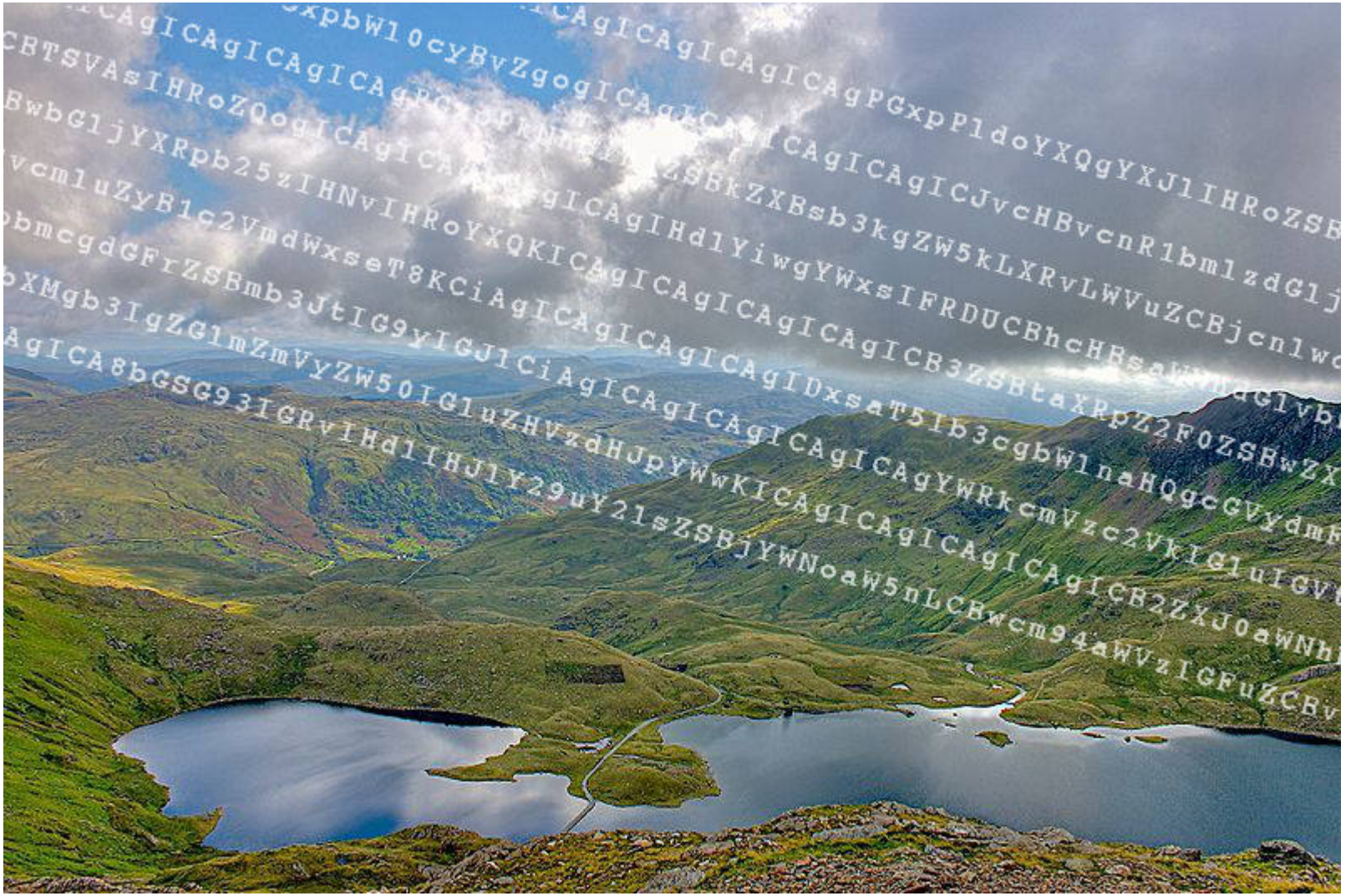
A W3C/IAB workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT)

