Better Than Nothing Sec BTNS

IETF 65, July 11, 2006

Chair: Love Hörnquist Åstrand

mailing list: anonsec@postel.org
jabber: btns@jabber.ietf.org
audio feed: http://videolab.uoregon.edu/events/ietf/

Pekka Nikander

- Pekka have resigned as WG-chair

- Love handle the WG for the next 6 months

- Sam will accept proposals for co-chairs

Thank you Pekka

Agenda

- Document status (5 min) - Chair

- Goals review (5 min) - Chair

- Problem and applic statement (15 min) - Joe Touch

- Use of IPsec (30min) - Sam Hartman

- Unauthenticated mode of IPsec (15 min) - Nico & Michael

- BTNS vs global PKI (15 min) - Nico and Michael

- Open issues (25 min)

    - API (scope and interaction w/ other workinggroups) - WG

    - Other issues - WG

- Next steps and wrap up (10 min) - Chair

Document status

- draft-ietf-btns-prob-and-applic

- draft-ietf-btns-core

- draft-ietf-btns-connection-latching

- draft-ietf-btns-ipsec-apireq

WG background and goals

- Three different groups of people

  - Protection transports (against off-path attackers)

  - Working towards channel bindings

  - SSH-like leap-of-faith use of IPsec

- WG chartered to

  - specify extensions to IPsec to support unauthenticated SAs

  - enable / encourage simpler and more rapid deployment of IPsec

Goals for this meeting

- Finish last items on PS/AS to make a fast re-spin and submit to IESG

- Discussion on core document

  - What is missing

  - What needs to be clarified

- Update milestones

Problem and applicability statement

Joe Touch
draft-ietf-btns-prob-and-applic-03.txt

Use of IPsec

Sam Hartman

Unauthenticated mode of IPsec

Nico Williams
Michael Richardson
draft-ietf-btns-core-01.txt

BTNS vs global PKI

Nico Williams
Michael Richardson

Technical discussion

- API
  - scope
  - interaction with other WGs

Technical discussion

- Any other issues ?

Next steps

- Re-spin PS/AS document, take to WG-LC

- More work on the core document

Milestones

May 06	May 06	WG LC on problem and applicability statement (a+b)
May 06	May 06	First version of IPsec interfaces draft (e)
May 06	May 06	Submit problem and applicability statement to IESG (a+b)
Aug 06	Aug 06	WG LC on IKE extensions (c)
Aug 06	Aug 06	WG LC on SPD and/or PAD extensions (d)
Sep 06	Sep 06	Submit IKE extensions to the IESG
Sep 06	Sep 06	Submit SPD and/or PAD extensions to the IESG
Nov 06	Nov06	WG LC on IPsec interfaces draft
Nov 06	Nov06	Submit IPsec interfaces draft to the IESG
Mar 06	Mar 07	Recharter or close the WG

Blue sheets ?