# Scene Setting

Stephen Farrell
stephen.farrell@cs.tcd.ie
Trinity College Dublin
IETF security area director (one of 2)

Natasha Rooney
nrooney@gsma.com
GSMA Technologist

(Including purloined slides from Jari Arkko)

https://down.dsg.cs.tcd.ie/marnew

# Contents

- Goals
- Technical Background
- IETF
- GSMA
- Scope (for discussion!)

# Note Well

These slides and this presentation are NOT intended to provide a full or comprehensive description of the background, we assume you know that and we only need to highlight a few things and dispel a few possible misconceptions. Add more legal crap here if you want, so that it looks like the IETF Note Well. But why'd you want that?

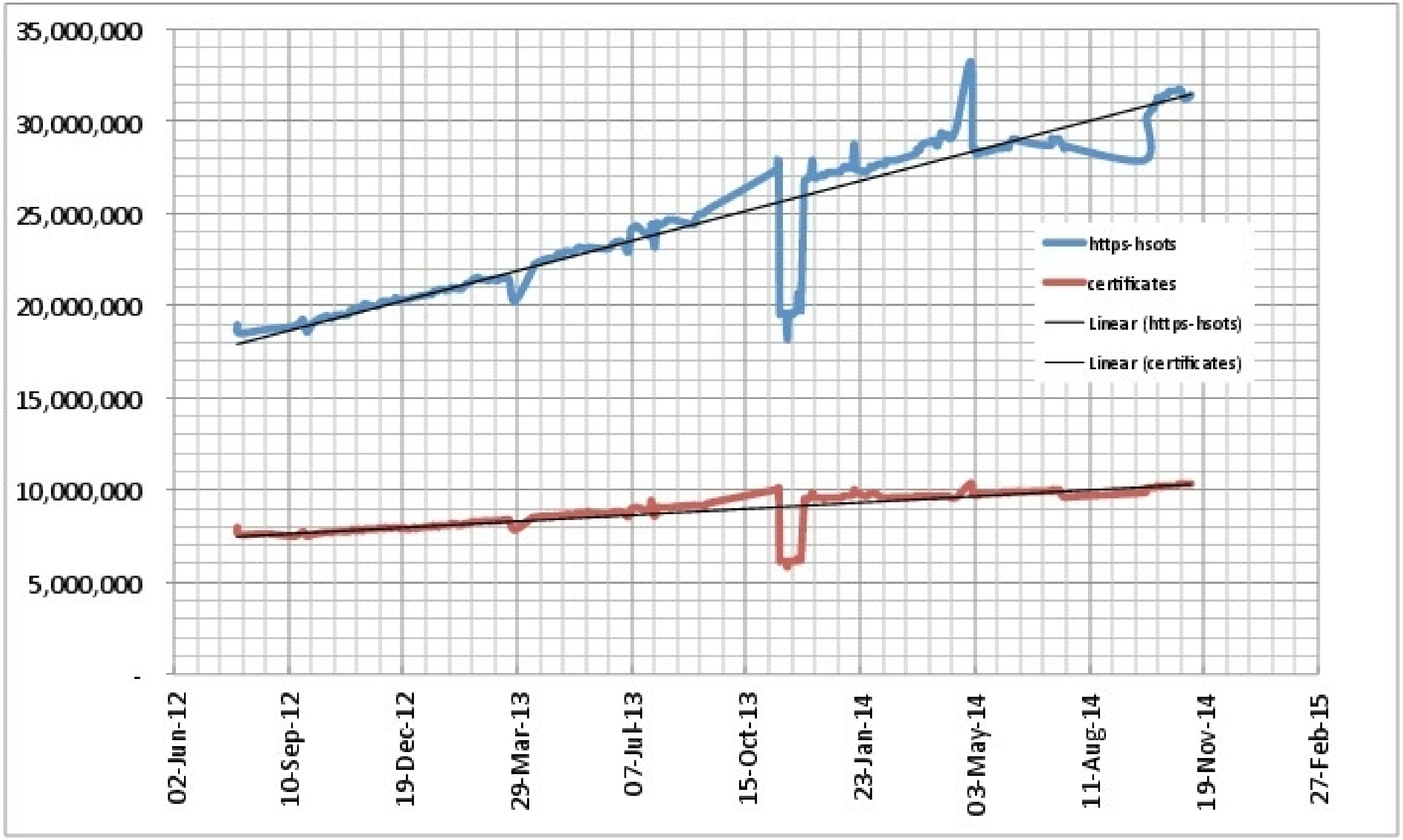
