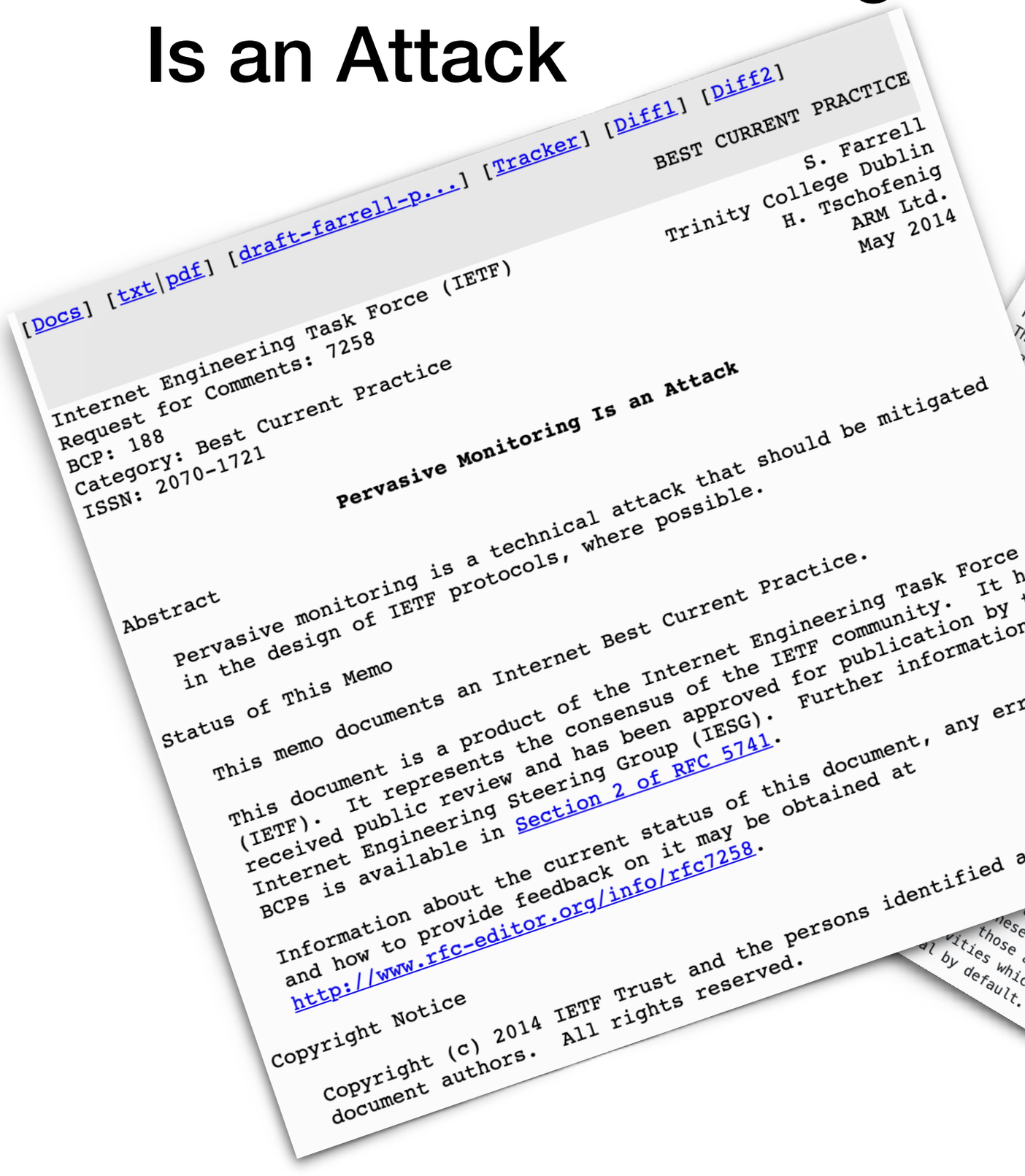
Systems Considerations

Dirk Kutscher
<ietf@dkutscher.net>

HotRFC@IETF-106

RFC 7258: Pervasive Monitoring Is an Attack



[Docs] [txt|pdf] [draft-farrell-p...] [Tracker] [Diff1] [Diff2]

