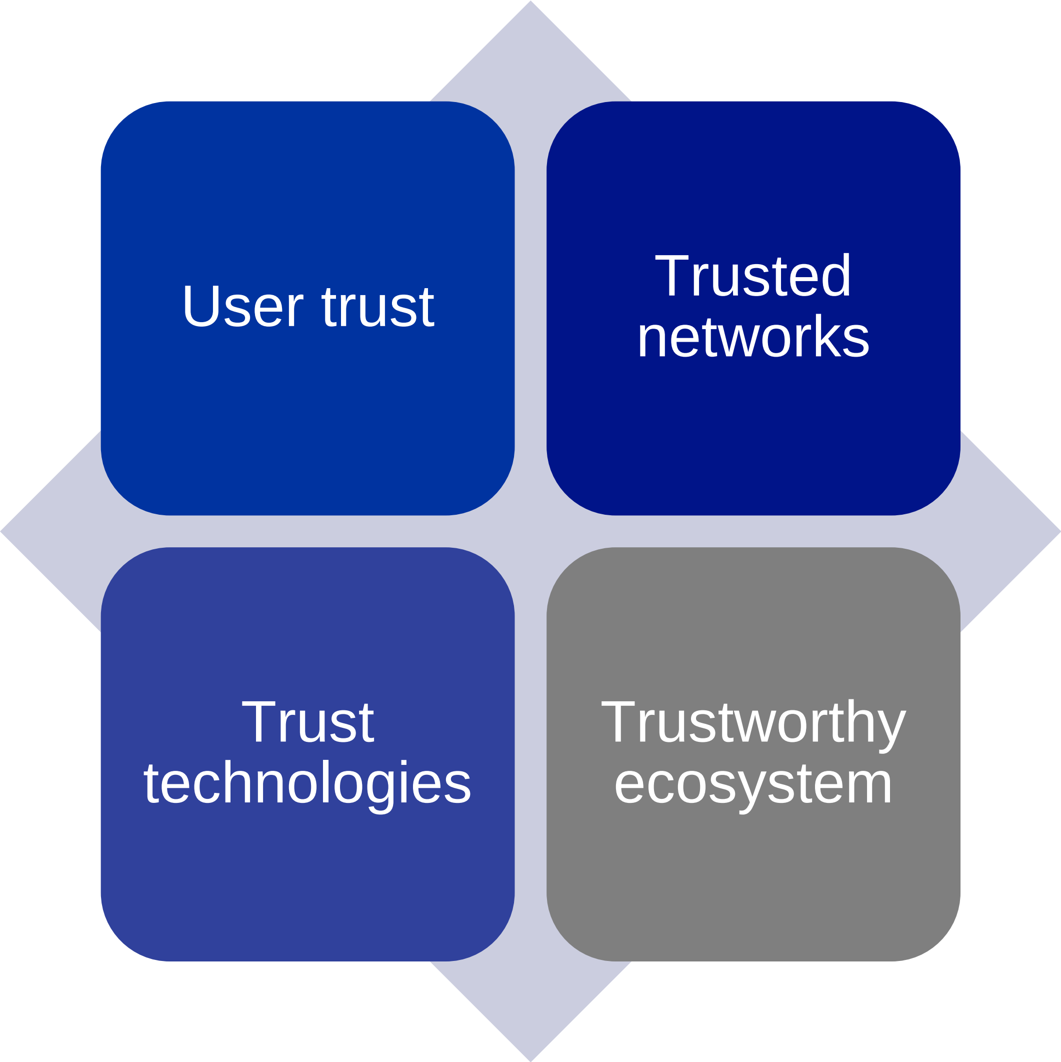
Trusted Internet

Encryption as Key Building Block

6 September 2016 @TLDCON, Tbilisi

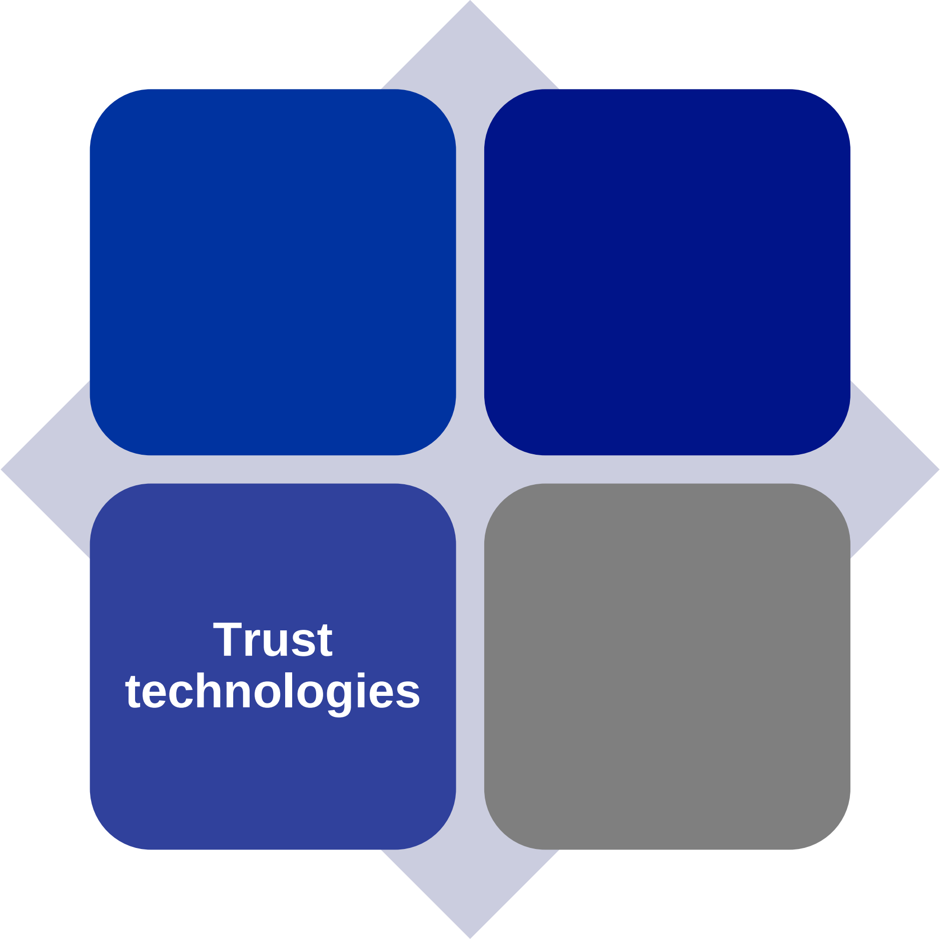
Maarit Palovirta (palovirta@isoc.org)

ISOC Trust Framework – An Integrated Approach



ISOC Trust Framework: http://www.internetsociety.org/doc/policy-framework-open-and-trusted-internet

