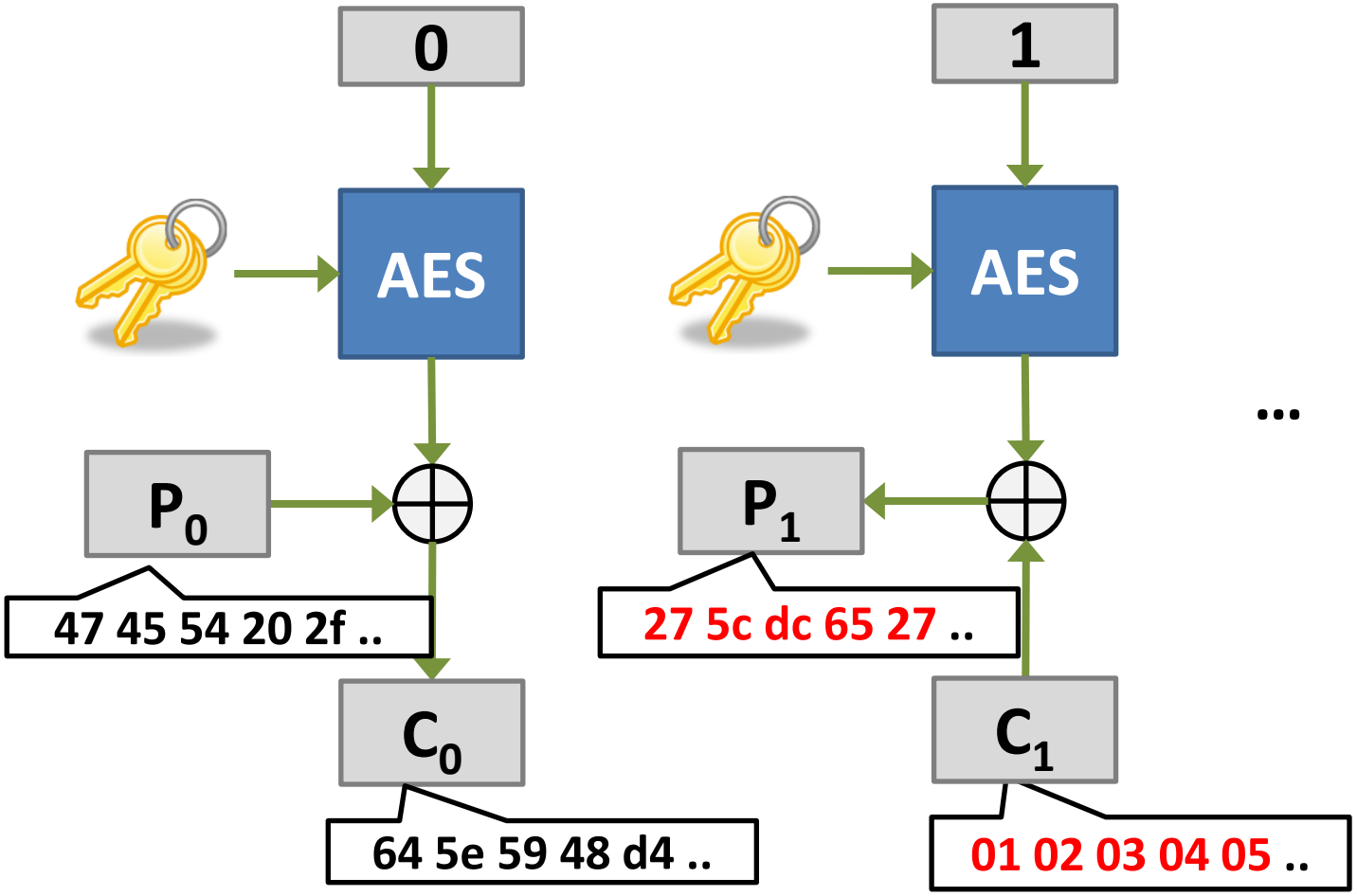
Stream cipher ciphertext channel



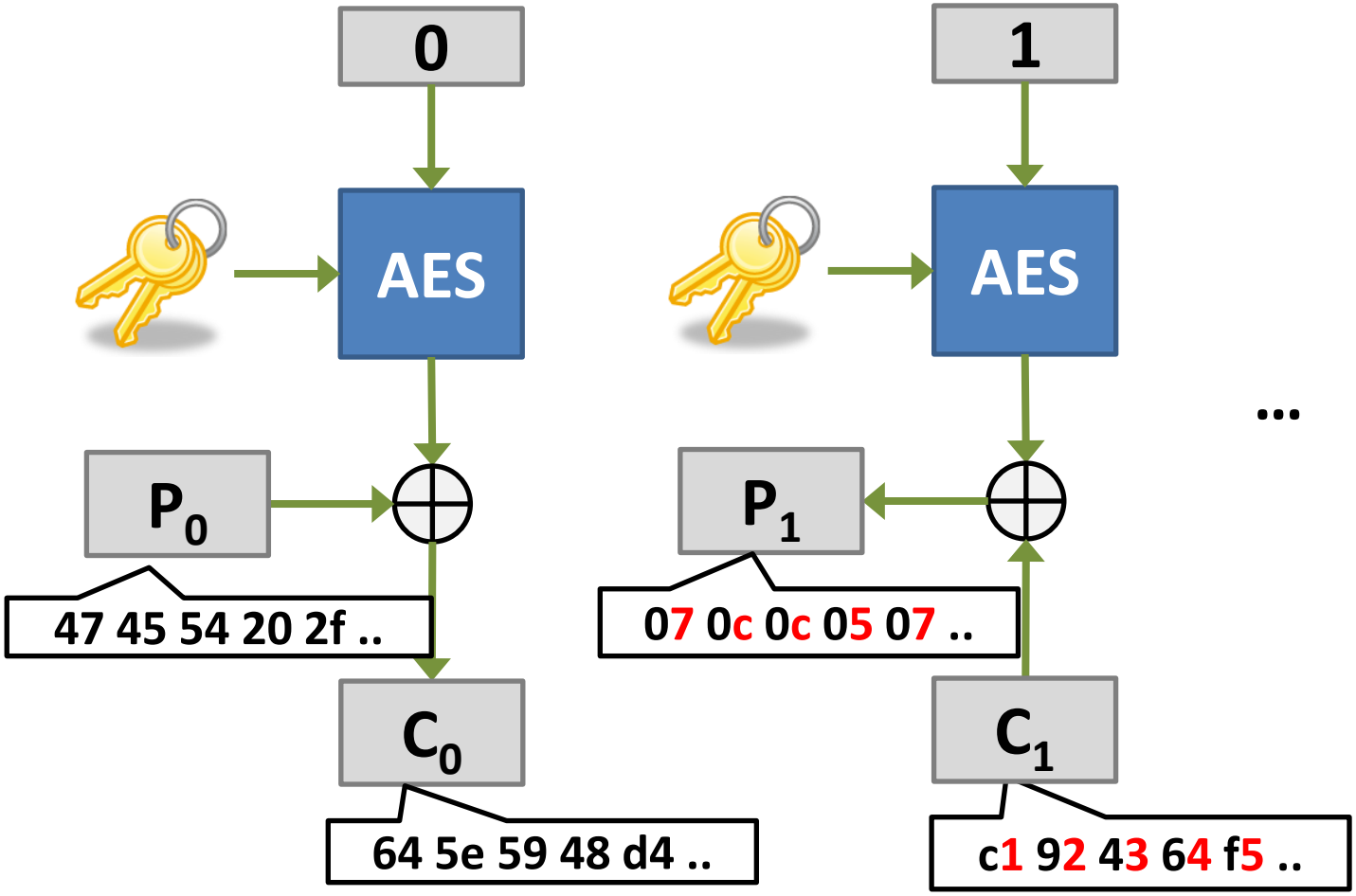
Stream cipher ciphertext channel



