STRINT Summary Slides

Thanks!

- We knew we could depend on you for discussion!
- Dan/Telefonica for hosting!

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