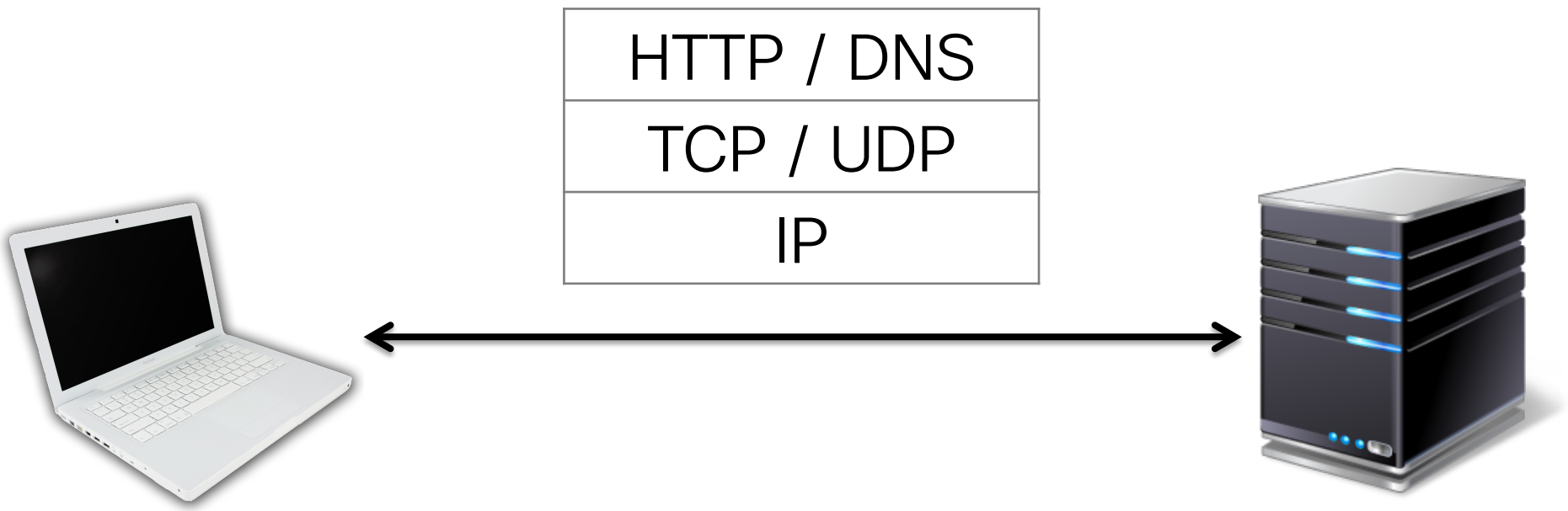
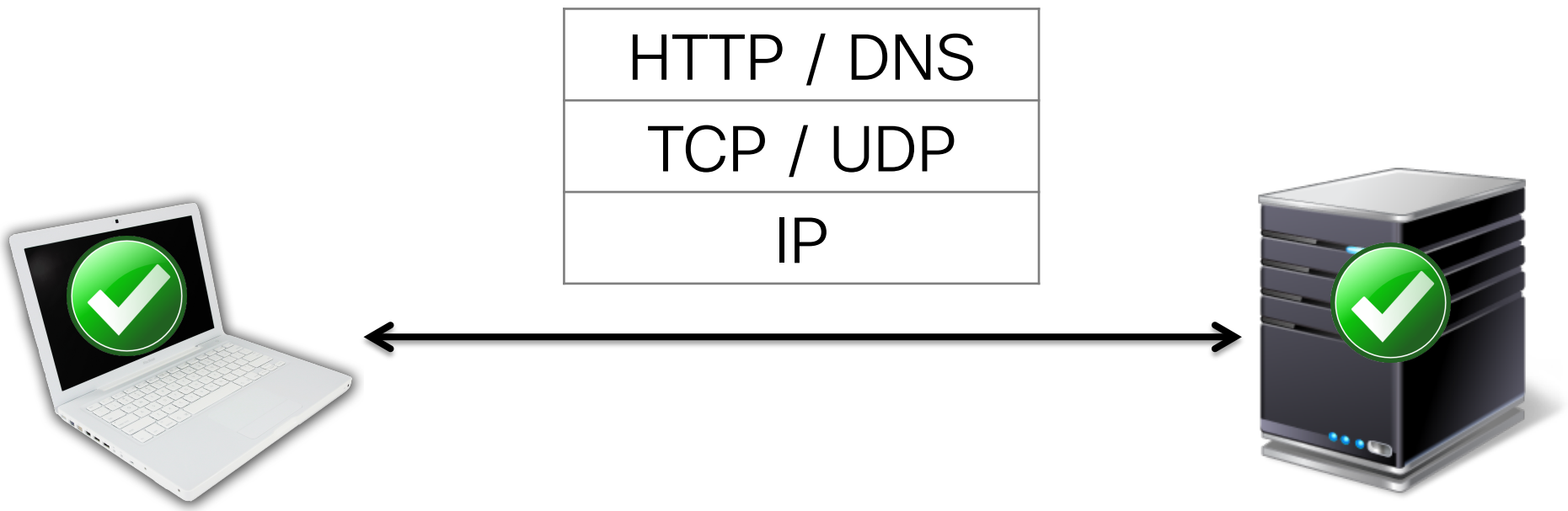
Privacy in the Internet Engineering Task Force

