

# THE COST OF THE "S" IN HTTPS

**David Naylor**

Peter Steenkiste

*Carnegie Mellon University*

Alessandro Finamore

Marco Mellia

Maurizio Munafò

*Politecnico di Torino*

Ilias Leontiadis

Yan Grunenberger

Dina Papagiannaki

*Telefónica Research*

**web content  
personalization  
+  
awareness of  
user privacy**

Encryption the  
de facto  
**default in HTTP 2.0**

**Ubiquitous HTTPS**

# TLS



Certificates  
+ Validation



Handshake



Cryptography



Authentication



Secrecy



# Direct Costs

mechanics of TLS



# Indirect Costs

everything is encrypted

# COSTS

deployment

1

load time

2

data usage

3

energy consumption

4

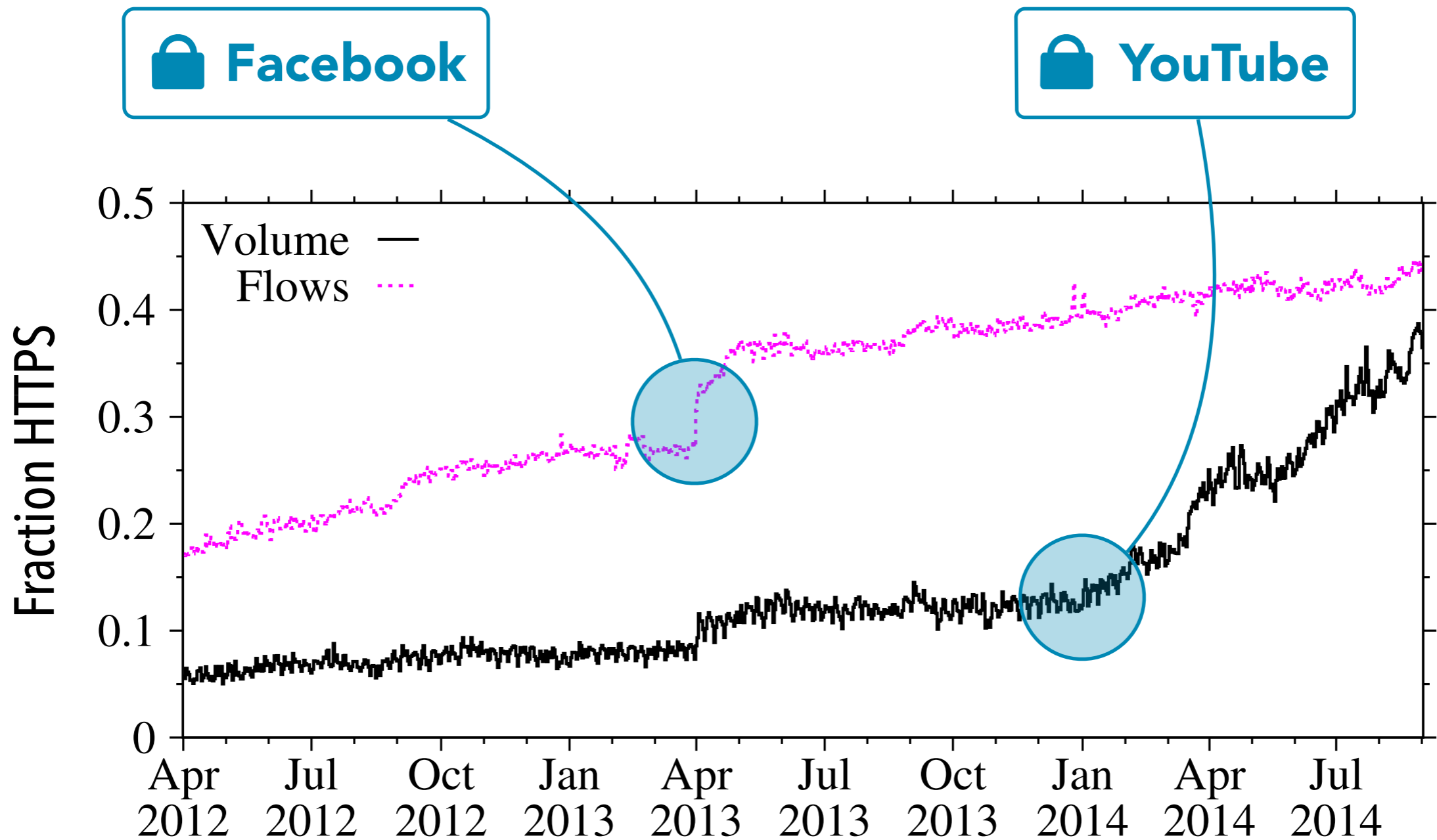
value-added services

5



DEPLOYMENT

# USAGE TRENDS



# TAKEAWAY

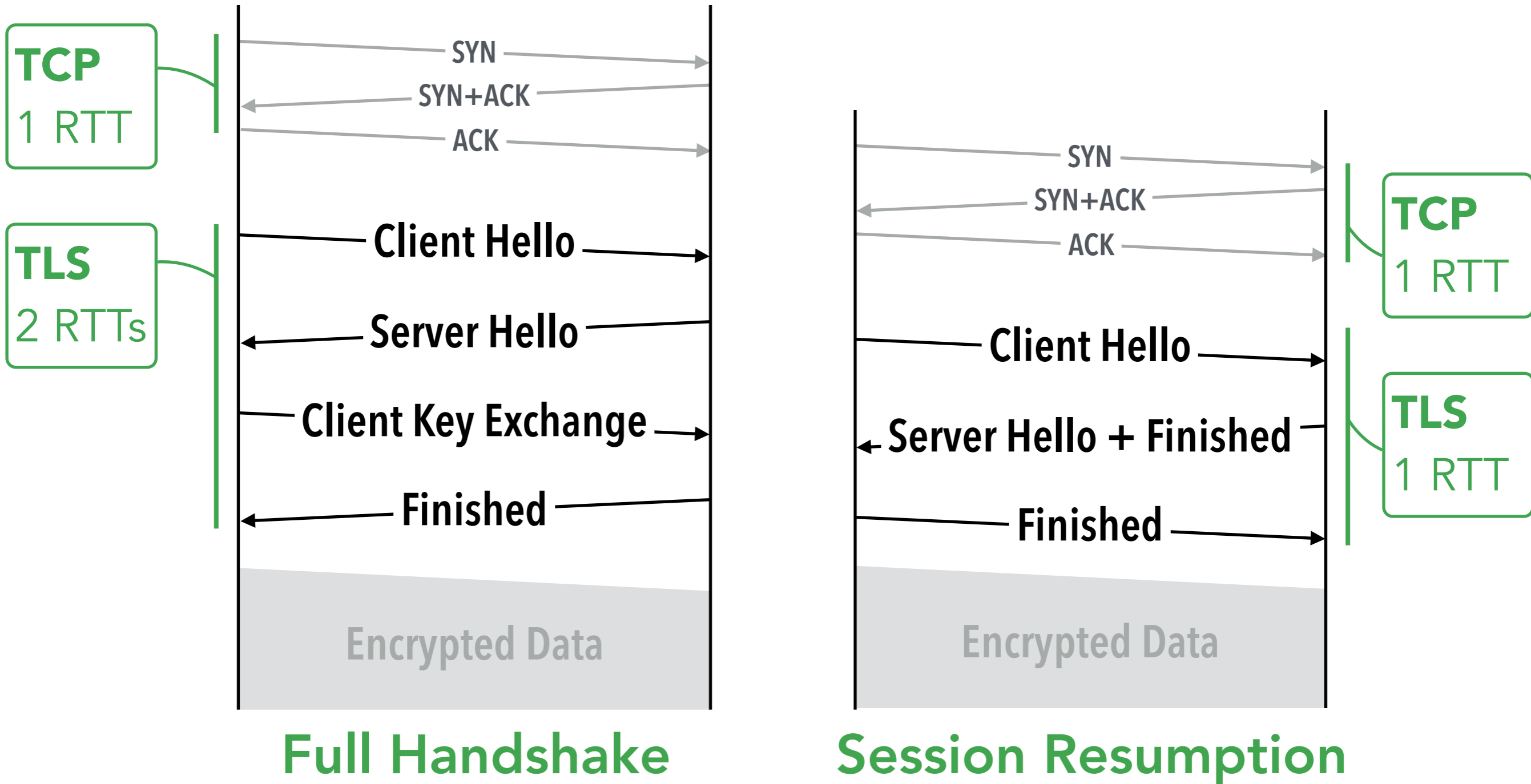
*HTTPS accounts for 50% of all HTTP connections and is no longer used solely for small objects, suggesting that the cost of deployment is justifiable and manageable for many services.*





