Security in the IETF

Russ Housley

IETF Chair

Vigil Security LLC

8 December 2010

Definition of Privacy

- RFC 2828 (“Internet Security Glossary”) has a reasonable definition of privacy:

$ privacy

(I) The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others. (See: anonymity.)

(O) "The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed." [I7498 Part 2]

Security Considerations

- RFC 2223 (and RFC 1543 before it) provides Instructions to RFC Authors; it requires a Security Considerations section in all RFCs
- But, neither RFC provides much guidance:

  "All RFCs must contain a section near the end of the document that discusses the security considerations of the protocol or procedures that are the main topic of the RFC."

Interpretation: 1st SEC AD

At the time, I think my view of "privacy" was that it was one the several attributes to be included within "security" though I realize that's not how it's viewed today and may not have been the shared view even then.

Steve Crocker

Interpretation: 2nd SEC AD

Compared to privacy, security is trivial. Most people have some sense of what security means, and we even have some definitions and particulars. Privacy, by comparison, is a much more subjective and cultural topic. What we mean by and the boundaries of privacy vary greatly among cultures. A lot of what we think of as privacy can fall under the security umbrella, and the stuff that does is rarely if ever controversial. However the stuff that doesn't fit there is where controversy begins.

Jeff Schiller

Interpretation: Consensus

- RFC 3552 / BCP 72 on Guidelines for Writing RFC Text on Security Considerations does not really address privacy considerations
- This is as close as it gets:

  “In general, the goal of a passive attack is to obtain information which the sender and receiver would prefer to remain private. This private information may include credentials useful in the electronic world and/or passwords or credentials useful in the outside world, such as confidential business information.”

Supportive IETF Culture Evolved

- Security Tutorial on Sunday of IETF meeting has raised awareness
- Security Directorate (SecDir) does review during IETF Last Call of every document
- Includes RFC 3552-related review
- Security Advisers assigned to WG when SEC ADs are aware of a need
- Only successful very early in WG life cycle