28 February – 1 March 2014, London #strint



Welcome, Introduction, Logistics

Welcome

- We are here to figure out next steps in how to strengthen the Internet in the face of Pervasive Monitoring (PM)
- We want to do that via ***discussion*** and not by watching slideware
  - Use the mics to provide your input
    - NOTE WELL: state your name, there are remote folks
  - There are 100 of us, we do not have time for long-winded rambling statements
    - Be succinct, but do not be shy!
  - Sessions have presenters and moderators
    - Presenter goal: tee-up discussion then sit down while moderator leads that
    - Not strictly saying “clarifying questions only” but closer to that than wanting presenter on feet entire session

Goals

- We start from the perspective that **PM is an attack** (draft-farrell-perpass-attack)
  - Elucidating and discussing the consequences of that is fine, please do not (ab)use people's time here by re-running the Vancouver Plenary/IETF Last-Call discussion!
- Down one level, our goals for the next 1.5 days are:
  - Discuss and hopefully come to agreement among the participants on concepts in PM for both threats and mitigation, e.g., “opportunistic” as the term applies to cryptography.
  - Discuss the PM threat model, and how that might be usefully documented for the IETF at least, e.g., via an update to BCP72.
  - Discuss and progress common understanding in the trade-offs between mitigating and suffering PM.
  - Identify weak links in the chain of Web security architecture with respect to PM.
  - Identify potential work items for the IETF, IAB, IRTF and W3C that help mitigate PM.
  - Discuss the kinds of action outside the IETF/W3C context might help those done within the IETF/W3C.
- This slide will be **displayed again** in a few minutes, so just think about it for now!

Administrivia

- Badges: Keep your badge, you need it tonight and tomorrow!
- Audio: We are streaming audio out, mics are live always
- Photos: Go ahead, but please respect people's personal space!
- Social networking: Whatever
- Microphones: state your name!
- Power: share outlets! there's not enough
- Scribes: We need more! See Hannes!
- IRC Scribes: We need more! See Hannes!
- Break-outs: Start thinking now about those, talk during/after breaks
- Fire regs: we're allowed 100 in the room, can the rest of you leave? :-)

Communications

- IM: #strint on irc.w3.org (http://irc.w3.org is fine)
- Mail: strint-attendees@lists.i1b.org
- Web: https://www.w3.org/2014/strint/
- Audio: http://nagasaki.bogus.com:8000/stream10
- Slides: http://down.dsg.cs.tcd.ie/strint-slides/
- In meeting wifi:
  - SSID: STRINT
  - WPA: w3c-ietf

Agenda#1

14:00-14:30 Welcome, logistics, opening/overview

14:30-15:30 Threats – What problem are we trying to solve?

Presenter: Richard Barnes; Moderator: Cullen Jennings

What attacks have been described? (Attack taxonomy)

What should we assume the attackers' capabilities are?

When is it really PM and when is it not?

Scoping – what's in and what's out? (for IETF/W3C)

15:30-16:00 Break

Agenda#2

16:00-17:30 COMSEC 1 – How can we increase usage of current COMSEC tools?

- Presenter: Hannes Tschofenig; Moderator: Leif Johansson
- Whirlwind catalog of current tools
- Why aren't people using them?
- In what situations are / aren't they used?
- Securing AAA and management protocols – why not?
- How can we encourage more/better use?

Agenda#3

17:45-18:30 Policy – What policy / legal/ other issues need to be taken into account?