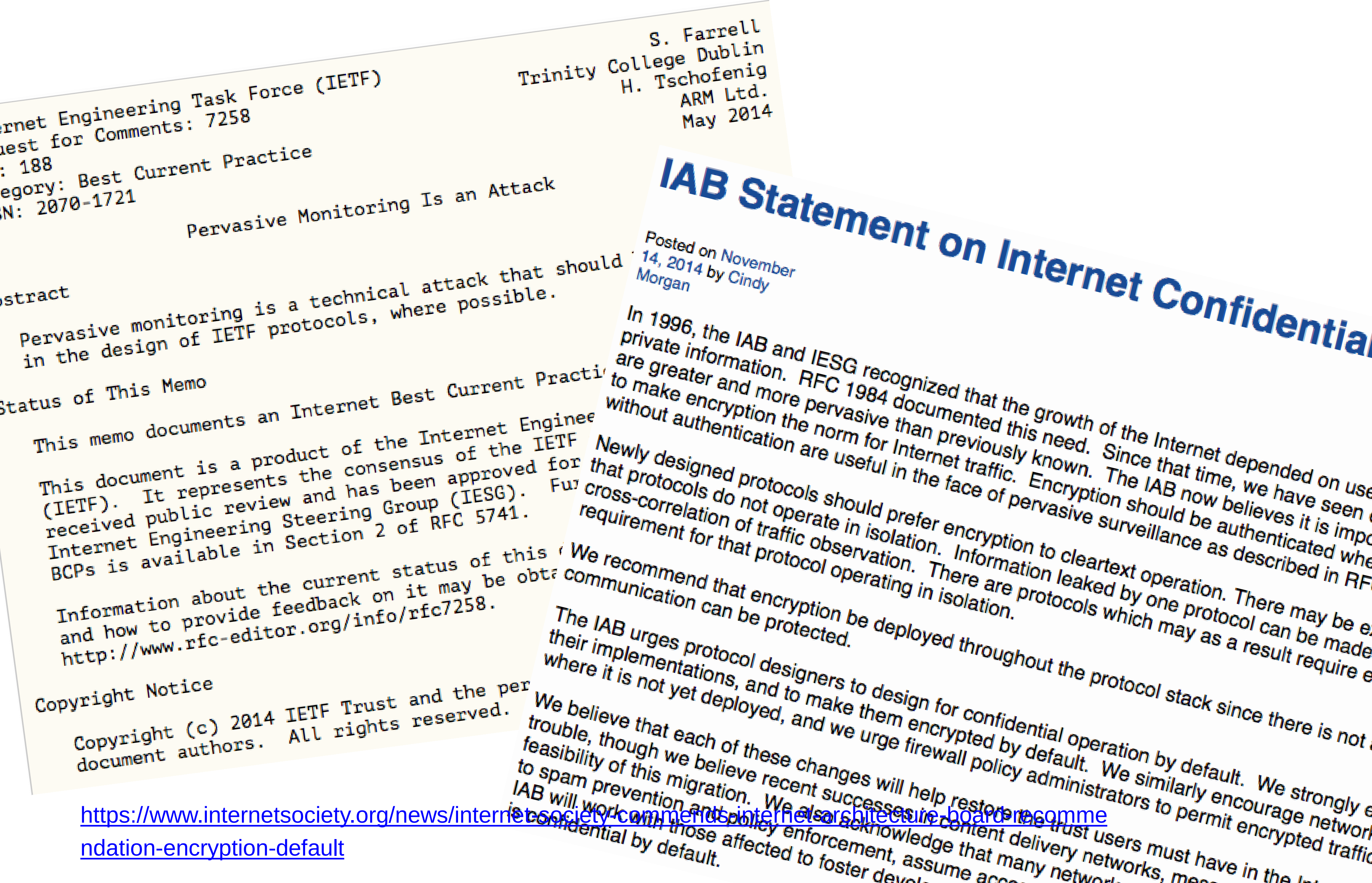
ISOC Trust Framework – Technologies of Trust



Technical building blocks for trusted networks, applications and services

- Confidentiality
- Authentication
- Integrity

Encryption Should Be the Norm for Internet Traffic



ernet Engineering Task Force (IETF)
uest for Comments: 7258
: 188
egory: Best Current Practice
N: 2070-1721

S. Farrell
Trinity College Dublin
H. Tschofenig
ARM Ltd.
May 2014

Pervasive Monitoring Is an Attack

ostract

Pervasive monitoring is a technical attack that should
in the design of IETF protocols, where possible.

Status of This Memo

This memo documents an Internet Best Current Practi

This document is a product of the Internet Enginee
(IETF). It represents the consensus of the IETF
received public review and has been approved for
Internet Engineering Steering Group (IESG). Fu
BCPs is available in Section 2 of RFC 5741.

