IETF & Privacy

(we need your advice!)

Jon Peterson
MIT– December 2010

The IETF builds protocols

- Protocols assume architectures
  - Ideally, these protocols should be useful in a variety of architectures.
  - However, certain protocols are not useful in some.
- We don’t mandate implementation style and deployment characteristics, but we constrain them in various ways.
  - Example: DNS was designed to have a single root.
- Ostensibly, the network intermediaries makes simple forwarding decisions, doesn’t inspect or log packets in any deeper semantics
  - Today, we have plenty of reason to fear otherwise

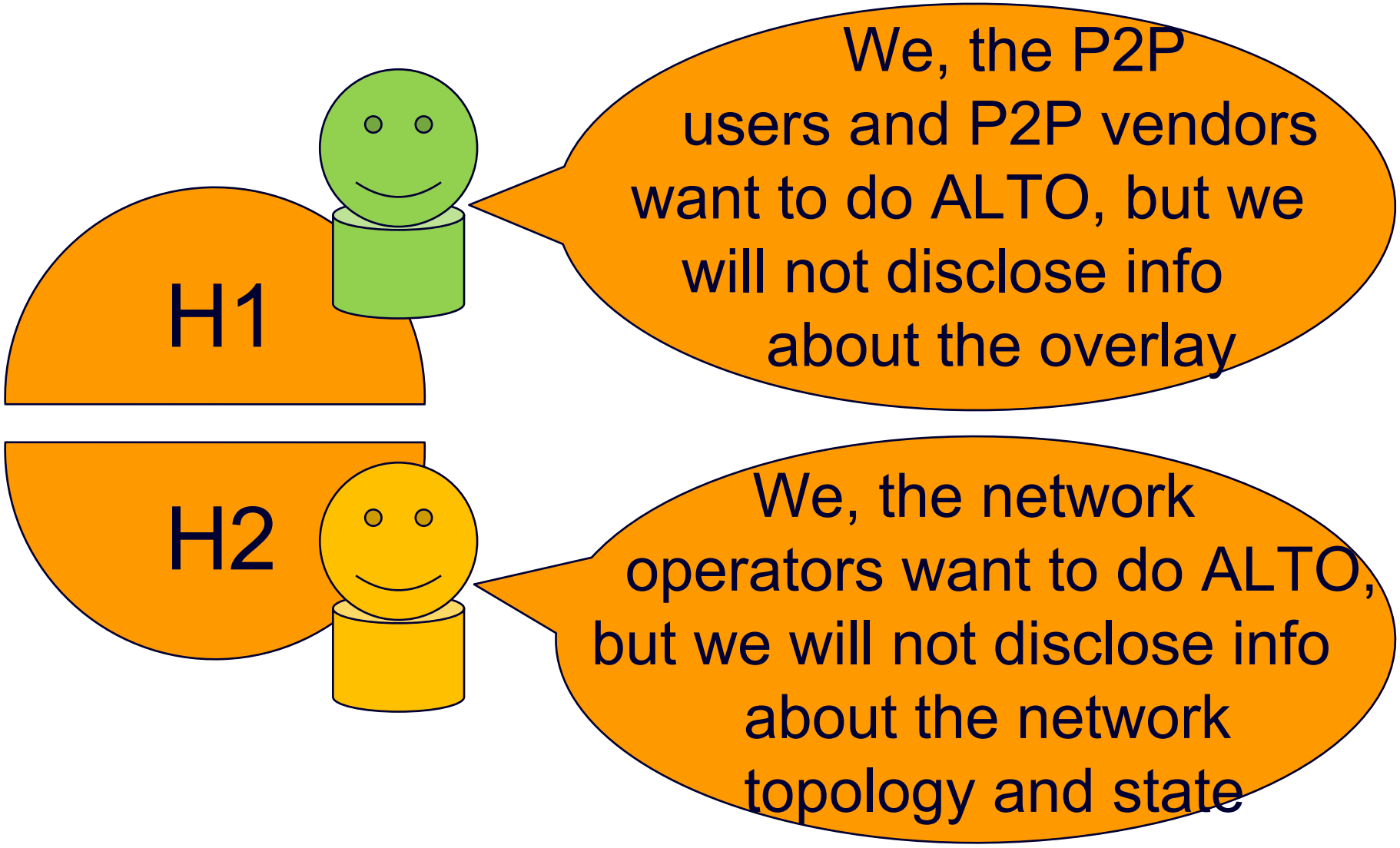
Architecting for privacy

- What does an application need to share to get a service delivered, and with whom?
  - Intermediation
    - SIP, for example, uses intermediaries to route requests
      - However, intermediaries inspect many other elements of requests
    - How can SIP share with intermediaries only the information they need to do their job? (RFC 3323 is a start)
      - How do we get other protocol designs to learn from this experience?
  - ALTO (ongoing right now)
    - How can the user share enough with the network for it to be useful and vice-versa?

IPv6 Privacy Addresses

- In IPv6 stateless addressing, the Interface identifier was constructed based on the MAC address.
  - This raised privacy concerns.
  - RFC 4941 supported a dynamically generated IPv6 Interface identifier.
- Questions:
  - Threat model: Who are we attempting to hide the address from? ISP, eavesdropper (where?), other communication partner, government (police, fire, medical)?
  - The same mechanisms that allow ISPs to track users are used to provide location for emergency services and to deal with certain security attacks (botnets).

“Hemispheres” in ALTO



How to bring them together?

Customizing data per recipient

- Classic “presence” problem
  - I might want to share different presence information with my friend than with my boss (RFC 2778)
  - Had we defined “presence” as a unique rather than a potentially manifold property, however, would this be possible?
    - Some presence architectures admit of only one view of presence, which is either shared with a particular recipient or not
  - We layer our basic architecture for geolocation privacy on top of this (RFC 4119)
- However, just because you choose to share information selectively, what about those you shared it with?
  - Policy framework in geopriv for expressing usage preferences about retention, redistribution, and so on

What we need

- Guidance to authors of protocol specifications on at least four fronts:
  - How do we build privacy threat models?
  - How do we design protocols that do not fall into obvious privacy traps?
  - What are some common ways around traps that you can't get out of?
  - How do we document traps that we don't how how to get out of?

- draft-morris-privacy-considerations