# Note Well

These slides and this presentation are NOT intended to provide a full or comprehensive description of the background, we assume you know that and we only need to highlight a few things and dispel a few possible misconceptions. Add more legal crap here if you want, so that it looks like the IETF Note Well. But why'd you want that?

# Goal of this slot

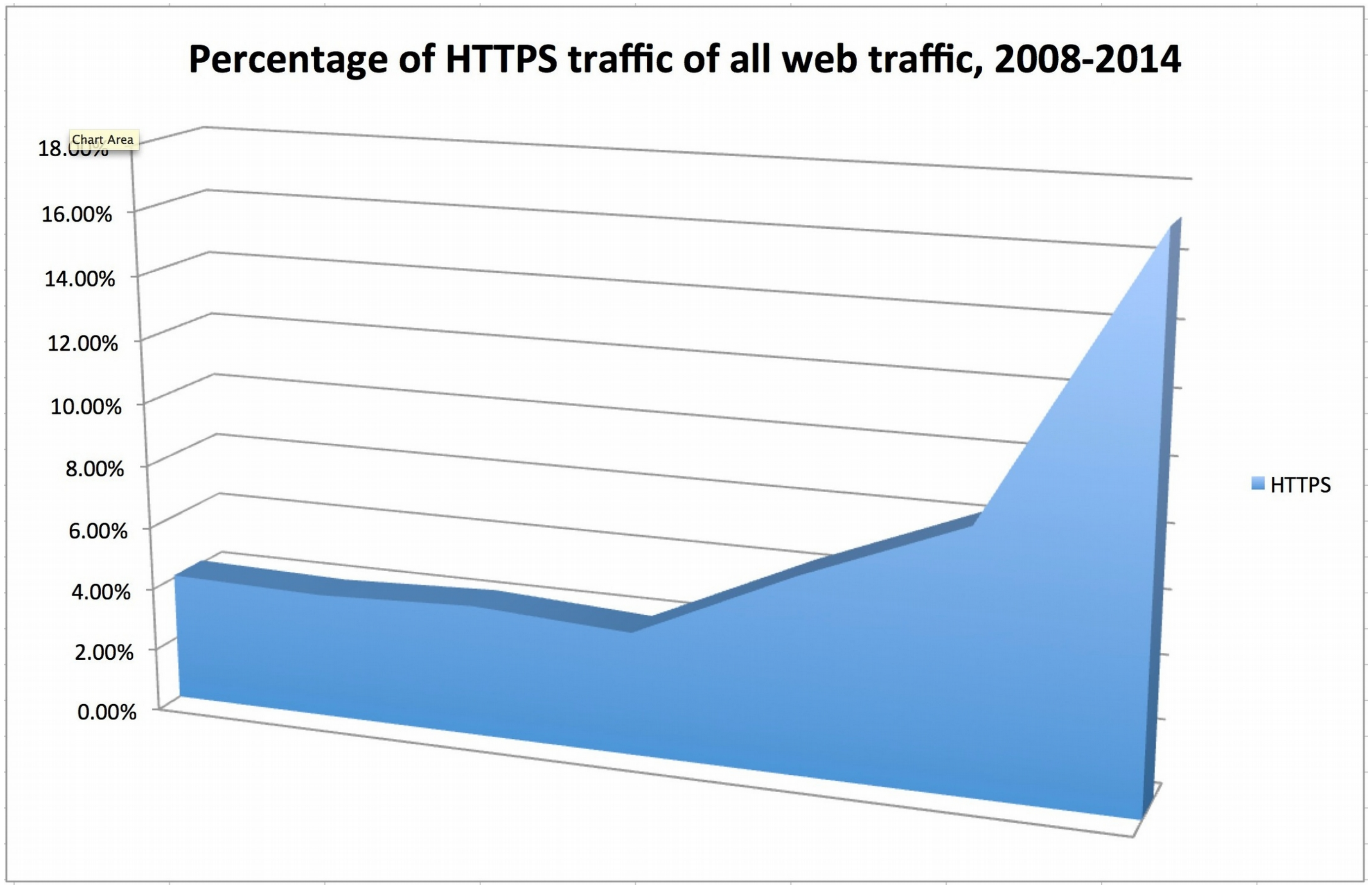
- Get (most of) us on the same page so we can be more productive
  - Both technical and process/organisational aspects to that
- Scope our discussions so we don't waste time with:
  - Unsolveable problems
  - Other people's problems
- Help focus so we're more likely to produce outputs that lead to improvements