Information about the current status of this
and how to provide feedback on it may be obta
http://www.rfc-editor.org/info/rfc7258.

Copyright Notice

Copyright (c) 2014 IETF Trust and the per
document authors. All rights reserved.

IAB Statement on Internet Confidential

Posted on November 14, 2014 by Cindy Morgan

In 1996, the IAB and IESG recognized that the growth of the Internet depended on use
private information. RFC 1984 documented this need. Since that time, we have seen
are greater and more pervasive than previously known. The IAB now believes it is impo
to make encryption the norm for Internet traffic. Encryption should be authenticated whe
without authentication are useful in the face of pervasive surveillance as described in RF

Newly designed protocols should prefer encryption to cleartext operation. There may be e
that protocols do not operate in isolation. Information leaked by one protocol can be made
cross-correlation of traffic observation. There are protocols which may as a result require e
requirement for that protocol operating in isolation.

We recommend that encryption be deployed throughout the protocol stack since there is not a
communication can be protected.

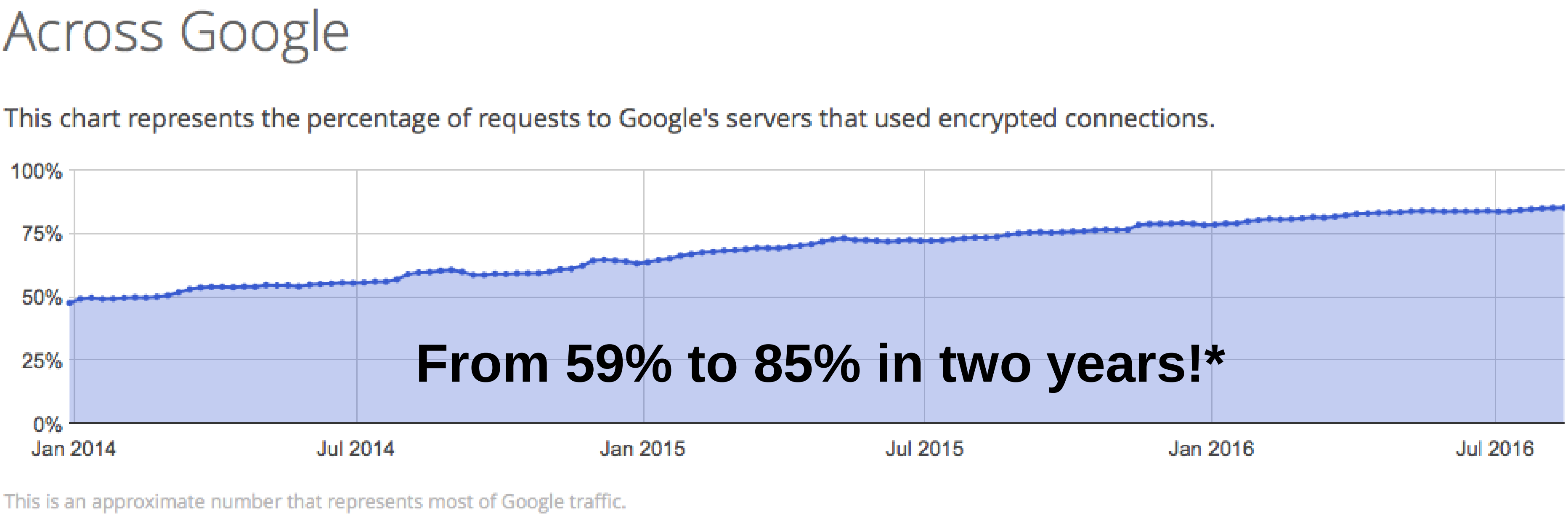
The IAB urges protocol designers to design for confidential operation by default. We strongly e
their implementations, and to make them encrypted by default. We similarly encourage network
where it is not yet deployed, and we urge firewall policy administrators to permit encrypted traffic

We believe that each of these changes will help restore the trust users must have in the In
trouble, though we believe recent successes in content delivery networks, mes
feasibility of this migration. We also acknowledge that many networks
to spam prevention and policy enforcement, assume acc
IAB will work with those affected to foster devel
is confidential by default.

https://www.internetsociety.org/news/internetsociety-commends-internet-architecture-board-recommendation-encryption-default

Where Are We?

