

Welcome to the World of Standards



Doc: TBA

Source: Bob Briscoe, BT

Agenda item: Liaisons

For: Discussion

Internet Architecture Board; Report Back



I A B

IAB Stack Evolution Programme: interaction with NFV

Internet Architecture Board (IAB)

- Architecture and Liaison activity for the IETF



IAB Stack Evolution Programme

- Addressing near-impossibility of evolving the Internet stack

This talk

- Prepared in co-operation with our IETF liaison: Diego Lopez
- Recent IAB workshop: Stack Evolution in a Middlebox Internet (SEMI)
<<https://www.iab.org/activities/workshops/semi/>>
 - participants decided to reach out to NFV ISG
 - this update is given in my personal capacity
- More formal liaison or joint action could follow

1. Pervasive monitoring by government agencies

- Snowden revelations

2. The middlebox tussle

- two perceived drivers: security protection & business protection
- widespread blocking of IETF extensibility mechanisms
 - new e2e protocols (IP next header numbers) blocked, e.g. SCTP
 - new services (port numbers) blocked (often leaving only https and http)
 - new protocol option numbers blocked (e.g. TCP options like multipath)

IAB/IETF response in both cases:

- plans to encrypt and authenticate all end-to-end protocol fields and data
 1. protects privacy*
 2. enforces architecture
- unsolicited services might be useful, but they have no right to data visibility

* Nov 2013 [IAB recommendation](#) to harden Internet Confidentiality

🌐 Market in (virtualised) network functions could shrink

🌐 Need to define new interface(s)

- need to shift from unsolicited to solicited intervention
- signalling from app to network function, or vice versa
- in-band preferred, out-of-band maybe
- think "ICMP that works"

ICMP: Internet Control Message Protocol

- **freshness – protocol extensions should deploy faster**
 - protocol extension often not possible with hardware middleboxes
 - more systematic update practices as NFV becomes the norm
- **a voice for the middlebox industry**
 - NFV ISG brings most middlebox vendors and operators together
 - the first time the IETF can address this industry in one place

Downsides also recognised

- **staleness**
 - many virtual appliances will still be updated rarely or never
- **not central to scope of NFV ISG**
 - data plane interfaces specific to each network function
 - (but security ToR does address pervasive encryption)

Invitation to relevant IETF activities

- IETF WGs: httpbis, TAPS, tcpinc, TLS, tsvarea, PCP, ...?
- non-WG mailing list: Handling pervasive monitoring (PERPASS)
- Potential activities: MCIC, SPUD, middlebox detection & error collection, ...?
- Collectively forming decisions on
 - trust model
 - crypto coverage in protocol headers
- next IETF meeting, Dallas 22-27 Mar 2015.

IAB stack evolution programme*

- lead: Brian Trammel

TAPS:	TrAnsPort Services
tcpinc:	TCP INCreased security
TLS:	Transport Layer Security
tsvarea:	Transport Area Plenary
PCP:	Port Control Protocol
MCIC:	Multiparty Content Integrity & Confidentiality
SPUD:	Session Protocol Under Datagrams

NFV ISG activity?

joint NFV-IETF initiative?