LOAD TIME

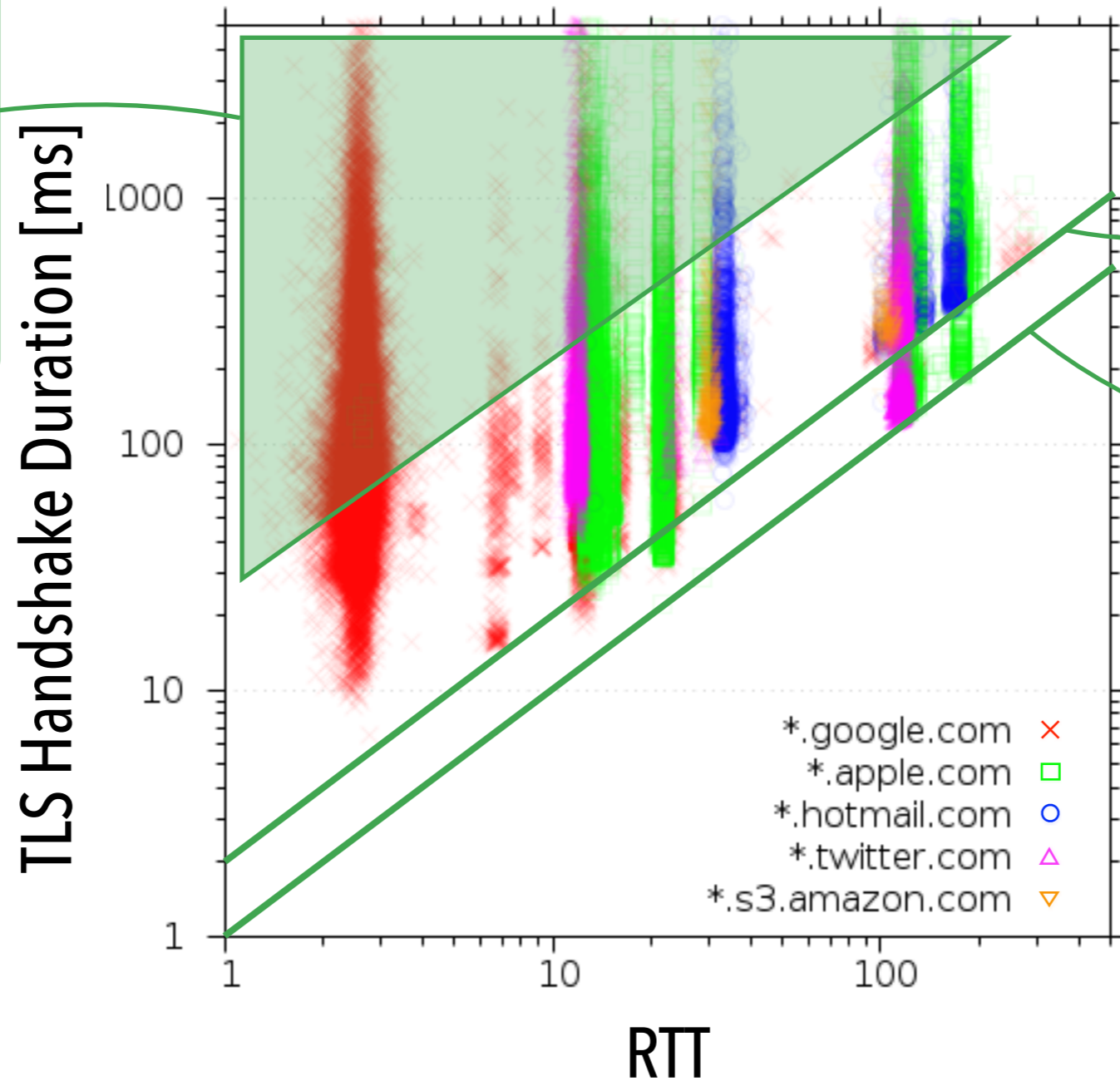
# TLS HANDSHAKE



# HANDSHAKE LATENCY

## Stragglers

Long handshake  
no matter how  
close server is

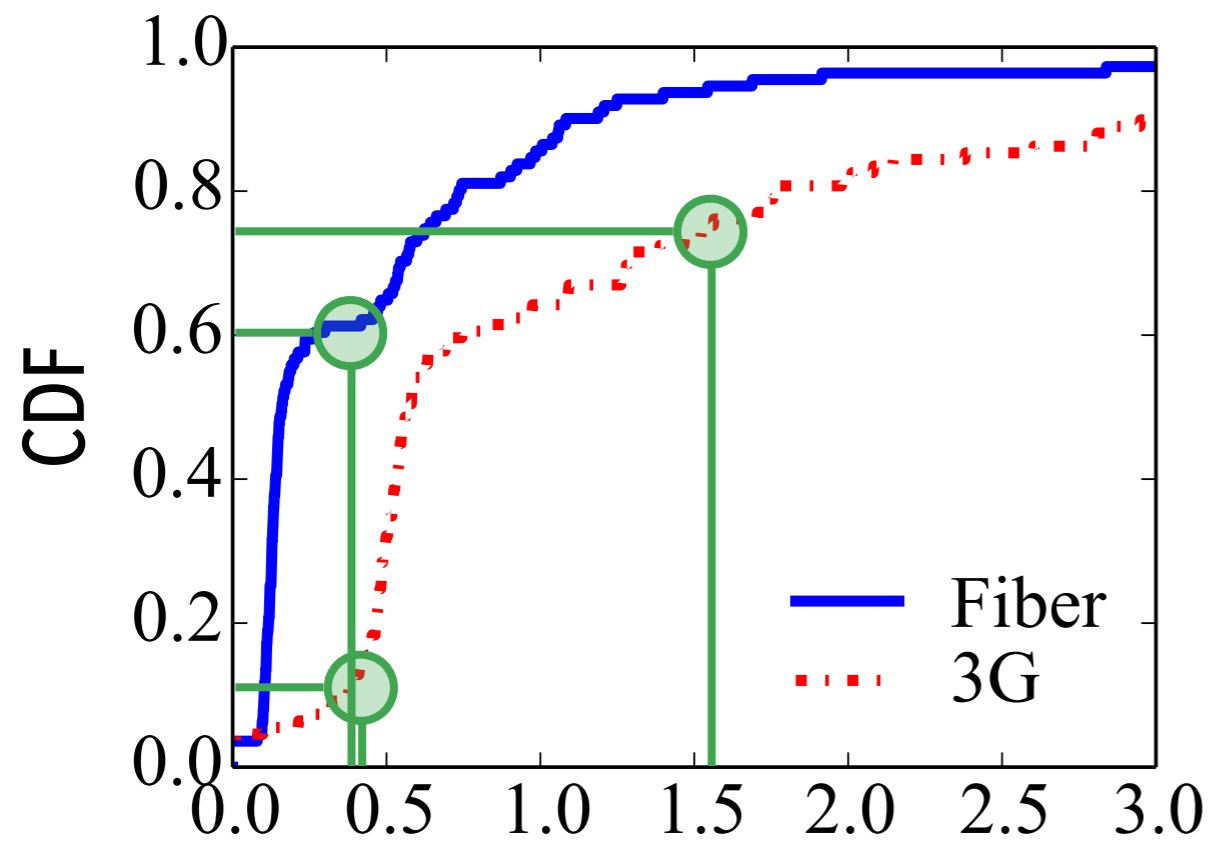


$y = 2x$   
Full handshake

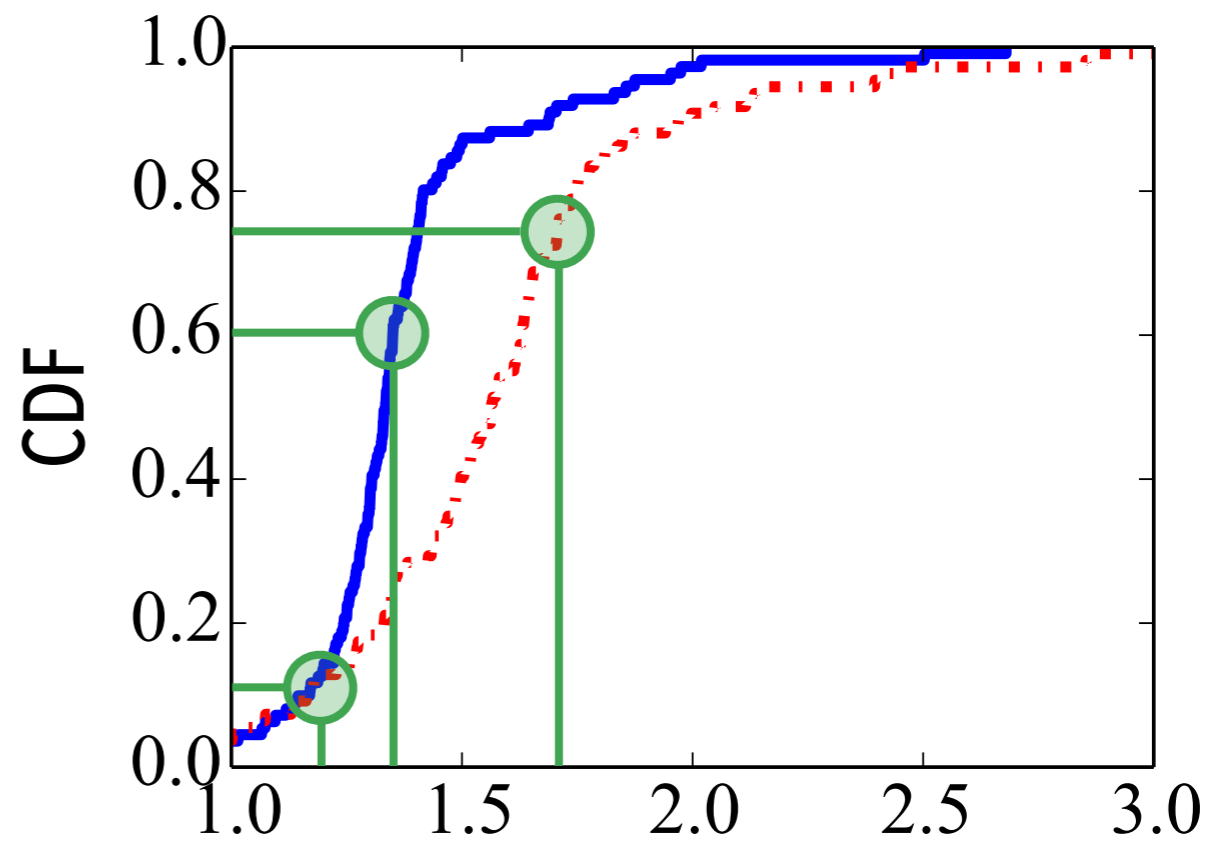
