Privacy in the Internet Engineering Task Force

Alissa Cooper
What the IETF does

<table>
<thead>
<tr>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP / DNS</td>
</tr>
<tr>
<td>TCP / UDP</td>
</tr>
<tr>
<td>IP</td>
</tr>
</tbody>
</table>
What the IETF does

<table>
<thead>
<tr>
<th>HTTP / DNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP / UDP</td>
</tr>
<tr>
<td>IP</td>
</tr>
</tbody>
</table>
What the IETF does

<table>
<thead>
<tr>
<th>HTTP / DNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP / UDP</td>
</tr>
<tr>
<td>IP</td>
</tr>
</tbody>
</table>
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.
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.
Policy history

  - “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

GFE = Google Front End Server

SSL Added and removed here! 😊

Traffic in clear text here.
QUANTUMINSERT

Web Server

The Internet

send anysite HTML page

implant

send TAO HTML page

TURMOIL

TURBULENCE

TURBINE
Analytics: Circuit Reconstruction (S//SI)
Where is X-KEYSCORE?
Where is X-KEYSCORE?

(TS//SI//NF) FAA702 Operations
Two Types of Collection

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.
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

Thank you

alcoop@cisco.com