Connecting Securely with Websites through HTTPS



Across Google

This chart represents the percentage of requests to Google's servers that used encrypted connections.

This is an approximate number that represents most of Google traffic.

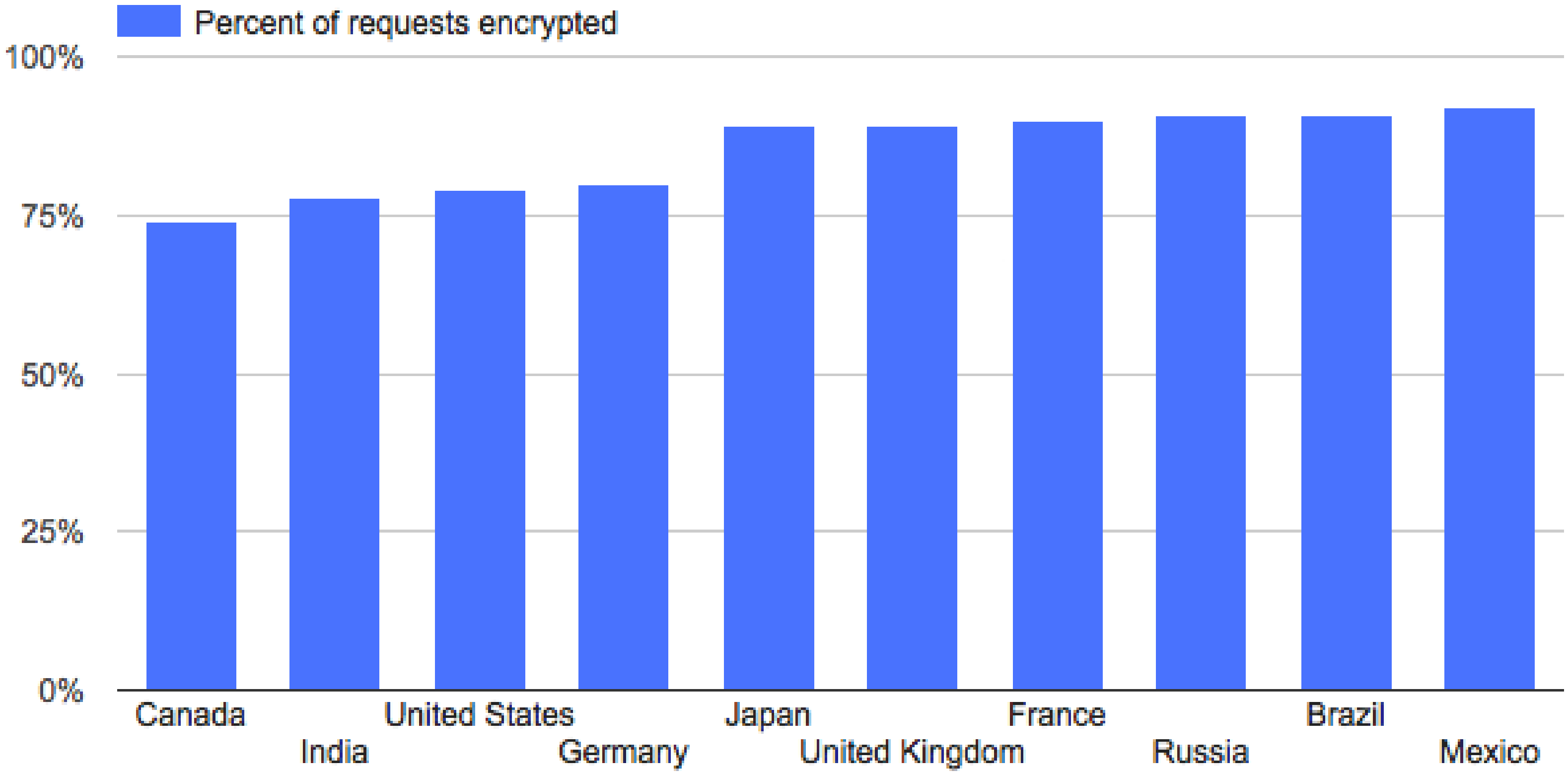
From 59% to 85% in two years!*