# Statistics, Web Capability



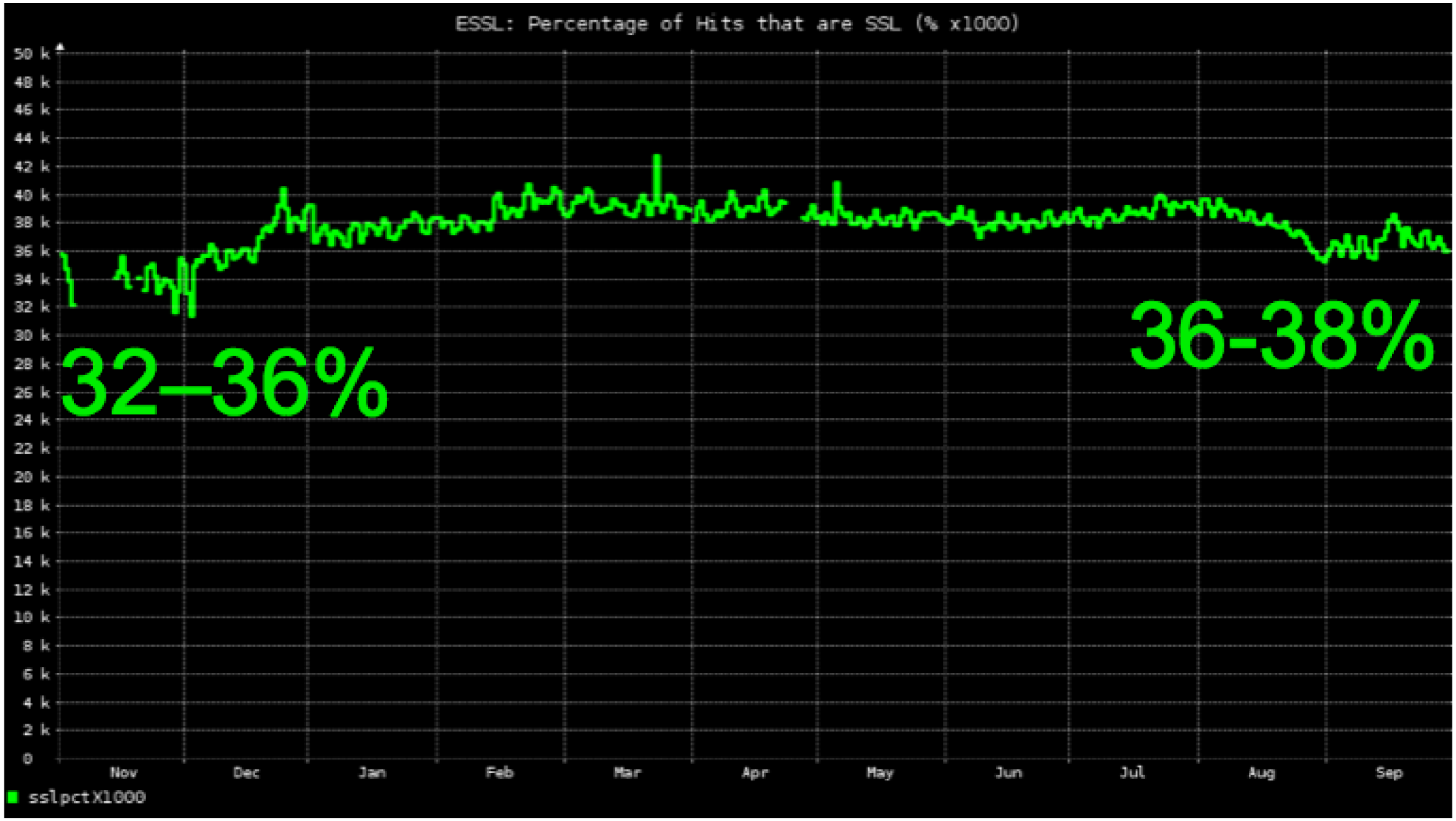
- Hosts responding to HTTPS on IPv4 scan and found certificates (Source: umich)