$y = x$   
Session  
resumption

# PAGE LOAD TIME

*Alexa Top 500*



HTTPS Increase: Difference  
(HTTPS-HTTP) [s]



HTTPS Increase: Ratio  
(HTTPS/HTTP)

# TAKEAWAY

*The extra latency introduced by HTTPS is not negligible, especially in a world where 1 second could cost 1.6 billion in sales.*

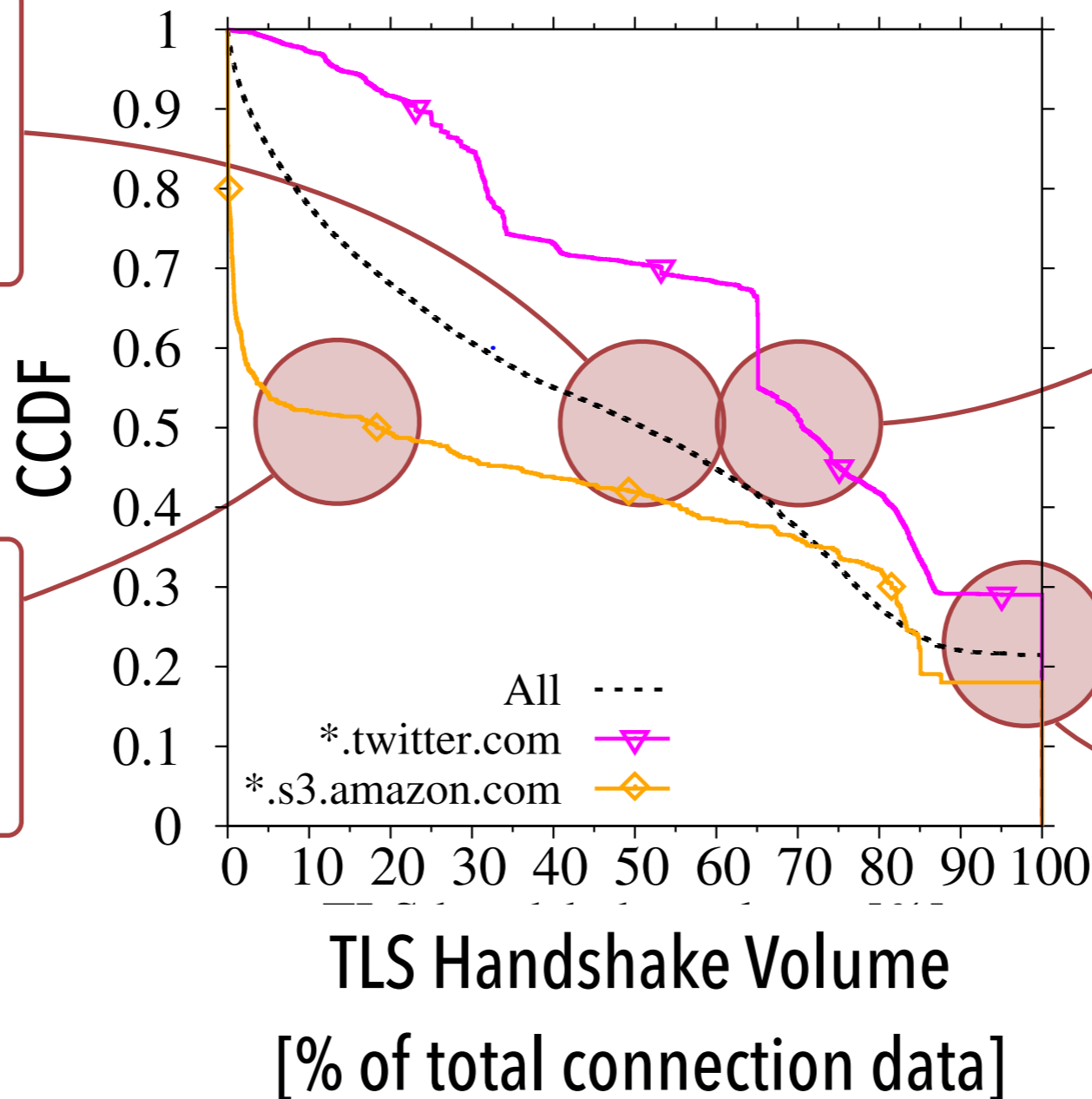
A large, light-colored number 3 is positioned on the left side of the image, set against a dark red background. The number is semi-transparent, allowing the background color to show through it. 