Alissa Cooper

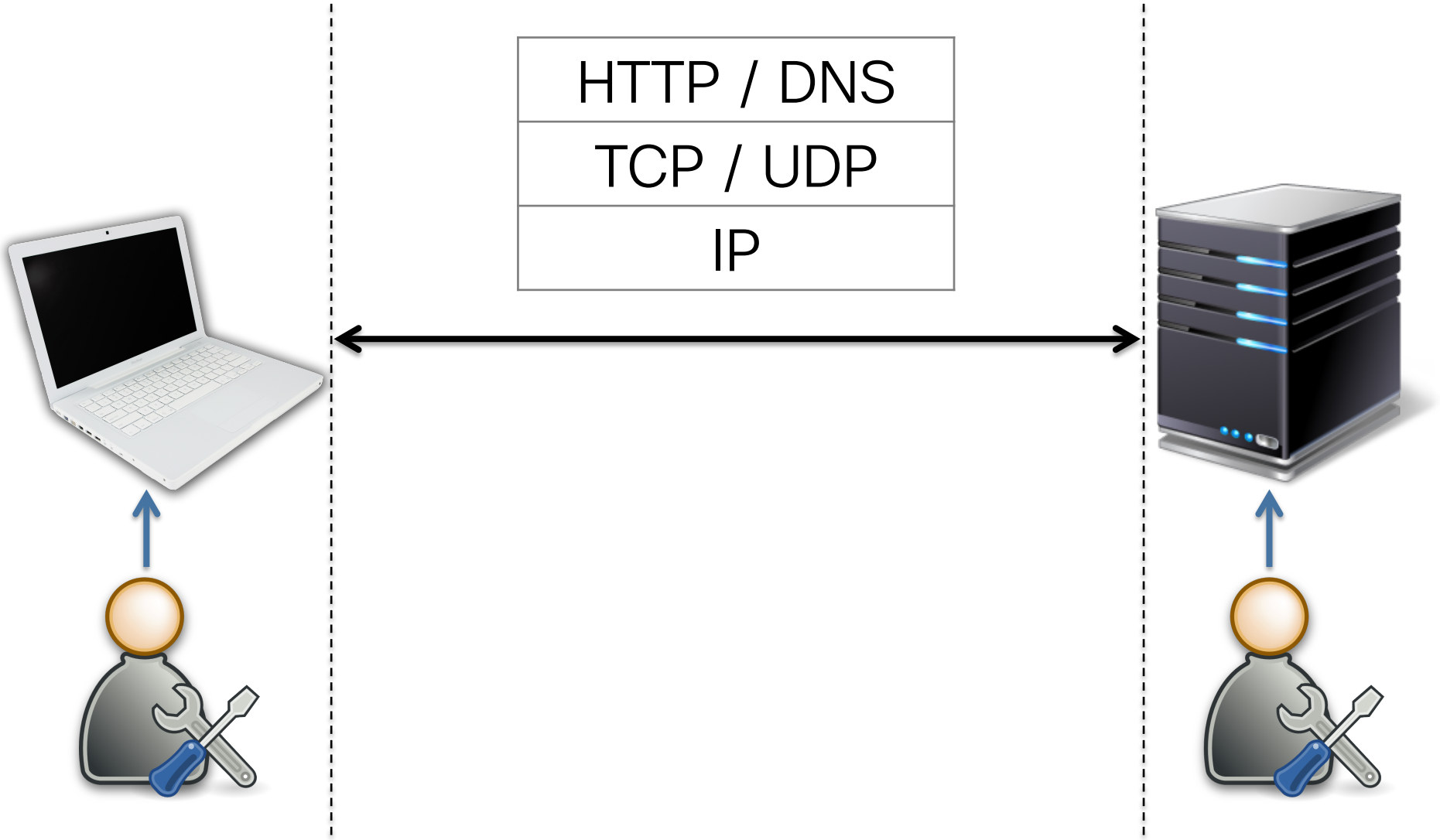
What the IETF does



What the IETF does



What the IETF does



Historic areas of focus

Confidentiality

Data integrity

Authentication

Historic areas of focus

Confidentiality

Data integrity

Authentication

Communications privacy threats mitigated:
surveillance, interception, spoofing, etc.

Information privacy threats not so much:
identification, correlation, disclosure, secondary use, etc.

Early years

Security Considerations

Security issues are not discussed in this memo.

Some security history

- 1993: Every spec must include security considerations (RFC 1543). But no guidance about what to include.
- 2003: Detailed guidance and threat model published (RFC 3552).
- Supportive IETF culture evolved.
  - Security Directorate (SecDir) reviews every spec before publication.
  - Security advisors can be assigned to working groups.
  - Security Area Advisory Group (SAAG) meetings and security tutorials at IETF meetings.

Security Area Directors, 1980s-2008

Policy history

- 1996: Statement on Cryptographic Technology (RFC 1984)
  - “encourage policies that allow ready access to uniform strong cryptographic technology for all Internet users in all countries”
- 2000: IETF Policy on Wiretapping (RFC 2804)
  - “The IETF has decided not to consider requirements for wiretapping as part of the process for creating and maintaining IETF standards.”

