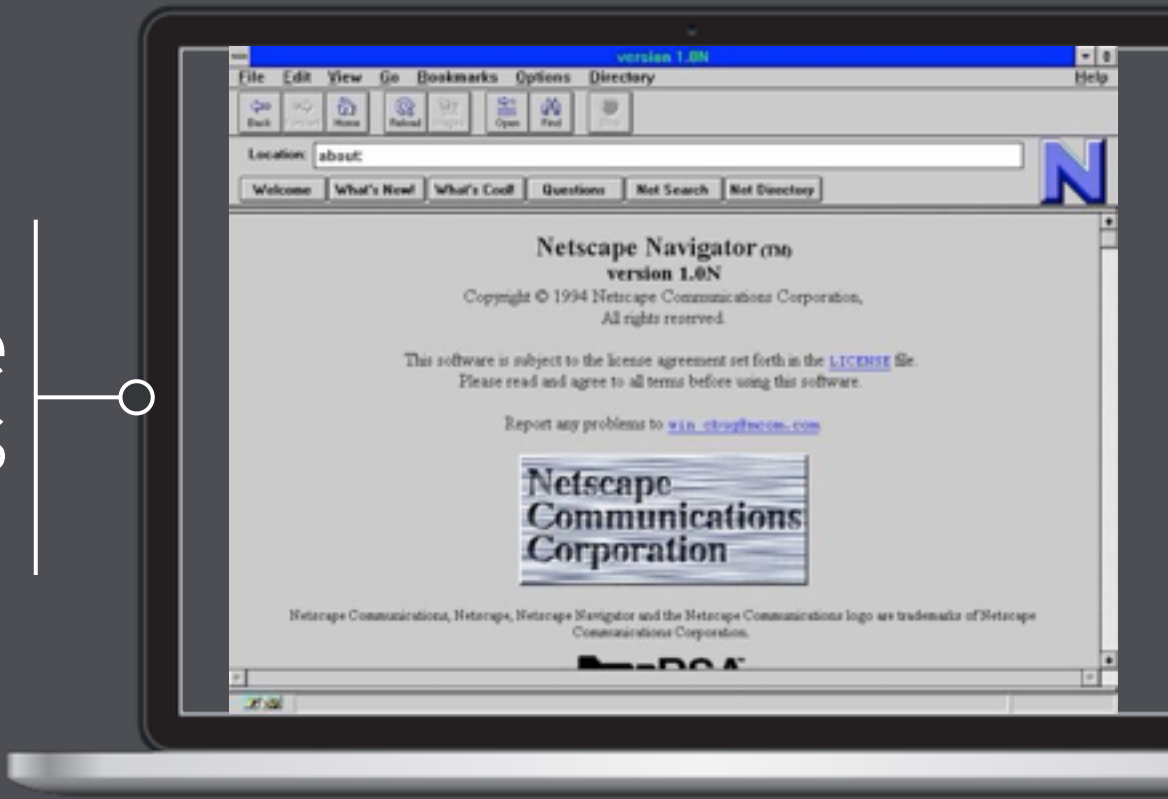
mozilla

The Road to **Encrypting All The Things**

J.C. Jones, Mozilla @JamesPugJones

Historic Reflection

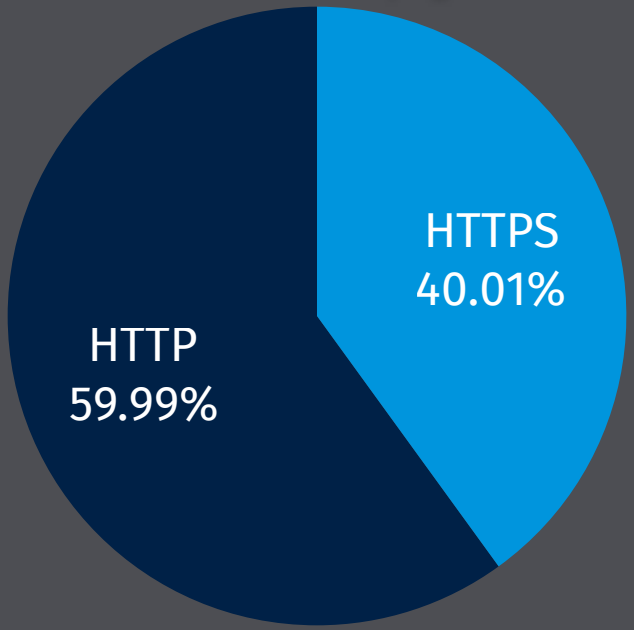
1995, Netscape released HTTPS



20 Years Later

Firefox 42 (Nov 2015)

