# Thoughts from the IAB Privacy Program

IETF 81

July 25, 2011

# IETF protocols can have privacy implications . . .

- Most protocols allow or require information about Internet **endpoints** to be shared (e.g., IP)
  - Endpoints or endpoint identifiers can be correlated with the people who use them
- Some protocols allow for **sharing of information** specifically about people (e.g., XMPP)
- Some protocols allow for direct **communication** between people (e.g., SIP)

# . . . but whether they do depends on implementation, deployment, and use

- **Endpoints** are not always proxies for people
- **Communication** is not always between people; protecting it is not always desirable
- **Shared information** is not always about people; protecting it is not always desirable

# In the face of uncertainty, we build threat models

A THREAT MODEL describes the capabilities that an attacker is assumed to be able to deploy against a resource.

"Guidelines for Writing Text on Security Considerations"

(BCP 72/RFC 3552)

# Towards systematic privacy threat modeling

- Early privacy threat modeling was piecemeal (see EAP and IPv6 entries at http://www.iab.org/activities/programs/privacy-program/privacy-reviews/)
  - Circumstance/happenstance triggers mitigation
  - Can yield counterintuitive results
- Efforts have evolved to at least try to identify which threats can be addressed (or not) (e.g., SIP privacy in RFC 3323, 3325)

**Q1: How to build systematic privacy threat models?**

# Scoping

More from BCP 72:

> The purpose of a threat model is twofold. First, we wish to identify the threats we are concerned with. Second, we wish to rule some threats explicitly out of scope.

Plenary has shown a few of the challenges in scoping privacy threats:

- Diversity of user privacy preferences/interests
- Existing incentive structures may not support privacy features desired by certain users/communities
- Norms or laws may drive direction of emphasis

# Scoping

**Q2: How to determine the boundaries of which threats must/should/may be addressed in protocol design?**

**Q3: How to document threats that are not or cannot be addressed?**

# Join the discussion

- Draft: draft-morris-privacy-considerations-03
- Mailing list: ietf-privacy@ietf.org

Q1: How to build systematic privacy threat models?
Q2: How to determine the boundaries of which threats must/should/can be addressed in protocol design?
Q3: How to document threats that are not or cannot be addressed?

# Q & A