Better Than Nothing Security (BTNS)

IETF-62, Minneapolis

March 2005

SIGN THE BLUE SHEETS

(When they show up)

Administrivia

- Scribe
- Jabber scribe
- Blue sheets
- Audio (mp3)

- Mailing list info at:
  http://www.postel.org/anonsec/

Agenda

- Goal of (second) BOF: determine if there is sufficient interest in this work. Scope work to match the interest of those willing to do it.

- Agenda bashing (5 min.)
- Review of BTNS Goals (15 min.)
- Charter bashing (20 min.)
- Milestones bashing (20 min.)

Work items

a) develop a framework document to describe the motivation and goals of these infrastructure-free variants of security protocols in general, and IPsec and IKE in specific

b) develop an applicability statement, characterizing a reasonable set of threat models with relaxed assumptions suitable for infrastructure-free use, and describing the limits and conditions of appropriate use of infrastructure-free variants

c) develop standards-track IKE extensions and/or profiles that support one or both of the bare RSA keys or self-signed certificates

d) Specify standards-track extensions to the SPD and PAD to support anonymous keying for IPsec and cryptographic channel bindings for IPsec

e) Develop an informational document giving advice to IPsec implementers and higher-level protocol designers on the use of IPsec in securing higher-level protocols

Milestones

First drafts for all in 2 months? Finer-grained milestones?

a) framework document

To IESG: 5 months?

b) applicability statement

To IESG: ???

c) IKE extensions (bare RSA keys and/or self-signed certificates)

To IESG: 6 months?

d) extensions to the SPD and PAD to support anonymous keying for IPsec and cryptographic channel bindings for IPsec

To IESG: 9 months?

e) informational document on the use of IPsec in securing higher-level protocols

To IESG: 6-8 months?

Closing

- Sign the blue sheets
- Mailing list info at http://www.postel.org/anonsec/