Moderators: Rigo Wenning/Christine Runnegar

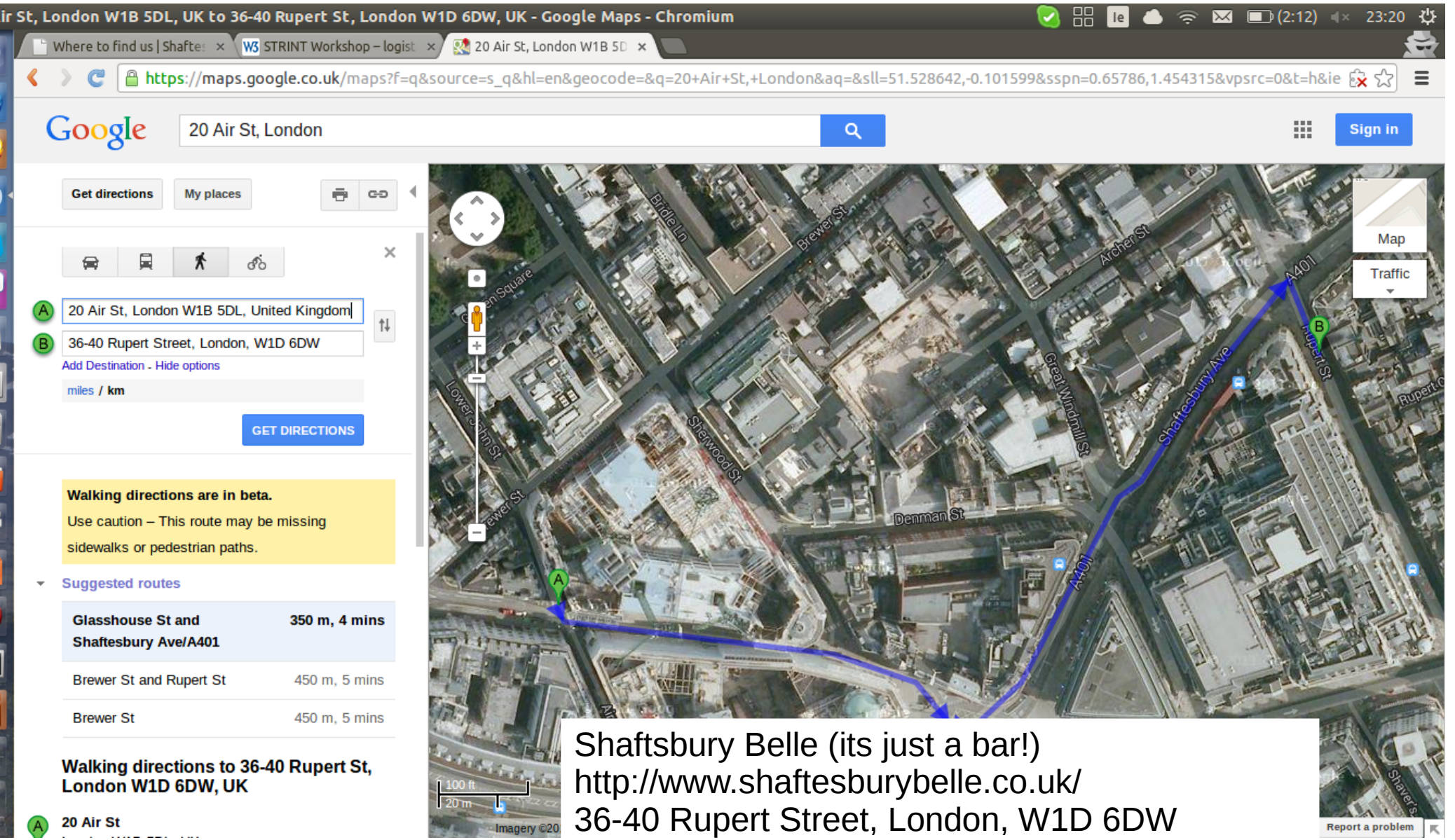
What non-technical activities do we need to be aware of?

How might such non-technical activities impact on IETF/W3C?

How might IETF/W3C activities impact on those non-technical activities?

18:30-19:00 Saturday plan, open-mic, wrap up day

Social Event - Friday



Shaftsbury Belle (its just a bar!)
http://www.shaftesburybelle.co.uk/
36-40 Rupert Street, London, W1D 6DW
Google says: 350m 4 minutes walk
Not full dinner; Bring your badge!

Agenda#4

09:00-09:15 Welcome again, logistics (chairs)

09:15-10:30 COMSEC 2 – What improvements to COMSEC tools are needed?

Presenter: Mark Nottingham; Moderator: Steve Bellovin

Opportunistic encryption – what is it and where it might apply

Mitigations aiming to block PM vs. detect PM – when to try which?

10:30-10:45 Quick Break

10:45-12:00 Metadata – How can we reduce the metadata that protocols expose?

Presenter: Alfredo Pironti/Ted Hardie; Moderator: Alissa Cooper

Meta-data, fingerprinting, minimisation

What's out there? How can we do better?

12:00-13:00 Lunch (Buffet)

Agenda#5

13:00-14:30 Deployment – How can we address PM in deployment / operations?