Globally (of all web traffic) around 45% of page loads on the Web use HTTPS (June 2016)**

* www.google.com/transparencyreport/https

** https://letsencrypt.org/2016/06/22/https-progress-june-2016.html, Firefox Telemetry, June 2016

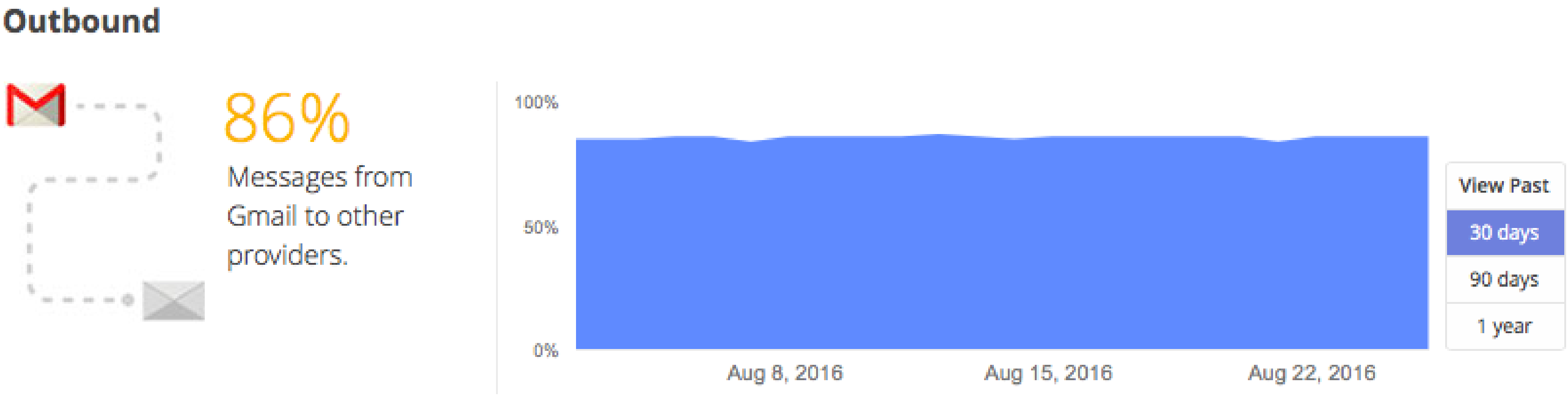
Encrypted Traffic by Country (HTTPS)



www.google.com/transparencyreport/https (August 2016)