Internet Engineering Task Force (IETF)
Request for Comments: 7258
BCP: 188
Category: Best Current Practice
ISSN: 2070-1721

BEST CURRENT PRACTICE

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

Pervasive Monitoring Is an Attack

Abstract

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

Status of This Memo

This memo documents an Internet Best Current Practice.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on BCPs is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7258.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

IETF

IAB Statement on Internet Confidentiality

IAB Chair <iab-chair@iab.org> | Fri, 14 November 2014 09:26 UTC

Help Setting | Show h

Please find this statement issued by the IAB today.

On behalf of the IAB,
Russ Housley
IAB Chair

= = = = = = = = = =

IAB Statement on Internet Confidentiality

In 1996, the IAB and IESG recognized that the growth of the Internet depended on users having confidence that the network would protect their private information. RFC 1984 documented this need. Since that time, we have seen evidence that the capabilities and activities of attackers are greater and more pervasive than previously known. The IAB now believes it is important for protocol designers, developers, and operators to make encryption the norm for Internet traffic. Encryption should be authenticated where possible, but even protocols providing confidentiality without authentication are useful in the face of pervasive surveillance as described in RFC 7258.

Newly designed protocols should prefer encryption to cleartext operation. There may be exceptions to this default, but it is important to recognize t protocols do not operate in isolation. Information leaked by one col can be made part of a more substantial body of information -correlation of traffic observation. There are protocols which sult require encryption on the Internet even when it would rement for that protocol operating in isolation.

ncryption be deployed throughout the protocol stack ingle place within the stack where all kinds of ected.

s to design for confidential operation by evelopers to include encryption in their crypted by default. We similarly to deploy encryption where it is icy administrators to permit

restore the trust users at this will take time and in content delivery networks, yments demonstrate the acknowledge that many network ffic management and intrusion licy enforcement, assume access to hese activities there are no solutions those affected to foster development of vities which allow us to move to an Internet l by default.

Encrypt everything!

DISPLAY LUMAscape

MARKETER

Agencies

WPP
OmnicomGroup
PUBLICIS GROUPE
IPG
dentsu
HAVAS
MERKLE
MDC Partners
AEGIS
AKQA
LBi
ROSETTA
CHI
icrossing
Innovation INTERACTIVE
camelot Mediasmith
at&t interactive
IBM
essence
yodle
REACHLOCAL
WebVisible

Agency Trading Desks

XAXIS
accuen
VIVAKI
RUN
CADREON
amnet
accordantmedia
AFFIPERF
IMPAQT
VARICK MEDIA MANAGEMENT

Creative Optimization

teracent
TUMRI
dapper
AdExtent
Impossible Software
adroit
struq
MIXPO
thunder
SPONGECELL
engageclick
promote
adacado
Dynamix
snapads
AdReady
CERTONA
richrelevance
ADISN

Retargeting

dotomi
criteo
MAGNETIC
AdRoll
TellApart
TRIGGIT
ciomantic
crossperimedia
MYBUYS
FetchBack
buysight
PERFECT AUDIENCE
ReTargeter
STEELHOUSE
mythings
mediaFORGE

Ad Servers

doubleclick by Google
atlas
Mediaplex
ELITA
mediamind
Sizmek
pictela
pointroll
flashtalking
trueffect
adform
adgear

Verification / Privacy

DV
IAS Integral Ad Science
GHOSTERY
whitepages
PROTECTED MEDIA
TRUST METRICS
FORENSIQ
THE MEDIA TRUST
ADXPOSE
privacychoice
TRUSTe

DSPs

Google
invitemedia
amazonadvertising
theTradeDesk
MediaMath
TURN
dataxu
EfficientFrontier
Chango
Simplifi
sitescout
DIGILANT
BEESWAX
adform
AdBuyer.com
acuity
BRANDSCREEN
CTRL SHIFT
getintent
choozle