Presenter: Eliot Lear; Moderator: Barry Leiba

"Mega"-commercial services (clouds, large scale email & SN, SIP, WebRTC…)

Target dispersal – good goal or wishful thinking?

Middleboxes: when a help and when a hindrance?

14:30-15:00 Break

15:00-16:15 3 x Break-out Sessions / Bar-Camp style (Hannes Tschofenig)

Content to be defined during meeting, as topics come up

16:15-16:30 Break-out reports

16:30-17:15 Open mic & Conclusions – What are we going to do to address PM?

Gather conclusions / recommendations / goals from earlier sessions

Break Outs

Break-out#1 – Research Questions

- Moderator: Kenny Paterson
- Do we need more/different crypto tools?
- How can applications make better use of COMSEC tools?
- What research topics could be handled in IRTF?
- What other research would help?

Break-out#2 – TBD

Break-out#3 – TBD

Thanks!

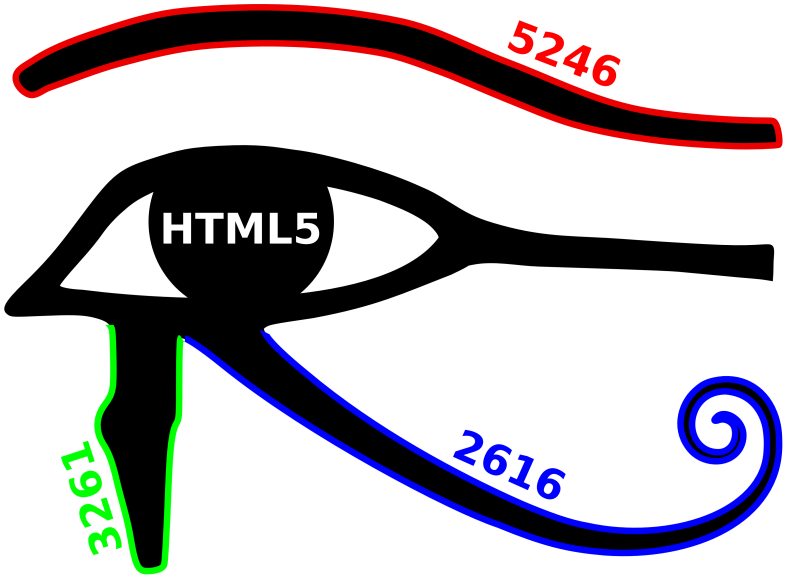
- To you for the 66 submissions
- To you for coming along today and contributing
- To the TPC for reviewing the submissions and arranging the agenda
- To the EU/STREWS for helping
- To Telefonica (Dan!) for hosting
- To the IETF NOC folks (Hans) for audio out help
- Dana and Greg for helping
- To IAB/W3C for sponsoring

The TPC:

Bernard Aboba
Dan Appelquist
Richard Barnes
Bert Bos
Lieven Desmet
Stephen Farrell
Karen O'Donoghoue
Russ Housley
Martin Johns
Ben Laurie
Eliot Lear
Kenny Paterson
Eric Rescorla
Wendy Seltzer
Dave Thaler
Hannes Tschofenig
Sean Turner
Rigo Wenning

Goals

- We start from the perspective that **PM is an attack** (draft-farrell-perpass-attack)
  - Elucidating and discussing the consequences of that is fine, please do not (ab)use people's time here by re-running the Vancouver Plenary/IETF Last-Call discussion!
- Down one level, our goals for the next 1.5 days are:
  - Discuss and hopefully come to agreement among the participants on concepts in PM for both threats and mitigation, e.g., “opportunistic” as the term applies to cryptography.
  - Discuss the PM threat model, and how that might be usefully documented for the IETF at least, e.g., via an update to BCP72.
  - Discuss and progress common understanding in the trade-offs between mitigating and suffering PM.
  - Identify weak links in the chain of Web security architecture with respect to PM.
  - Identify potential work items for the IETF, IAB, IRTF and W3C that help mitigate PM.
  - Discuss the kinds of action outside the IETF/W3C context might help those done within the IETF/W3C.
- Time to start discussing these goals (Well, for 10 minutes now, more later)



Strengthening the Internet
Against Pervasive Monitoring

London, 28 Feb – 1 Mar 2014
https://www.w3.org/2014/strint