We’ve been here (or nearby) before

IETF Technical Plenary, November 2013

Brian Carpenter

Ancient traditions

- “Security issues are not addressed in this memo” (RFC1126,1989)
- “All RFCs must contain a section near the end of the document that discusses the security considerations...” (RFC1543,1993)
- “if we wish to eliminate the phrase "security issues are not discussed in this memo" from future RFCs,we must provide guidance...” (RFC2316,1998)

Early efforts

- It’s easy to sneer at the IETF for not taking security seriously before 1998, but unfair, e.g.
  - RFC1244 “Site Security Handbook” in 1991.
  - First IPsec and S/MIME RFCs in 1995
- Nevertheless, there was a general tendency to ignore security issues, including confidentiality and privacy, until the late 1990s.
- That left a legacy of protocols and operational practices that were unfavourable to privacy.

In fairness to the IAB

- First security workshop, 1994 (RFC 1636)
- Second security workshop, 1997 (RFC 2316)
  - Leading to RFC 3365, Strong Security Requirements for IETF Standard Protocols, 2002.
- Privacy workshop, 2010 (RFC 6462)
  - Leading to RFC 6973, Privacy Considerations for Internet Protocols, July 2013

Public policy impact #1

- In the mid 1990s, it was quite clear that a secure Internet needed to use strong cryptography (as did secure e-commerce).
- But many governments, influenced by signals intelligence agencies, wanted to restrict use of strong crypto.
- This shackled the IETF in many discussions:
  - As in “We can’t do that because it’s illegal in France” (it was never just the NSA).

Outcome #1

- In 1996, there was a long debate in the IETF; we even had a speaker from the NSA.
  - The plenary discussion took place in Salem, Mass., home of the witch trials (now known as Danvers).
- The result was RFC 1984, signed by the IAB & IESG.
- Key recommendation: “encourage policies that allow ready access to uniform strong cryptographic technology for all Internet users in all countries.”
- I assume that the signals intelligence agencies were not amused.

Public policy impact #2

- In 1999/2000, there were recurrent requests to document features for wiretapping (“legal intercept”) in IETF specifications.
- Evidently, many governments, influenced by police and signals intelligence agencies, wanted to observe traffic.
- This bothered people in the IETF
  - privacy concerns & potential for misuse
  - wiretapping features would increase security loopholes

Outcome #2

- Another long debate in the IETF
  - It was said that in some countries, operators & vendors would be legally forced to provide wiretaps.
- The result was RFC 2804, signed by the IAB & IESG.
- Key recommendation: “The IETF has decided not to consider requirements for wiretapping as part of the process for creating and maintaining IETF standards.”
  - But “the IETF does not take a moral position”
  - And wiretapping mechanisms “should be openly described”
- I assume that the police and signals intelligence agencies were not amused.

Is there an underlying principle?

- It seems that the common theme of RFC 1984 and RFC 2804 is this:

  IETF technology should be able to make the Internet secure (including the ability to protect privacy) but should be neutral with respect to varying cultural views of legality and privacy.

Personal comment

- I expect we'll have another long debate.
- I hope for significant improvements in privacy protection in future IETF specifications.
- I assume that the police and signals intelligence agencies will not be amused.