Protocol for initial page load

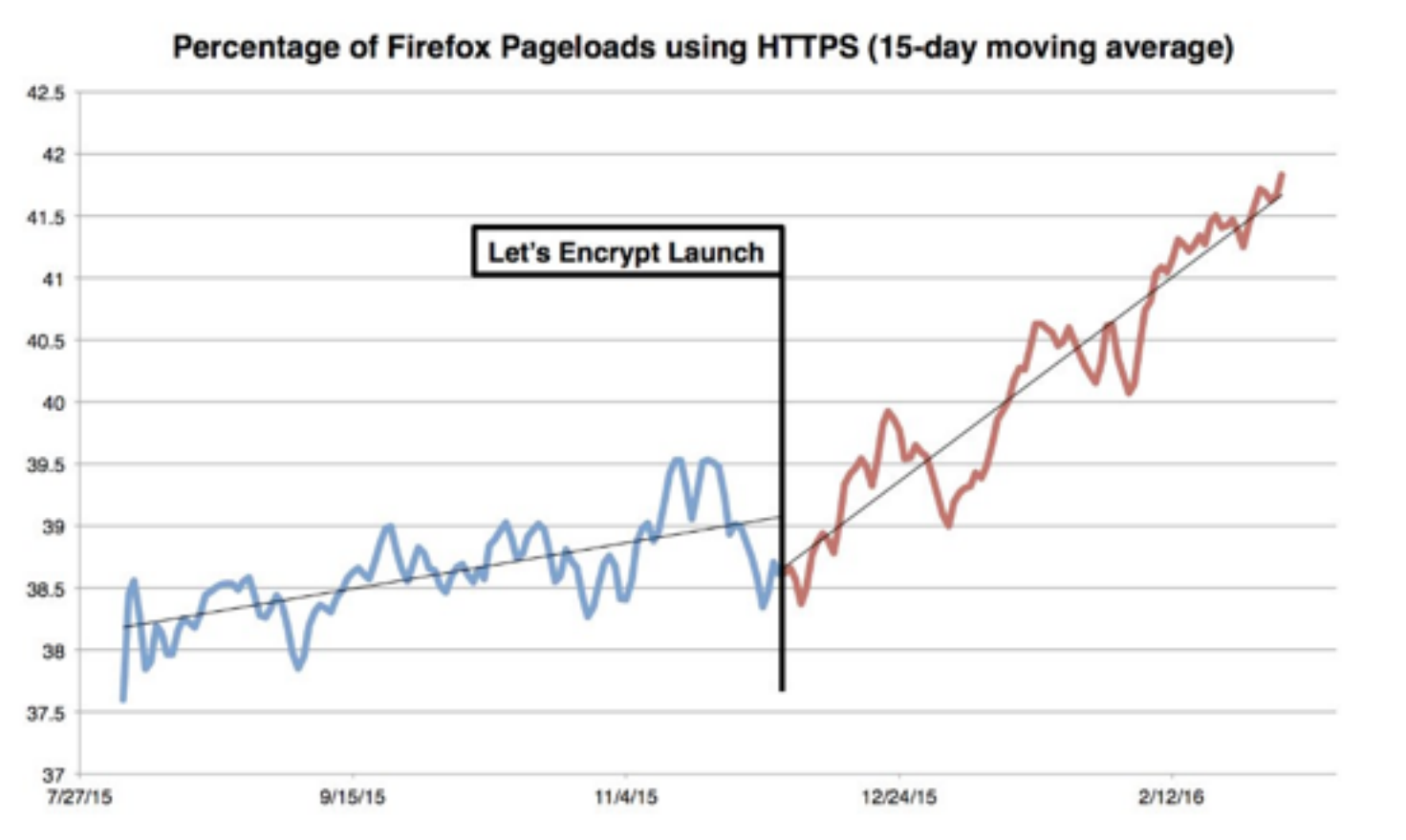


Not enough HTTPS on the Internet

- ~40% of initial page loads
- ~65% of all subsequent requests

Data: telemetry.mozilla.org

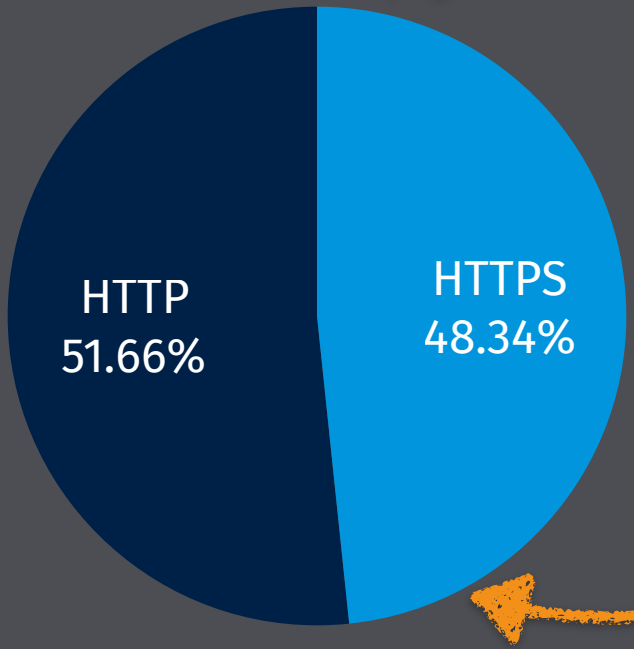
Then Let's Encrypt launched...