AppNexus

Media Planning and Attribution

MarketShare
COGNITIVE MATCH
DataSong
M FACTOR
NETWORKED INSIGHTS
CONVERTRO
colspace
SQAD
TUNE
VISILIP
C3 Metrics
admetrix
OPTIMINE
MARKETING EVOLUTION
ThinkVine
Encore
ConversionLogic
COMMERCE SIGNALS
Korrelate

Tag Mgmt

TagMan
ensighten
TEALIUM

Measurement and Analytics

OMNITURE
unica
dynata
Core metrics
tracksimple
webtrends
Google Analytics
nielsen
METAMARKETS
comScore
biz science
MOAT
VIZU
PATHMATICS
ojento
LUCID
aprimo

Exchanges

DoubleClick
RIGHTMEDIA
Facebook Exchange
ADECN
OpenX
INDEX EXCHANGE
RhythmOne
PULSEPOINT
district m
gumgum
PLYmedia
smartyads
ZEROSIA
adjug

DMPs and Data Aggregators

bluekai
x+1
ak
LOTAME
Demdex
exelate
SIGNAL
brilig
quantcast
eyeota
krux
bizo
PARIO
Red Aril
JovianDATA
datonics
upfront
LiveRamp
CIRCULATE
acxiom
grapeshot
proximic
bombora
PEER39
4DmantX

Data Suppliers

experian
acxiom
datalogix
NOVA
EPSILON
TARGUSinfo
TruSignal
NETEZZA
mastercard
bluecava
where
IRi
EQUIFAX
Viz
IXI
infogroup
CLICKKEY
DATALINE
cardlytics

Ad Networks

Horizontal

YAHOO!
Google
CONVERSANT
Bing ads
amazon media group
Aol.
adconion
Undertone
eXponential
audience
24/7 MEDIA
Digital Remedy
SOLVE media
Brand net
BurstMedia
AT&T AdWorks
integrity
AdDynamix
traffic marketplace
UNDERDOG Media

Video / Rich Media

TREMOR VIDEO
videology
meebo
YuMe
BBE
TubeMogul
BrightRoll
spotXchange
adotube
smartclip
MATOMY
seedtag
ScanScout
BREAK
Mobile

Vertical / Custom

ravora
MOB SOC
LONGBOARD MEDIA
ADIFY
EVOLVE MEDIA
Sportsgenic
RGM ALLIANCE
GourmetAds
NetShelter
MODE MEDIA
MAXPOINT
martini media
Q1Media
InflectionPointMedia
IDGTechNetwork
SQUERN
playwire
Ideas People
brightcom
ToneFuse

Targeted Networks / AMPs

rocketfuel
Albert
interclick
Collective
dstillery
Taykey
precisiondemand
SRAX
VIANT
33across
true[X] media
radiumone
ownerIQ
resonate
adadyn
NetSeer
yp
pulse360
Adblade
adaramedia
pesrset
inadco
XGRAPH
CONTEXTWEB
rockerbox

Performance

epic
vm
MATOMY
advertise.com
convertmedia
moxy media
VigLink
conversion junction
VIBRANT
Kontera
MADISON LOGIC
FLUENT
LinkShare
php
adknowledge
MARCHEX
hydra
neverblue
Datran Media
MediaTrust
affinity
Tatto Media
TheUseful
sourceknowledge

Mobile

AdMob
quattro
crossbeard
millennialmedia
Jumptap
rhythm
INMOBI
transpera
BLUESTREAK

Sharing Data / Social Tools

facebook
ShareThis
AddThis
tynt
GIGYA

SSPs

AdmeId
rubicon project
PubMatic
LIFTDNA
Beanstock
ReviNet
ALTITUDE
sonobi

Publisher Tools

yieldex
FATTAIL
ShortTail
ujet
ISOCKET
SOUSA
komoona
adelphic
BuySellAds
admix
Adslot.
yieldbot
BuzzFeed
scout analytics
INSTICATOR
DailyMe
Mochila
dayilife
PerfectMarket
MIXPIER
outbrain
PARSELY
TabOola
Gravity
Luminate
Browsi