Some information privacy history

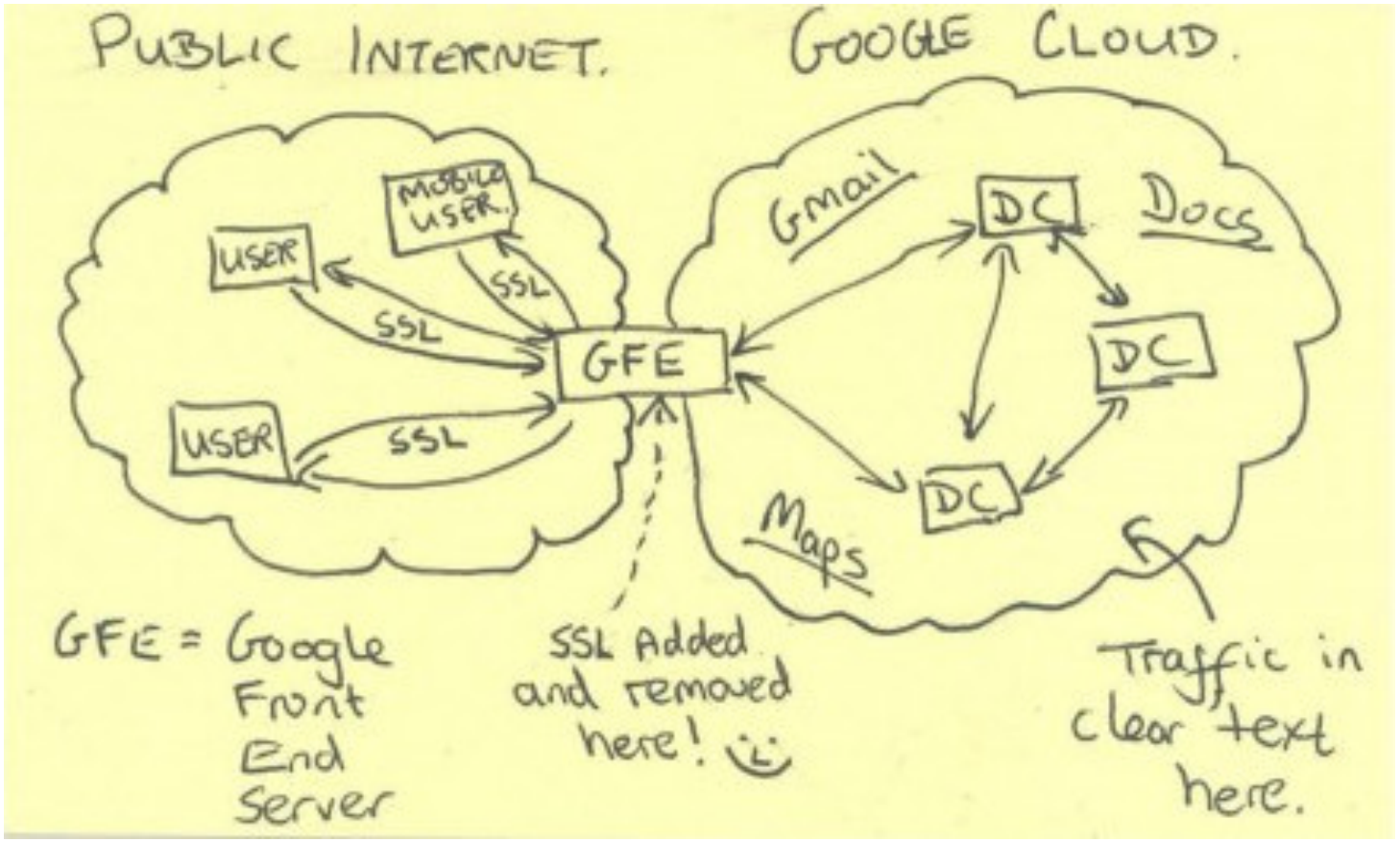
- Until recently: Ad hoc treatment
  - IPv6 “Privacy Addresses” (RFC 3041/4941)
  - SIP privacy extensions (RFC 3323/3325)
- 2010: IAB Privacy Program formed
  - Workshop, plenary talks, liaising with other standards groups
- 2013: Privacy Considerations for Internet Protocols (RFC 6973)