Stream cipher ciphertext channel



Stream cipher ciphertext channel

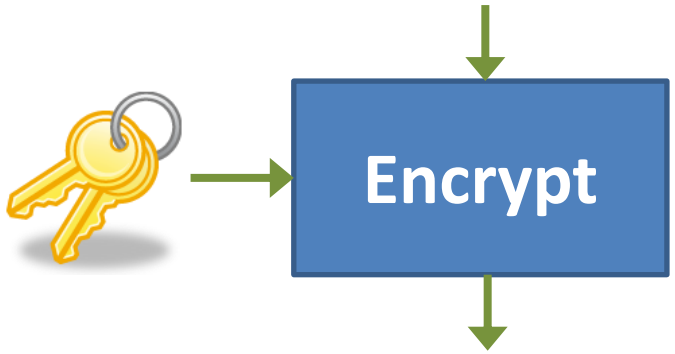


Incomplete HTTP request example

GET / HTTP/1.1\r\n

Host: www.site.com\r\n

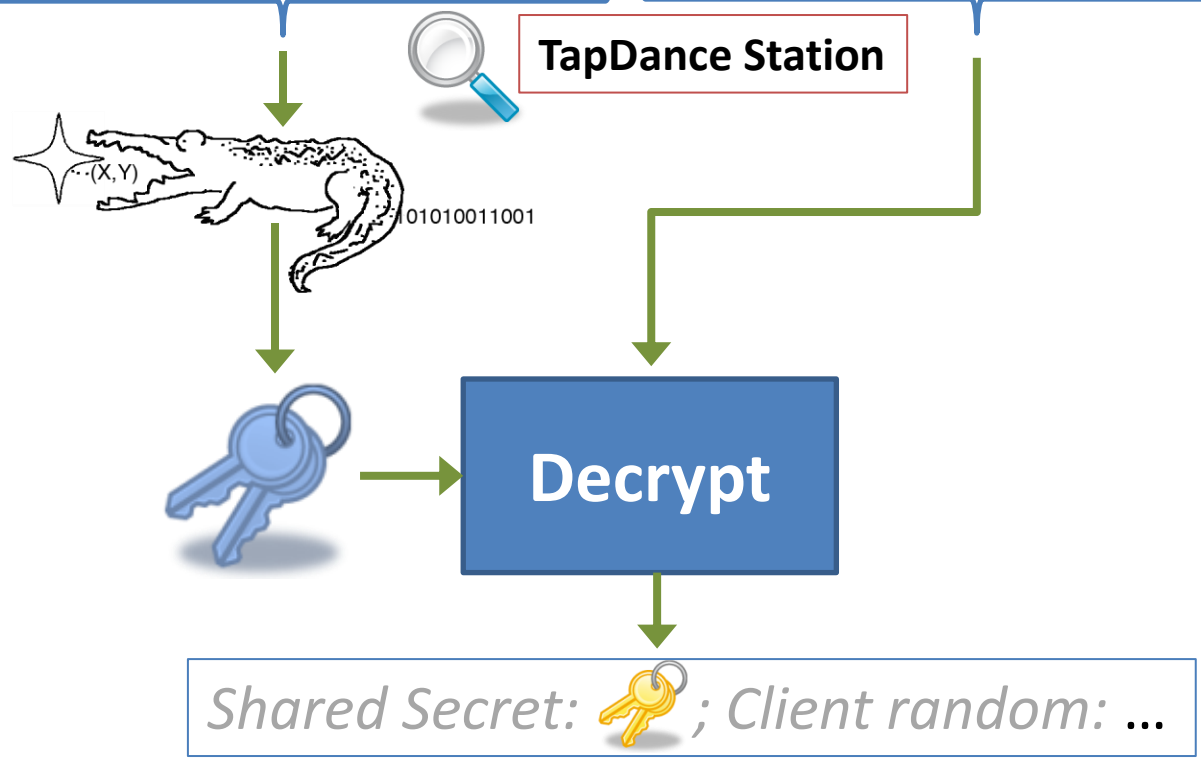
X-Ignore: u]DhsYGxVxEvuZEhESta…\r\n



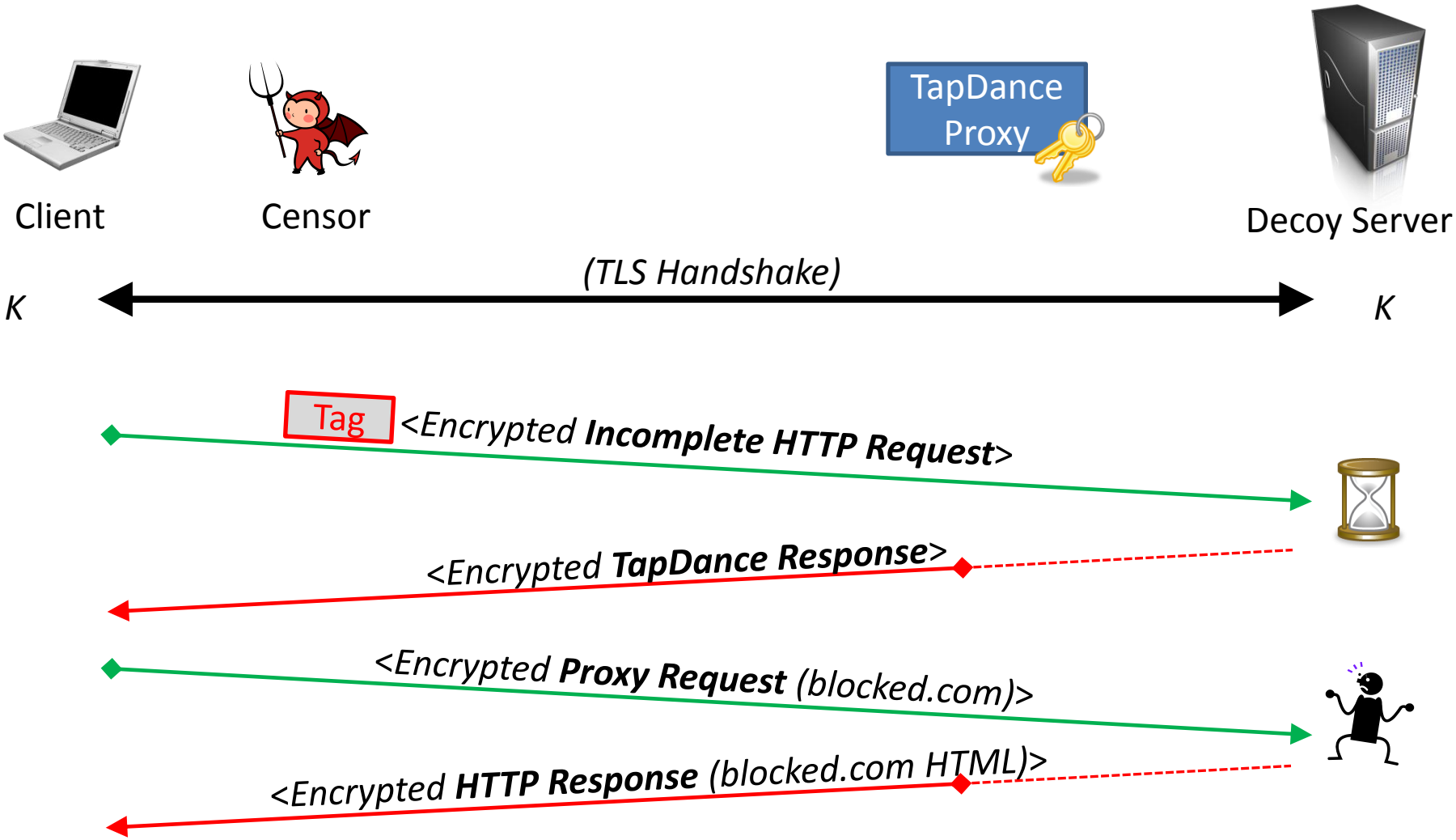
\x1e\x91\xb2\xce\x94\x8a\x6b\x3c\x78\x8c\x6f\x03
\x5e\xef\x97\x34\xf1\x2e\xc6\xe6\x7f\x10\xc8\x46
\xf9\x25\x6a\x0c\xff\x6d\x38 … \x70\xd7\x2c\x63 …

