Better Than Nothing Sec
BTNS

IETF 64, Nov 10, 2005

Chairs: Love Hörnquist Åstrand and Pekka Nikander

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

PLEASE MAKE SURE YOUR WLAN IS NOT IN AD HOC MODE!

Agenda

- Document status
- Goals
- Technical discussion
    - Problem statement
    - IKE extensions
    - Open issues
    - Open mike

WG background and goals

- Three different groups of people
  - Protection against off-path attackers
  - Working towards channel bindings
  - SSH-like leap-of-faith use of IPsec
- WG chartered to
  - specify extensions to IPsec so that IPsec will support creation of unauthenticated SAs
  - enable and encourage simpler and more rapid deployment of IPsec

Meeting goals

- Complete discussion on Problem statement and applicability statement
- Confirm direction of the SPD/PAD/IKE extensions document
- Other technical discussions
- Update milestones

Problem and applicability statement

Joe Touch

draft-ietf-btns-prob-and-applic-01.txt

An Unauthenticated Mode of IPsec

Nico Williams
draft-williams-btns-00.txt

Open issues w.r.t. the problem and applicability statement

- Auto-detection
  - Just do IKE
  - DNS
- Whether upgrading to BTNS later is ok?
- Clarify applicability statement

Issues on the table

- Do we need IKE extensions or not?
- Exact details of SPD/PAD extensions
- Auto detection of BTNS
- Bare keys vs. self-signed certs
- API issues

Next steps

- Re-spin PS/AS document
- External review of PS/AS document
- Adopt Nico’s draft as a WG item?
- Re-spin Nico’s draft
- First IPsec interfaces draft

Milestones

Sep 05	Sep 05	First version of SPD and/or PAD extensions draft
Oct 05	Jan 06	WG LC on problem and applicability statement (a+b)
Oct 05	Jan 06	First version of IKE extensions draft (if needed)
Nov 05	Feb 06	First version of IPsec interfaces draft (e)
Nov 05	Feb 06	Submit problem and applicability statement to IESG (a+b)
Jan 06	Mar 06	WG LC on IKE extensions (c)
Jan 06	Mar 06	WG LC on SPD and/or PAD extensions (d)
Feb 06	Apr 06	Submit IKE extensions to the IESG
Feb 06	Apr 06	Submit SPD and/or PAD extensions to the IESG
Mar 06	Jun 06	WG LC on IPsec interfaces draft
Mar 06	Jun 06	Submit IPsec interfaces draft to the IESG
May 06	Jun 06	Recharter or close the WG

Blue sheets ?