Privacy Considerations for Internet Protocols

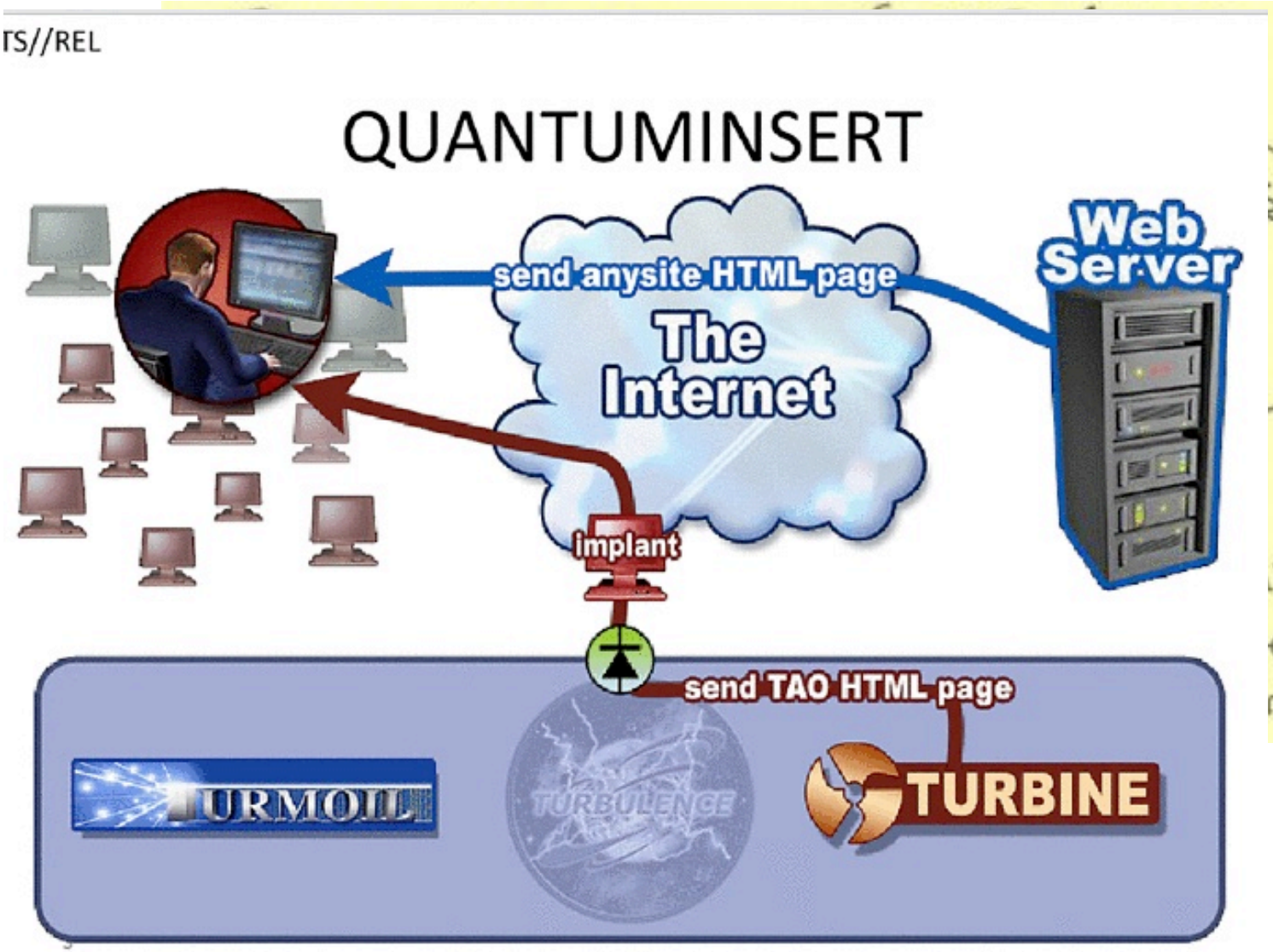
- Terminology
- Threat Model
  - Combined Security-Privacy Threats: surveillance, stored data compromise, intrusion, misattribution
  - Privacy-Specific Threats: correlation, identification, secondary use, disclosure, exclusion
- Threat Mitigations
  - Data minimization: anonymity, pseudonymity, identity confidentiality
  - User participation
  - Security
- Guidelines
  - Identifiers, persistence, fingerprinting, correlation, retention, user controls, defaults, etc.

Some information privacy history

- Until recently: Ad hoc treatment
  - IPv6 “Privacy Addresses” (RFC 3041/4941)
  - SIP privacy extensions (RFC 3323/3325)
- 2010: IAB Privacy Program formed
  - Workshop, plenary talks, liaising with other standards groups
- 2013: Privacy Considerations for Internet Protocols (RFC 6973)
- Supportive culture harder to cultivate for information privacy, but we’ve been trying.
  - Issues and expertise more diffuse
  - Guidance inherently less concrete
  - Really hard problems: traffic analysis, fingerprinting, ...
- Something else happened in summer 2013 ...


PUBLIC INTERNET.
GOOGLE CLOUD.
MOBILE USER.
USER
USER
SSL
SSL
SSL
GFE
Gmail
DC
Docs
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here!
Traffic in clear text here.