Internet Society

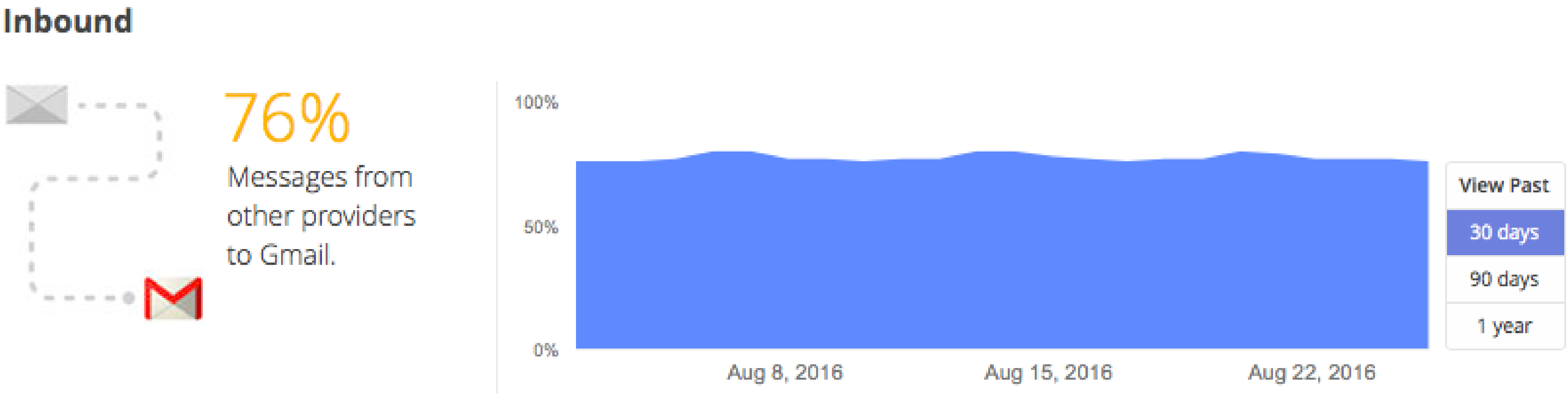
How Much e-mail Encrypted in Transit?



Outbound

86%

Messages from Gmail to other providers.



Inbound

76%

Messages from other providers to Gmail.

www.google.com/transparencyreport/saferemail

Challenges – Political and Technical

- Encryption can help “bad actors” hide communications.
- Debate on “backdoors” and tamper-resistant technology.
- Some countries may block encryption technologies.
- Deployment – issues in network management design, development, management and usability.
- Old hardware/ software and lack of technical resources may hinder adoption.
- Certificate/ key management.

How Does ISOC Support?

Cryptech Project

- **Goal:** is to create an open-source hardware cryptographic engine that…
  - is of general use to the broad Internet community, covering needs such as securing email, web, DNSsec, PKIs.
  - can be built by anyone from public hardware specifications and open-source firmware and operated without fees of any kind.
- **Team:** A loose international collective of engineers, funded diversely and is administratively quartered outside the US.
- Visit: www.cryptech.is

Let’s Encrypt Initiative (www.letsencrypt.org)

- A free, automated, and open certificate authority (CA), provided by the Internet Security Research Group (ISRG).

- Key principles:

  - ❑ **Free:** Anyone who owns a domain name can obtain a trusted certificate at zero cost.
  - ❑ **Automatic:** Software running on a web server can interact with Let’s Encrypt to obtain a certificate, configure it for use, and automatically take care of renewal.
  - ❑ **Secure:** A platform for advancing TLS security best practices.
  - ❑ **Transparent:** All certificates issued or revoked will be publicly recorded and available for anyone to inspect.
  - ❑ **Open:** The automatic issuance and renewal protocol will be published as an open standard that others can adopt.
  - ❑ **Cooperative:** A joint effort to benefit the community, beyond the control of any one organization.

Deploy360 – Support for Deployment

- Provide hands-on information on DNSSEC, DANE protocol and TLS for applications.

- Work with first adopters to collect and create technical resources and distribute these resources.

- Content specific to: Network Operators, Developers, Content Providers, Consumer Electronics Manufacturers, Enterprise Customers

- Visit: http://www.internetsociety.org/deploy360

Reality Check

- “Everything is out in the open” does not work.
- Encryption will reduce the number of parties that will see traffic but does not eliminate them – content provider, browser vendor, proxy provider, corporate IT department.
- Choice of technology is voluntary and the capacity to deploy/adopt a certain technology can depend where you are.
- Surveillance shifts but is not eliminated.
- Technical progress may have unwanted outcomes – regulation to limit security, fragmentation, device control.

Thank You