Ad Servers

doubleclick by Google
24/7 MEDIA
apt
LiveIntent
Adgear
ADTECH
ZEDO
OpenX
AdJuggler
adzerk
aiMatch

Media Mgmt Systems and Operations

DDS
Soperative
telmar
centro
media
theorem
MEDIABANK
facilitate
TRAFFIQ
BIONIC
Solbright
AdPro
SQAD

PUBLISHER

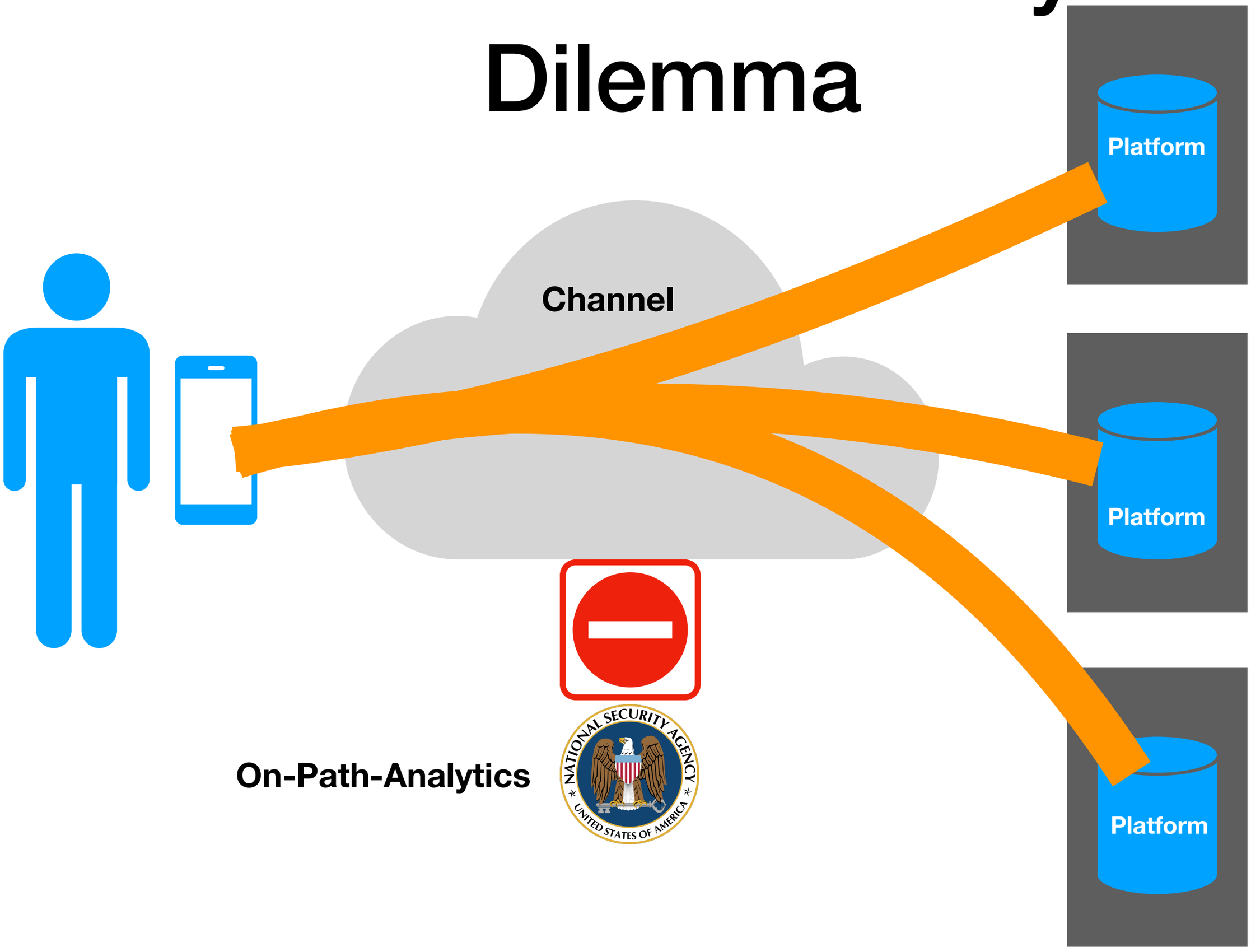
PEOPLE

LUMA

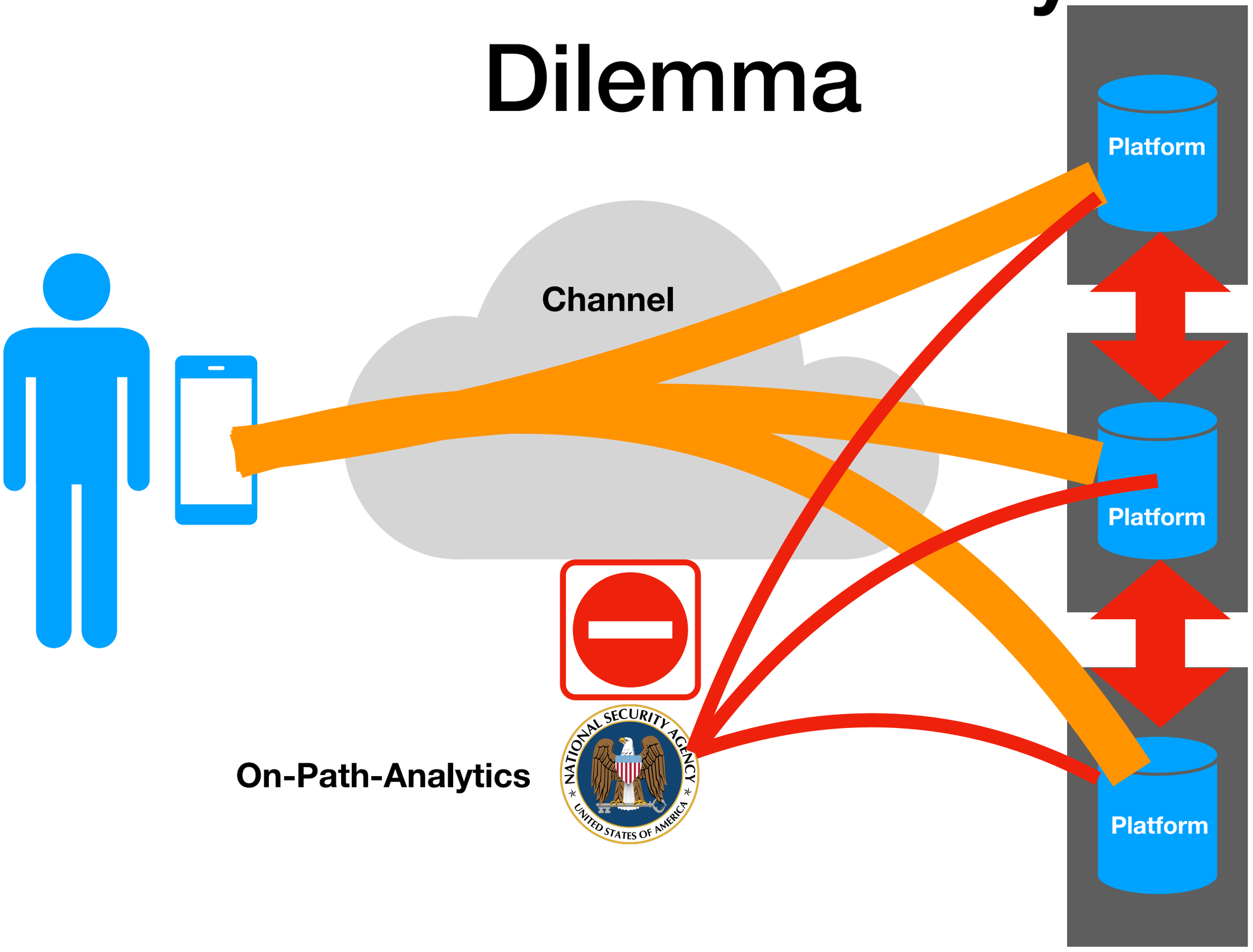
Denotes acquired company

Denotes shuttered company

The Confidentiality Dilemma



The Confidentiality Dilemma



Our Reaction So Far

[Docs] [txt|pdf|xml|html] [Tracker] [Email] [Diff1] [Diff2] [Nits]

Versions: 00 01 02 03

Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 7, 2020

S. Farrell
Trinity College Dublin
July 6, 2019

We're gonna need a bigger threat model
draft-farrell-etm-03

Abstract

We argue that an expanded threat model is needed for Internet protocol development as protocol endpoints can no longer be considered to be generally trustworthy for any general definition of "trustworthy."

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 7, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

[Docs] [txt|pdf|xml|html] [Tracker] [WG] [Email] [Nits]

Versions: 00

Internet Architecture Board (IAB)
Internet-Draft
Intended status: Informational
Expires: February 23, 2020

M. Nottingham
August 22, 2019

The Internet is for End Users
draft-iab-for-the-users-00

Abstract

This document explains why the IAB believes the IETF should consider end-users as its highest priority concern, and how that can be done.

Note to Readers

