Tradeoffs between Anonymity and Identifiability

Bob Hinden

IETF 63 Paris

3 August 2005

The Problem

- It's good to protect disclosure of the user identify and location
- It's bad to protect identity and location of hackers, BOTs, broken machines, etc.

Environment Matters

- Enterprise Network
  - Most enterprises don't want their employees to be anonymous
  - They require knowledge of identity and location
- Public Wireless Network
  - Protect disclosure of users identity and location from other users important
- Subscribed Network
  - Certain amount of identity disclosure is required to get service
  - Problem here is disclosure of saved secrets

Questions

- Can we protect the good user and at the same time detect the hacker or terrorist?
- Will making anonymity easier have the side effect of making it harder to stop SPAM and DoS attacks?
  - Current anti-SPAM work appears to be going in the opposite direction
- Can our Identity and Location be protected and still make it possible to identify malicious users and broken machines?
- Will this work make Network management much harder or impossible?
- What is the impact on Infrastructure services?
  - Routing, DNS, Firewalls, etc.

How Critical is this problem?

- Do the benefits outweigh the costs?
  - For example, IPv6 Privacy Addresses obscure identity of single node on Link, but Prefix still allows location and traffic analysis
- Are the more serious identity disclosure problems related to disclosure of saved secrets?
  - Not wiretapping

Conclusions

- The issues raised here need to be addressed
- Finding the right tradeoffs may be very hard
  - There are many constraints and variables