8 Months Later...

Firefox 47 (June 2016)

Protocol for initial page load



+8% in 7 Months

On a path to **HTTPS Everywhere**

Data: telemetry.mozilla.org

mozilla

Creating a New Certificate Authority

Threat Model

Risk: If someone issues a bad certificate, then Let’s Encrypt is no longer trusted. Close the doors, it’s over.

Becoming Trusted

Trust from the Web PKI is binary

Becoming Trusted

Trust from the Web PKI is binary

Threat Model

Risk: If someone issues a bad certificate, then Let's Encrypt is no longer trusted. Close the doors, it's over.

Threats: Insiders. Datacenter staff. Hardware couriers. Network and Protocol. Laptops.

Unexpected Challenges

Datacenter:
IPv6, power, space…

Picking a Datacenter

Physical security critical

“Perpetual storage,”

“Perpetual storage,”

by which we mean

magnetic tape.

Resolving DNS is really difficult.

Resolving DNS is really difficult.

like, for real.

Security tape.

Security bags.

mozilla

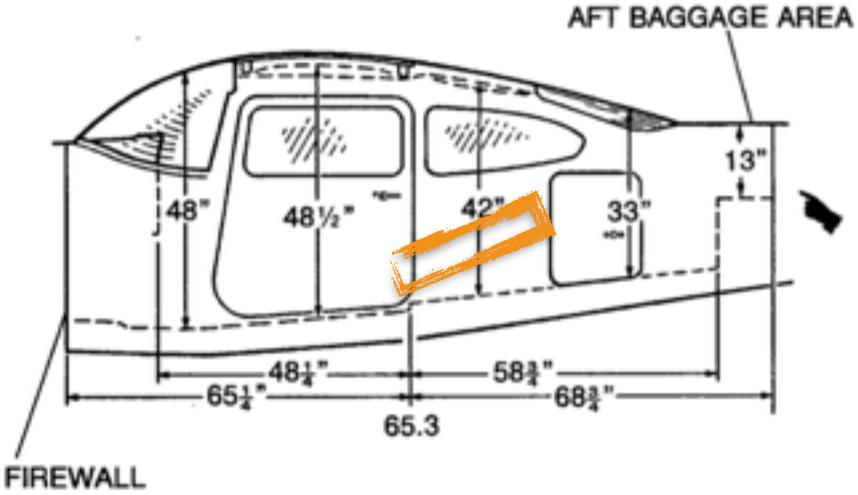
Security tape.

Security bags.

Moving a keyed hardware security module (HSM).

Last Resort:

CABIN HEIGHT MEASUREMENTS

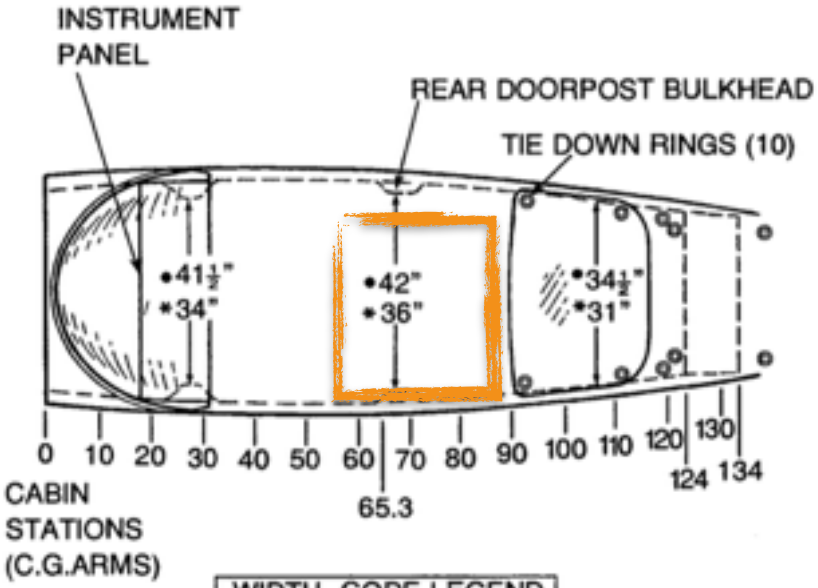


DOOR OPENING DIMENSIONS

	WIDTH (TOP)	WIDTH (BOTTOM)	HEIGHT (FRONT)	HEIGHT (REAR)
CABIN DOOR	32"	36½"	41"	38½"
BAGGAGE DOOR	15¾"	15¾"	22"	20½"

CESSNA
MODEL 182S
SECTION 6
WEIGHT & BALANCE / EQUIPMENT LIST

CABIN WIDTH MEASUREMENTS



WIDTH CODE LEGEND
• LOWER WINDOW LINE
* CABIN FLOOR

#1 Lesson

Remember your threat model.

Timeline


2012
Fundraising starts
May 2013
Formed ISRG
November 2014
Announced
November 2015
Public Beta
June 2013
First Snowden
disclosures

Questions?

- Datacenters?
- Server Architecture?
- Traffic Model / Modeling?
- Threat Models
- Governance / Policy

... and others!

J.C. Jones @JamesPugJones
jc@mozilla.com