Information Sciences Institute

btns-prob-and-applic-02

Joe Touch

David Black

Yu-Shun Wang

USC Viterbi
School of Engineering

Current Status

- 02 update 2/17/06
  - Resolve 01 issues (posted 12/05, updated 2/06)
  - Address detailed feedback from individuals
    - Public feedback addressed on mailing list 2/06
- Summary of Changes
  - Document reorganization
  - Issues addressed
  - Pending issues
- Next Steps

Revision Summary

- Sec 1 (intro)
  - Removed redundant CB, TCP spoofing
- Sec 2 (PS)
  - Added net layer motivation (IP layer, IPsec)
- Sec 3 (overview)
  - Add high-level requirements; security services provided
- Sec 4 (AS)
  - Remove modes -> move to end Sec 3
- Sec 5 (Sec. Consid.)
  - Move threat model here from PS; reorganize

Issues Done 1-6 (of 15)

NOT LISTED = clarify text as suggested

- #3 Sec 2 - explain why application credentials cannot be used in IPsec
  - different format, no API for injecting credentials
- #5 Sec 3.1.2 - explain why IPsec is needed with SSL/TLS
  - (e.g., to avoid transport level attacks)
- #6 Sec 3.1.4 - channel binding should not expose passwords
  - (see Nico's ID); clarify further.

Issues Done 7-15

- #7 Sec 3.2 - BTNS not undermine IPsec access control
  - (address earlier and in security considerations)
- #10 clarify S-CBB self-signed SSL example
  - (host in URL matches host in certificate)
- #11 clarify HTTPS and channel binding example
- #13 Sec 5.3 (now 4.2 in v01)
  - use ssh rather than SSL as leap of faith
- #15 update OE description
  - From mailing list text

Issues Not Addressed

Information Sciences Institute

#8 AS for SAB and CBB

- Current on/off-list feedback conflicts
- Request additional feedback based on current document structure

#9 IKE vs CBB Strength

- # vulnerabilities
- level of protection provided

Information Sciences Institute

#12 Sec 5 replication

- is there a better way to handle this?

#14 Leap of Faith

- discuss this on the list further (from last IETF)

Next Steps

- Seeking another round of feedback…
  - Hopefully the last before last call ;-)