The issues list for this draft can be found at https://github.com/intarchboard/for-the-users

The most recent (often, unpublished) draft is at https://intarchboard.github.io/for-the-users

Recent changes are listed at https://github.com/intarchboard/for-the-users/commits/master

See also the draft's current status in the IETF datatracker, at https://datatracker.ietf.org/doc/draft-iab-for-the-users/

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on February 23, 2020.

Dirk Kutscher

Great Expectations

without comments

Protocol Design and Socioeconomic Realities

(~~PDF version~~)

The Internet & Web as a whole qualify as wildly successful technologies, each of which empowered by wildly successful protocols per RFC 5218's definition [1]. As the Internet & Web became critical infrastructure and business platforms, most of the originally articulated design goals and features such as global reach, permissionless innovation, accessibility etc. [5] got overshadowed by the trade-offs that they incur. For example, global reach —intended as enabling global connectivity — can also imply global reach for infiltration, regime change and infrastructure attacks by state actors. Permissionless innovation — motivated by the intention to overcome the lack of innovation options in traditional telephone networks — has also led us to permissionless surveillance and mass-manipulation-based business models that have been characterized as detrimental from a societal perspective.

Most of these developments cannot be directly ascribed to Internet technologies alone. For example, most user surveillance and data extraction technologies are actually based on web protocol mechanisms and particular web protocol design decisions. While it has been documented that some of these technology and standards developments have been motivated by particular economic interests [2], it is unclear whether different *Internet* design decisions could have led to a different, "better" outcome. Fundamentally, economic drivers in different societies (and on a global scale) cannot be controlled through technology and standards development alone.

This memo is thus rather focused on specific protocol design and evolution questions, specifically on the question how technical design decisions relate to socio-economic effects, and aims at providing input for future design discussions, leveraging experience from 50 years of Internet evolution, 30 years of Web evolution, observations from economic realities, and from years of Future Internet research.

IP Service Model

Systems Considerations

- **Suggest looking at bigger picture and starting more principled discussion**
- Consolidation/Centralization
  - Need a discussion without sensationalizing issues
  - Technical vs. economic factors
- **Control points in the network**
  - Censorship by authoritarian regime bad
  - Parental & enterprise control seems useful
- **For the user…**
  - Applications don’t want to trust the infrastructure
  - Can users trust the applications?
  - Role of operating systems…

Systems Considerations

Dirk Kutscher
<ietf@dkutscher.net>

HotRFC@IETF-106