Incomplete HTTP request example

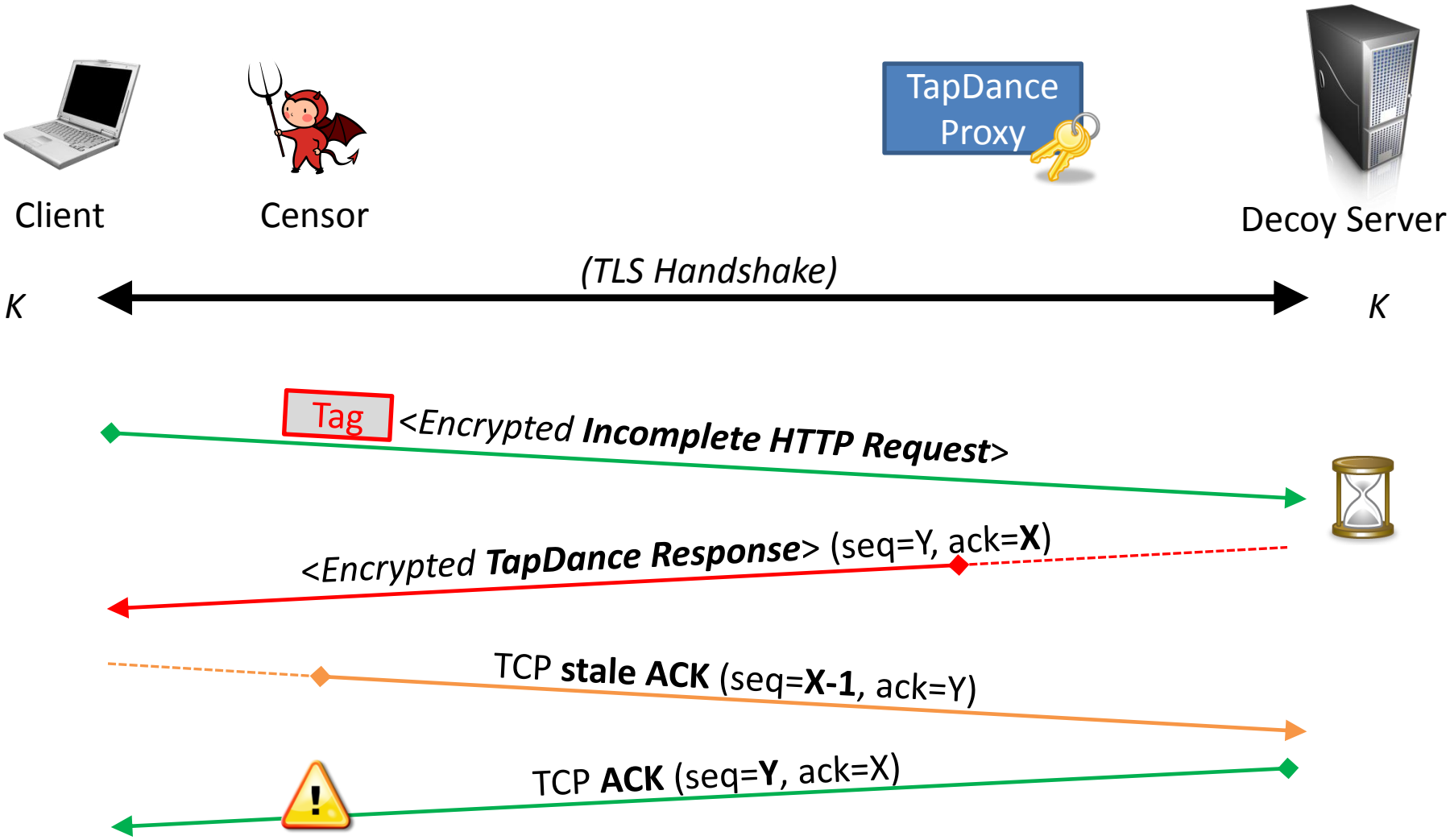
\x1e\x91\xb2\xce\x94\x8a\x6b\x3c\x78\x8c\x6f\x03
\x5e\xef\x97\x34\xf1\x2e\xc6\xe6\x7f\x10\xc8\x46
\xf9\x25\x6a\x0c\xff\x6d\x38 … \x70\xd7\x2c\x63 …