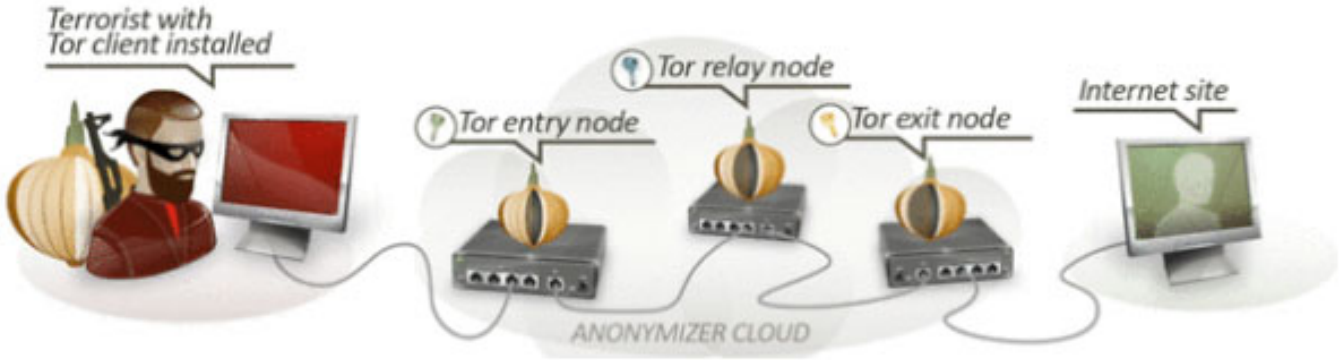
TS//REL

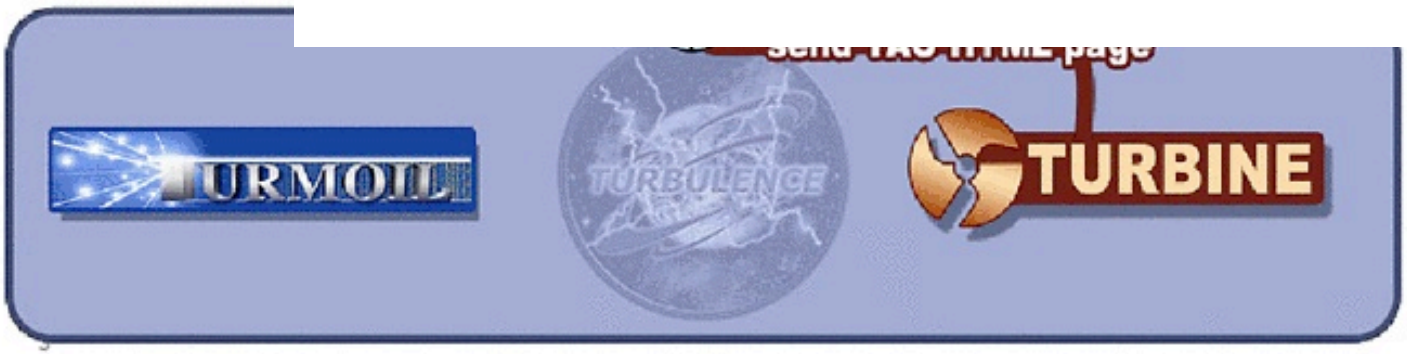

QUANTUMINSERT
send anysite HTML page
The Internet
Web Server
implant
send TAO HTML page
TURMOIL
TURBULENCE
TURBINE