DATA USAGE

# HANDSHAKE OVERHEAD

**Overall:**  
for 1/2, handshake  
is > 50% of volume

**Amazon S3:**  
for 1/2, handshake  
is < 10% of volume



**Twitter:**  
for 1/2, handshake  
is > 70% of volume

**"Pre-Opening":**  
handshake is  
100% of volume

# HTTP PROXIES

## Compression

Compression ratio: **28.5%**

*Average daily per-user savings: 2.1 MB*

## Caching

Cache hit ratio: **14.9%**

*Average daily ISP savings: 16 TB*



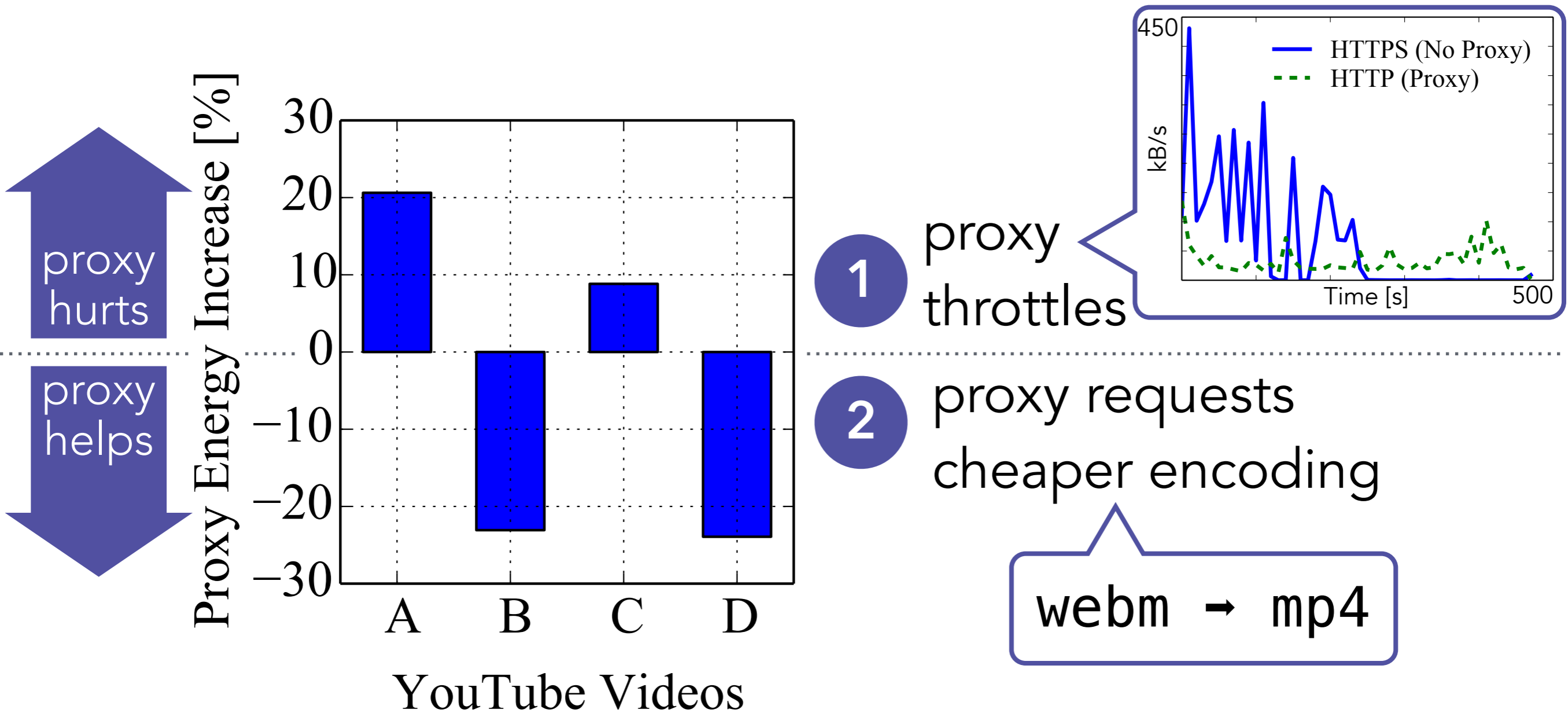
# TAKEAWAY

*Users are unlikely to notice significant jumps in data usage due to loss of compression, but ISPs stand to see a large increase in upstream traffic due to loss of caching.*



ENERGY  
CONSUMPTION

# VIDEO PLAYBACK



# TAKEAWAY

*HTTPS' cryptographic operations have almost no impact on energy costs, but the loss of proxies can significantly impact battery life (positively and negatively).*

A large, light-colored number '5' is positioned on the left side of the page, partially overlapping the text. The background is a solid orange color.

