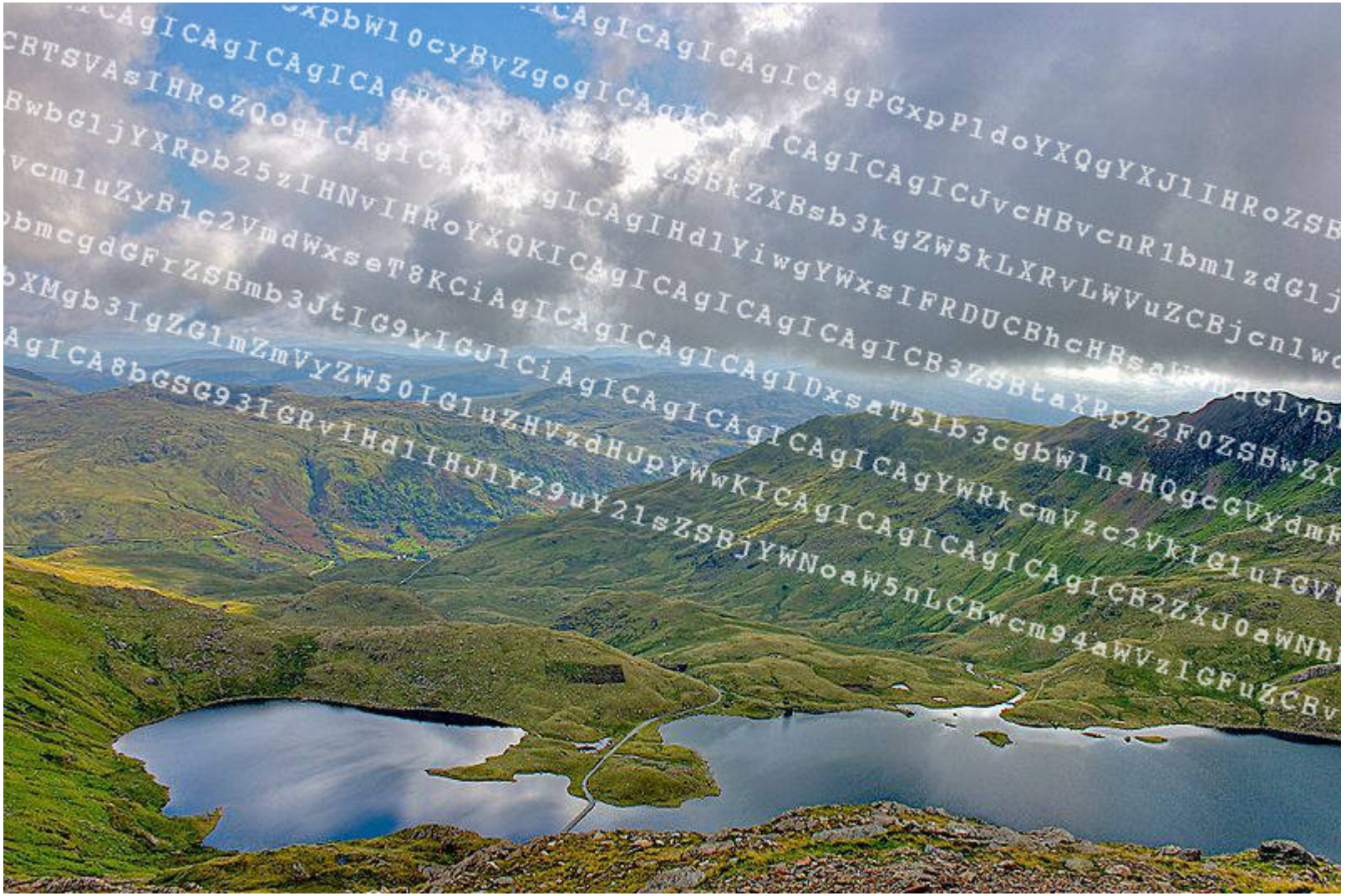
A W3C/IAB workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT)

28 February – 1 March 2014, London #strint



IETF89 saag Summary

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.

Various Links

- 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/

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

Summary#1

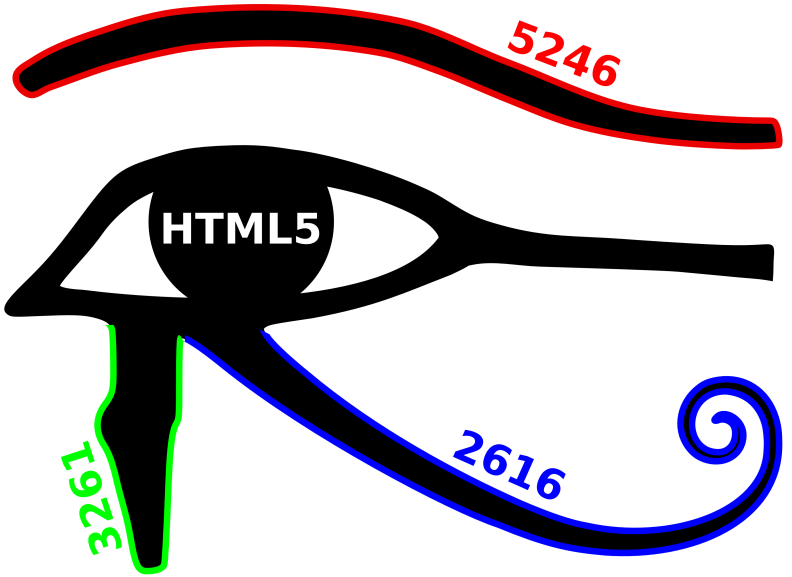
- Crypto works, do more, raise-the-bar as Russ said?
  - “Tor stinks” :-)
  - Crypto is not free, but is worth it, and getting cheaper
  - Middleboxes as ever
- Data minimization is worthwhile but hard
  - Try XMPP if willing victims exist; There is traffic analysis literature
- Threat model → RFC
  - Include traffic analysis issues (more?)
- Opportunistic keying definition and maybe mechanism cookbook→ RFC
  - Requiring a tight coupling of authentication and ability to encrypt not a good plan

Summary#2

- Policy: technical community could do better to explain PM related issues to policy makers
- UI issues not out of scope of workshop – how to reflect that in IETF/W3C?
- Good if someone creates new security guidance and gamification of protocol use
  - Copy-and-paste guidelines (BetterCrypto.org); can IETF help? Not necessarily RFC material
- Easier security configuration (esp for servers) can help privacy
  - Out-of-box, maybe more-than-MTI
- Can we improve captive portals? Maybe scope for protocol work
- We should add a new RFC to BCP 72 (RFC 3552)
  - Not ready for that yet, think about when?

Break Outs

- Opportunistic Keying
- More-than-MTI/On-by-default
- World-ipv6-day: s/IPv6/browser-hard-fail/
- Crypto researcher interest
- Traffic Analysis researcher interest



Strengthening the Internet
Against Pervasive Monitoring

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