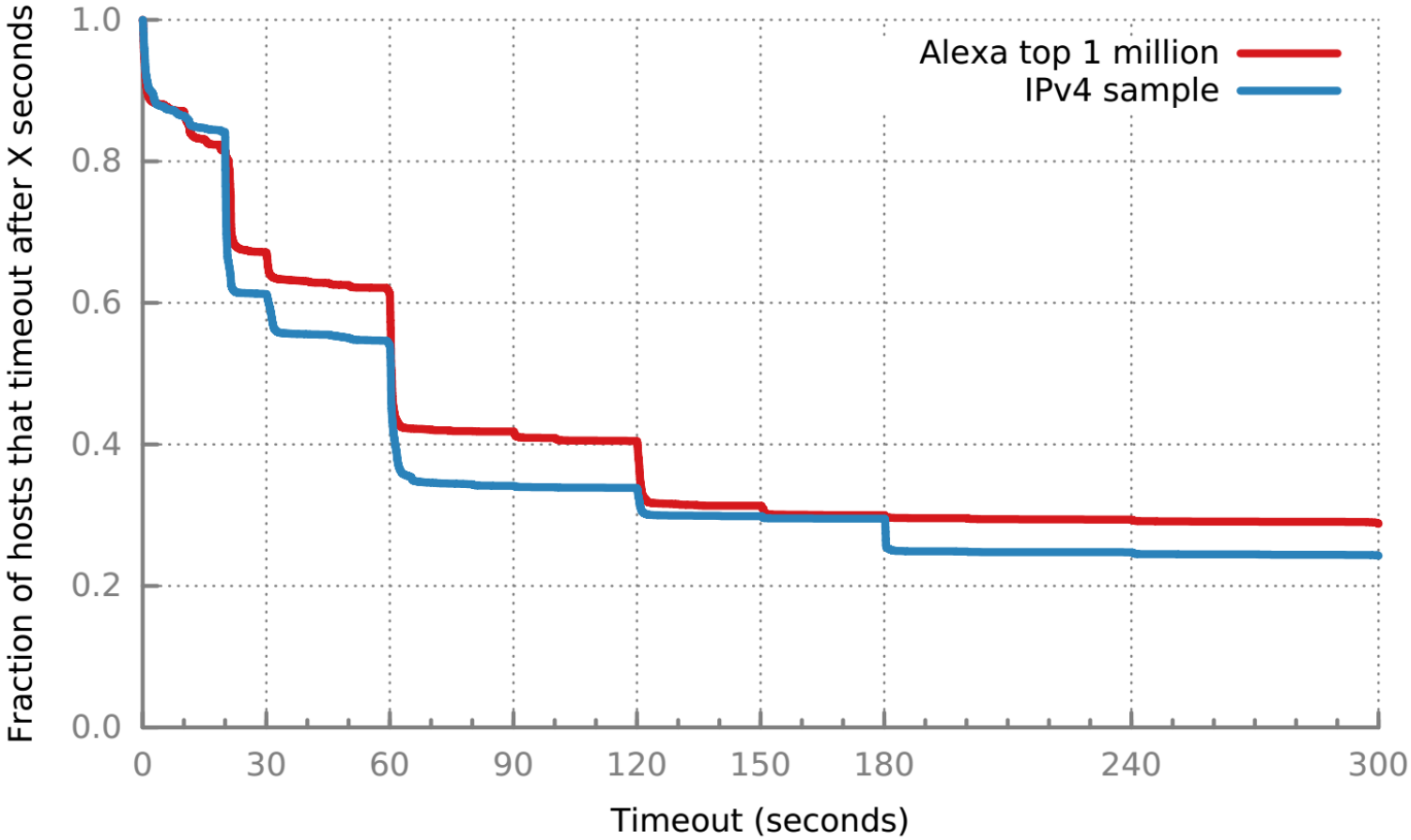
TapDance Protocol Overview



TapDance Active Attack



Hosts that allow Incomplete Requests



Previous work comparison

	Telex	Cirripede	Decoy Routing	TapDance
Steganographic channel	ClientRandom	TCP ISN	ClientRandom	TLS Ciphertext
No Inline blocking	✗	✗	✗	✓
Asymmetric flows	✗	✓	✓	✓
Replay attack defense	✓	✗	✗	✗
Traffic analysis defense	✗	✗	✗	✗

Future Work

- Real world deployment
- “Single-packet” (stateless) TapDance
- Traffic fingerprinting defense
- Active defense

Conclusion

- ***TapDance*** removes **inline blocking** requirement for End-to-Middle proxies, facilitating **deployment**
- Continues to function with **asymmetric traffic**
- Tradeoff of **active attack vulnerability** versus **deployability**