BTNS Problem and Applicability Statement

Joe Touch

David Black

Yu-Shun Wang

Document Status

- Versions:
  - draft-ietf-btns-prob-and-applic-00.txt
    - July 1, 2005
  - draft-ietf-btns-prob-and-applic-01.txt
    - Sept. 23, 2005
- Feedback from only a few parties
  - Broader feedback solicited

Feedback Status

- 00->01
  - Most comments incorporated
  - Some not fully addressed
    - We *DID* try to address all comments
    - Some were not sufficient – working on revisions
- 01->(02 – TBA)
  - Revisit open issues from 00-01
  - New issues

A Note on Feedback

- Not all changes added ‘as suggested’
  - Some suggest broader revision is needed
  - *ALL* were addressed in some way
- Is feedback on feedback desired?
  - Can/will send (based on what was received)
    - Point-by-point
    - Summarized replies
  - List where feedback may need public input

Pending Clarifications

- Channel bindings
- VoIP in examples
- Limits of manual keying (RFC 3723/4107)
  - Re: “IPsec doesn’t require IKE”
- Clarify IPsec services
  - Access control
- SSL/TLS should address common case
  - Client has no certificate
- OE
  - Re: “discovery, not key lookup”
- BGP motivation
  - (next 2 slides)
- Clearer text on three variants
  - Unauth, Channel-bound, leap-of-faith (?)

BGP Motivation

- BGP requirements are varied
  - Reducing configuration
  - CPU load / need for hardware
  - Performance
- Not all requirements addressed here
  - BTNS is *inspired* by BGP security issue
  - BTNS may be *part* of a BGP solution
  - BTNS is useful in other scenarios

About CPU Load/Perf

- Recall it was part of the proposed work
  - And nixed ☹
- It may be part of other efforts
  - E.g., Triage (www.postel.org/triage)
  - ID in time for BOF at Dallas
- Provably strong security is expensive
  - Fast security may be desired as an alternative