# VALUE-ADDED SERVICES

# LOTS OF MIDDLEBOXES

*(that operate on packet contents)*

compression

virus scanning

forensics

parental filtering

ad blocking

app-aware load balancing

intrusion prevention

caching

transcoding

app analytics

# EXAMPLE: PARENTAL FILTERING

**Internet Watch Foundation Blacklist**

**5%** pure domain or subdomain

# TAKEAWAY

*Though difficult to quantify, the loss of in-network services is potentially substantial; some of that functionality could be equally well performed on the client, while others may require a total rethink.*



# COSTS

deployment

1

load time

2

data usage

3

energy consumption

4

value-added services

5



# Direct Costs

## mechanics of TLS



*engineer 'em away*  
e.g., Google QUIC



# Indirect Costs

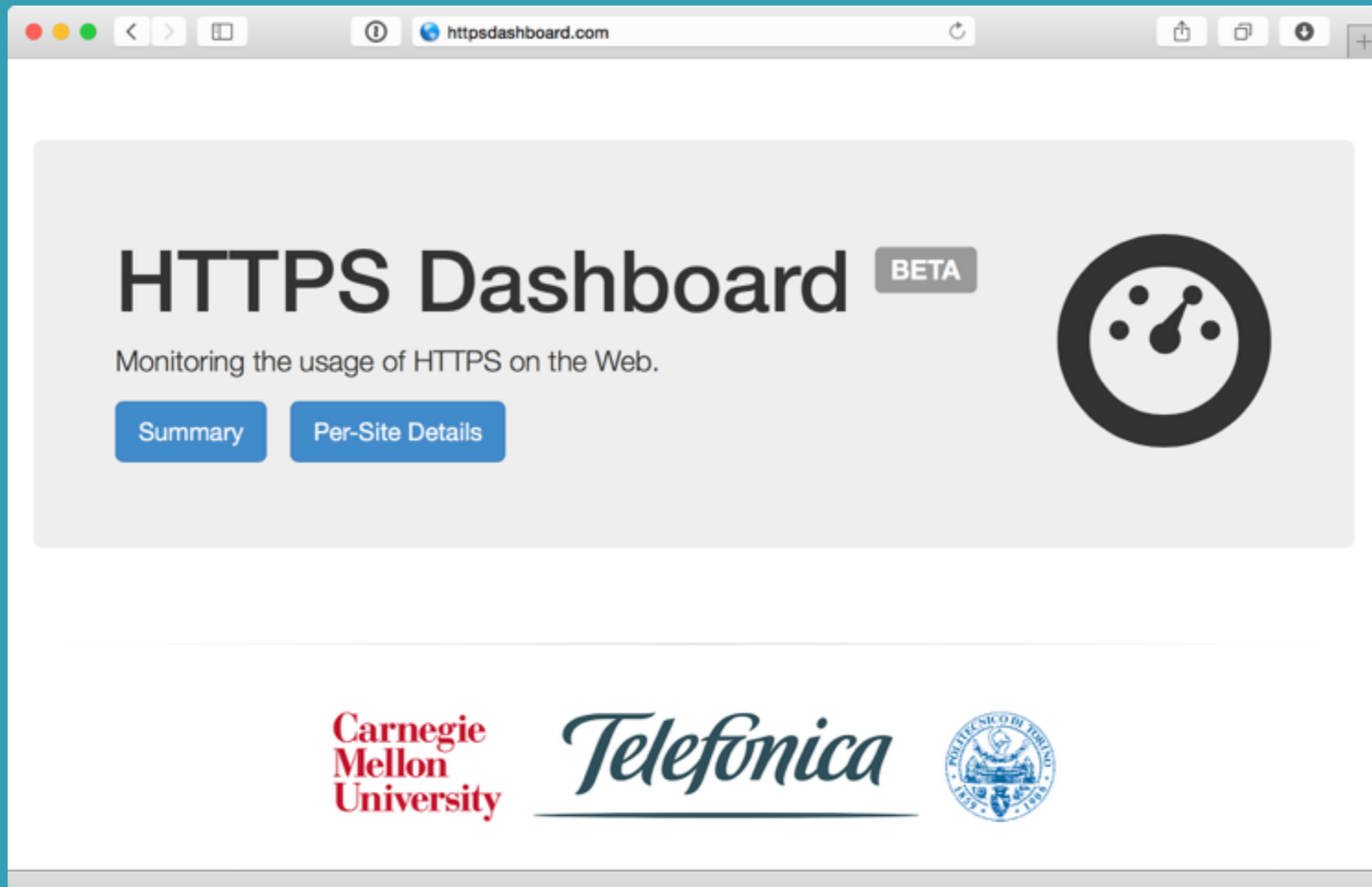
## everything is encrypted



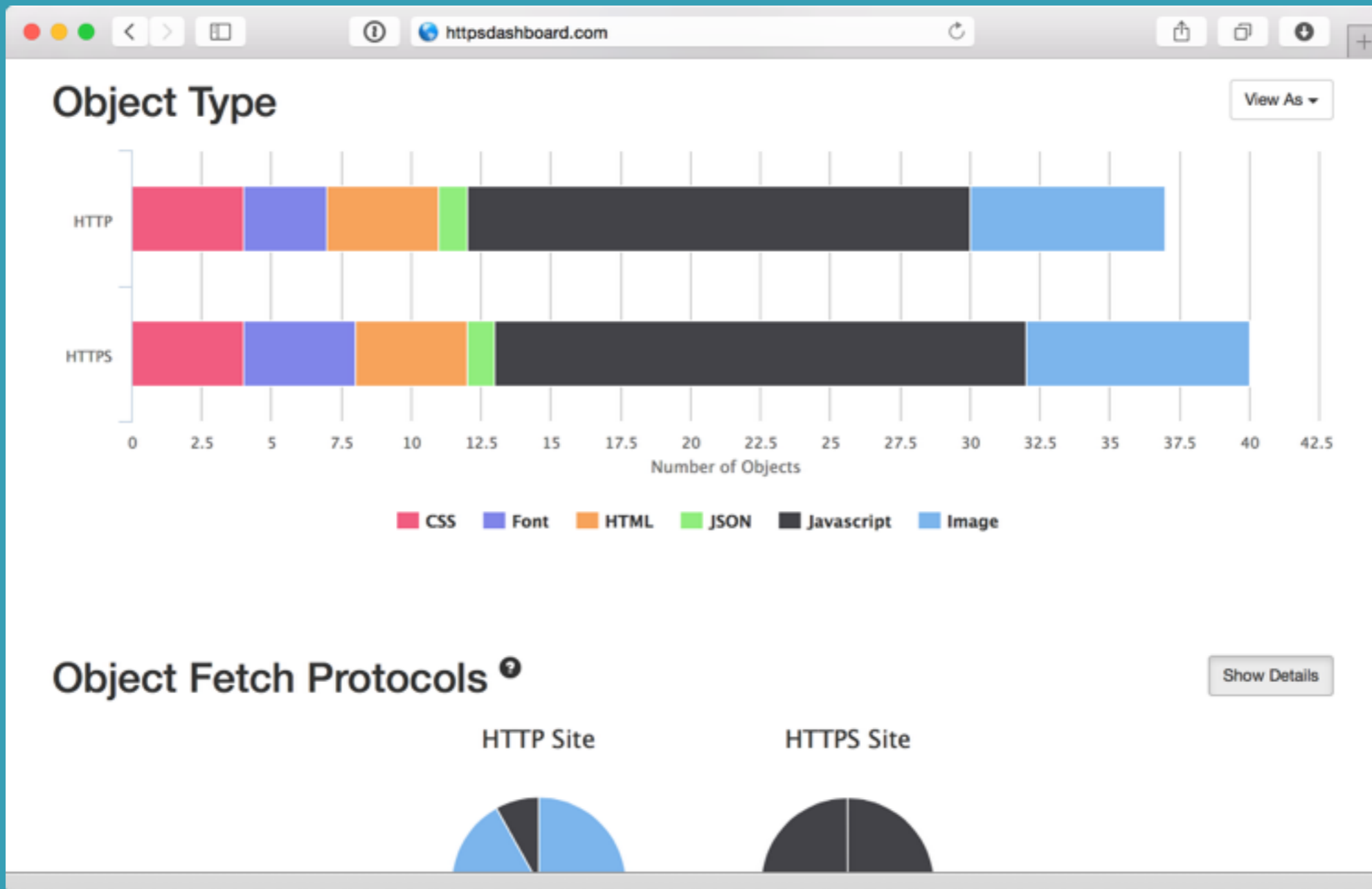
*need to rethink some things*  
e.g., Trusted Proxies



[github.com/dtnaylor/web-profiler](https://github.com/dtnaylor/web-profiler)



httpsdashboard.com



[httpsdashboard.com](https://httpsdashboard.com)

# THE COST OF THE "S" IN HTTPS

**David Naylor**

Peter Steenkiste

*Carnegie Mellon University*

Alessandro Finamore

Marco Mellia

Maurizio Munafò

*Politecnico di Torino*

Ilias Leontiadis

Yan Grunenberger

Dina Papagiannaki

*Telefónica Research*