TS//REL

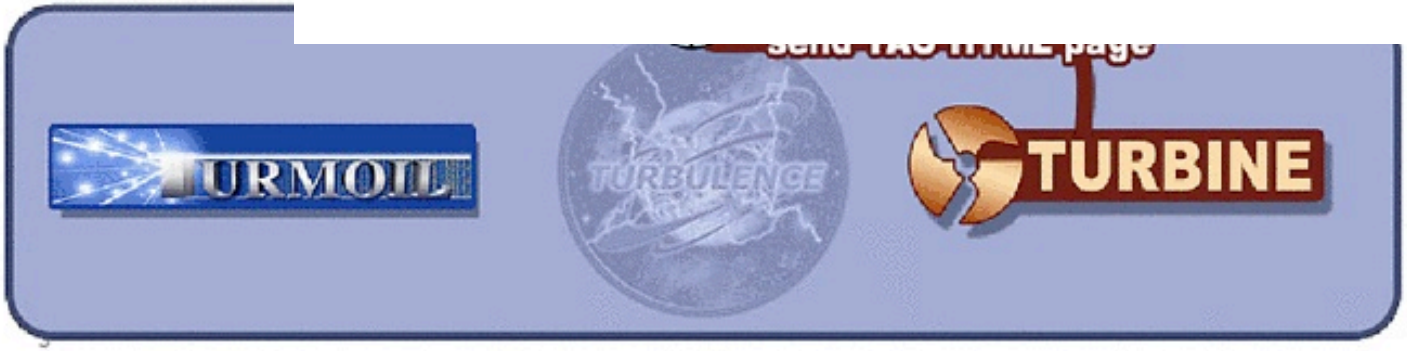
TOP SECRET//COMINT// REL FVEY

Analytics: Circuit Reconstruction (S//SI)





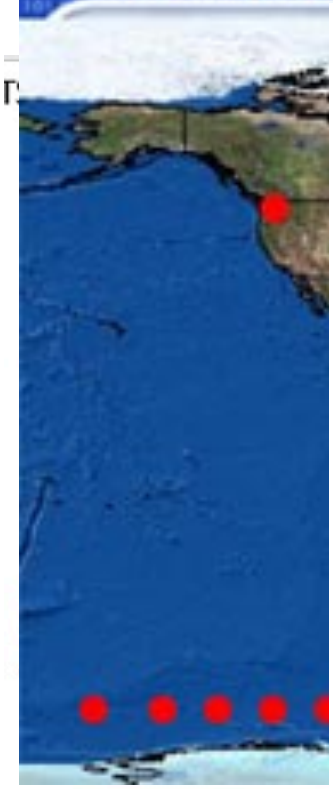
(S//SI)



or text here.

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Where is X-KEYSCORE?



TOP SECRET//SI//ORCON//NOFORN

Gmail facebook Hotmail Google YAHOO! skype paltalk.com YouTube AOL mail

(TS//SI//NF) FAA702 Operations

Two Types of Collection

PRISM

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.

(FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

You Should Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

TOP SECRET//SI//ORCON//NOFORN

Speaking of supportive culture …

- RFC 7258: “Pervasive monitoring is an attack”
- RFC 7435 on “Opportunistic Security:” use encryption whenever possible even if not perfect.
- IAB Statement on Confidentiality: encrypt everything!
- New work
  - Best choice cryptographic ciphers and modes
  - Encryption for DNS requests
  - Encryption for TCP
- Increased use of Crypto Forum Research Group (CFRG)
  - Need crypto algorithms everyone can trust.
- Refactored IAB Privacy and Security Program
  - Pervasive monitoring threat model

References

- A Privacy Mechanism for the Session Initiation Protocol (SIP) (RFC 3323). http://tools.ietf.org/html/rfc3323
- Guidelines for Writing RFC Text on Security Considerations (RFC 3552). http://tools.ietf.org/html/rfc3552
- IAB and IESG Statement on Cryptographic Technology and the Internet (RFC 1984). http://tools.ietf.org/html/rfc1984
- IETF Policy on Wiretapping (RFC 2804). http://tools.ietf.org/html/rfc2804
- Instructions to RFC Authors (RFC 1543). http://tools.ietf.org/html/rfc1543
- Opportunistic Security: Some Protection Most of the Time (RFC 7435). http://tools.ietf.org/html/rfc7435
- Pervasive Monitoring Is an Attack (RFC 7258). http://tools.ietf.org/html/rfc7258
- Privacy Considerations for Internet Protocols (RFC 6973). http://tools.ietf.org/html/rfc6973
- Privacy Extensions for Stateless Address Autoconfiguration in IPv6 (RFC 3041). http://tools.ietf.org/html/rfc3041
- Privacy Extensions for Stateless Address Autoconfiguration in IPv6 (RFC 4941). http://tools.ietf.org/html/rfc4941
- Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks (RFC 3325). http://tools.ietf.org/html/rfc3325
- Simple Network Management Protocol (RFC 1157). http://tools.ietf.org/html/rfc1157

Thank you

alcoop@cisco.com