# Statistics, Web Traffic



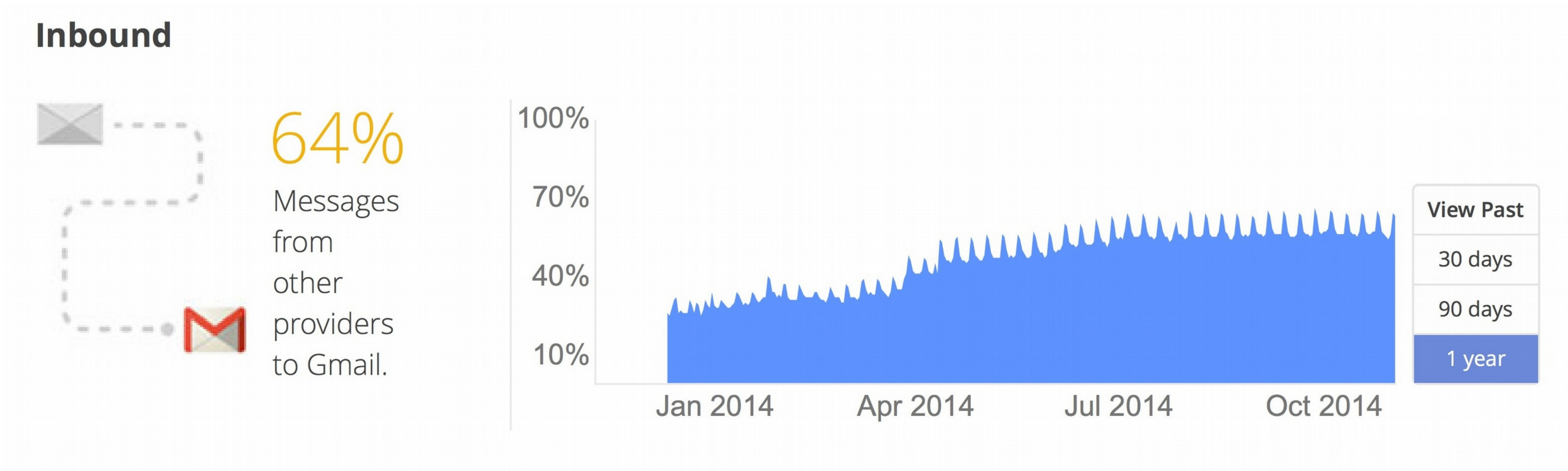
- HTTPS increased 4% to 17% from 2008 to 2014, for all web traffic (Source: IIJ)

# Statistics, Web-Traffic



- A CDN sees now 37% and expects 50% in two years (Source: Akamai)

# Statistics, E-Mail Traffic



Inbound

64%

Messages from other providers to Gmail.

