Parantaisiko tekniikka Internetin tietosuojaa?

Jari Arkko

puheenjohtaja, IETF
Internet-asiantuntija, Ericsson Research

I. Taustaa laajamittaisesta valvonnasta
II. Tekniikan rooli
III. IETF:n työ tietosuojan parantamiseksi

Keskustelun taustaksi

- IETF tai muut tekniset organisaatiot eivät ole poliittisen keskustelun paikkoja
- Ja on syytä olla varovainen tekemästä liian nopeita tulkintoja uutistietojen perusteella; ongelmat maailmassa ovat laajoja
- Mutta meidän PITÄÄ kuitenkin ymmärtää mitä uhkia Internet-liikenteellä on ja kehittää tekniikka vastaamaan niihin

Haavoittuvuuksia, jotka mahdollistavat tiedustelun

- Suojaamaton tietoliikenne (yllätys???)
- Pilven sisäinen tietoliikenne
- Suora pääsy toisen osapuolen palvelimeen
- Suora pääsy avainmateriaaliin (esim. lavabit?)
- Kolmannet osapuolet (esim. varmenne)
- Ohjelmiston haavoittuvuudet (esim. RNG)
- Heikot standardit (esim. Dual_EC_DBRG)

Tiedustelu on kuin mikä tahansa tietosuojaan kohdistuva hyökkäys

- ... tai ainakaan sitä ei voida erottaa hyökkäyksistä
- Saatua tietoa voidaan käyttää hyvään tai pahaan, vrt. salasanojen varastaminen
- Motiiveista riippumatta hyökkäyksiä vastaan joudutaan varautumaan samalla tavalla
- IP-tekniikka vs. tiedustelu ei ole uusi asia (vrt. RFC 3365)

Voivatko tietoliikenneinsinöörit tai tutkijat auttaa?

- Teknologia auttaa, tietyissa rajoissa (luotatko keskustelun toiseen puoleen?)
- Joidenkin hyökkäyksien esto tai tekeminen vaikeammiksi (passiivinen->aktiivinen jne.)
- Internetin tietoturvaa on ollut vaikea parantaa - tämän vuoden keskustelu tarjoaa myös tilaisuuden tehdä muutoksia

Mitä sitten voitaisiin tehdä?

- Suojaamaton tietoliikenne - suojaa se!
- Heikot standardit - julkiset, avoimet kehitysprosessit, vanhojen algoritmien poisto, ...
- Takaportit ja heikkoudet toteutuksissa - eri toteutuksia, avoin lähdekoodi, katselmointi, ...

Mitä IETF tekee?

- Keskustelee asiasta - avoimesti
  - PERPASS, Plenary, IAB WS, WGs, ...
- Tutkii ongelmaa ja mahdollisia ratkaisuja
  - Lista http://down.dsg.cs.tcd.ie/misc/perpass.txt
- Spesifisiä ehdotuksia
  - Algoritmien päivitykset
  - HTTP 2.0, TLS 1.3 (aloitettu jo aiemmin)
  - ...

Isoimmat odotettavissa olevat muutokset

- Monet palvelut ovat siirtyneet TLS:n käyttöön viime vuosina - nyt tämä trendi kiihtyy
- TLS algoritmien päivitys & PFS - toteutukset ja speksit
- Tietoturva automaattisesti päälle HTTP 2.0:ssa?
  - Uusi protokolla vain HTTPS-linkeille
- Sovellukset (mm. pikaviestit ja sähköposti; UTA WG)
- TLS 1.3

Haasteita

- Sähköposti: end-to-end tietoturva
- Web: Välityspalvelimet (proxy), varmentaja-listat (CA)
- WebRTC, VoIP, Internet of Things: vasta kehittymässä, riskit eivät täysin tunnettuja
- Päätelaitteiden, käyttöjärjestelmien, jne. turvallisuus
- Kansalliset Internetit

Lisätietoja

- Bruce Schneier esitelmöi asiasta: http://www.ietf.org/live
- Liity IETF:n sähköpostilistoille:
  - PERPASS: https://www.ietf.org/mailman/listinfo/perpass
  - APPSAWG: http://tools.ietf.org/wg/appsawg
  - HTTPBIS: http://tools.ietf.org/wg/httpbis
  - TLS: http://tools.ief.org/wg/tls
- Blogini http://www.ietf.org/blog

Kiitos