- Gmail traffic encrypted from other e-mail providers rises from 27% to 64% since early 2013 (source: Google)

# Updates...

- The above are mostly from Summer 2014
- Updates for July 2015
  - https://www.ietf.org/proceedings/93/saag.html
- Mail: stable 80% out, 56% in for Google
  - https://www.google.com/transparencyreport/saferemail/
- Web: browser: 36% (pageload) to 55% (transaction) are TLS
- CDN: ~50% traffic is SSL

# A few caveats (1)

- Nobody sensible is talking about a fully-ciphertext Internet or web
  - Destination addresses at least need to be visible at the relevant layer
- We are talking about multiple layers of encryption becoming normal
  - WPA/802.1X, (MPLS-OS), VPN (IPsec or other), **TLS**, application layer
- We are also talking about identifiers at each layer becoming more privacy friendly, e.g. MAC address randomisation, DNS privacy, even SNI (likely only in some cases)
- DO NOT USE THE WORD “TRUST” WITHOUT QUALIFIERS!
  - Who is trusting whom for what? If you don't **always** say, the disussion will likely de-rail

# A few caveats (2)

- We do not have an Internet-scale way of managing keys for end-to-end encryption in many applications
- We do not have great ways of handling anti-spam or inbound malware detection when presented with ciphertext (but do we have any great ways of doing either?) - that'll push some functions from middle to edge
- Not being qualified, I'm not addressing transport issues, but some here are qualified and we'll need to consider those too

# Technical Overview

- Deployment of encryption is increasing for many reasons
  - More threatening environment, “powerful features,” Pervasive monitoring, avoiding middleboxes
- That is a trend that will continue and perhaps accelerate
- We should assume these are facts for this w/s
  - Even if one believed otherwise, it won't be productive to spend time arguing that
  - Instead, we're here to help figure out what might be done to make a world of mostly ciphertext better

# IETF Process Background

- 1996, RFC 1984, no broken crypto nor export control on crypto
- 2000, RFC 2804, says why IETF does not standardise wiretap
- 2002, RFC 3365, BCP 61 – strong security only
- 2003, RFC 3552, BCP 72, Guidelines for security considerations
- 2013, RFC 6973, Privacy considerations
- 2014, RFC 7258, BCP 188, Pervasive monitoring is an attack
- 2014, IAB statement on Internet confidentiality
- 2015, RFC 7525, BCP 195, Modern TLS guidelines
- 2015, RFC 1984, BCP xxx – RFC 1984 becomes a BCP

# IETF Process Background

- Nov 2013, Brian Carpenter's fine IETF-88 summary of the history to then:
  - https://www.ietf.org/proceedings/88/slides/slides-88-iab-techplenary-7.pdf
  - We've been here before. We think the high level analysis remains the same.
- May 2015, My summary of progress since IETF-88
  - https://down.dsg.cs.tcd.ie/misc/perpass-retreat-2015-final.pdf
  - Lots of different activities are under way to improve securiyt and privacy
- Main point: the underlying statements are technically worked out positions agreed over two decades that have undergone significant public debate. Changing those is extremely hard, regardless of what change one would like (and that is correct). Those technical positions do strongly influence IETF outputs.

# GSMA Process Background

- Over to Natasha!

# Suggested Scope (for discussion)

- In discussion we should assume: No broken crypto, Ciphertext increasingly common, congestion does need to be controlled as do other transport issues and Network mangement including efficient use of resources, in RAN and elsewhere, has to work
  - How/why is RAN different for transport; help us understand the complexities of the RAN and how hard it is to manage and why those matter
- What are the precise problems caused by more ciphertext
- Identify players, incl. Users, and resulting tensions and how ciphertext changes those
- Some solutions will be radically changed by ciphertext, it's ok to talk about that
- As good as possible Quality of experience for end user is a goal
- Our aim for the next two days is to analyse the sitiuation and identify specific achievable tasks that could be tackled in the IETF or GSMA (or elsewhere?) and that improve the Internet given the assumptions above
- We should not delve into:
  - Ways of doing interception (legal or not), see RFC2804 for why
  - Unpredictable political actions

DISCUSS...