Better Than Nothing Sec btns

IETF 63, Thu, Apr 4, 2005

Chairs: Love Hörnquist Åstrand and Pekka Nikander

mailing list: anonsec@postel.org
jabber: anonsec@ietf.xmpp.org

Agenda
(for bashing)

• Document Status	5 min	Chairs
• Goals	10 min	Chairs
• Technical Discussions		
◦ Problem & Applicability	15 min	Joe Touch
◦ IKE extensions	10 min	Nico Williams
◦ Open mike	10 min?	
• Next steps	5 min	Chairs

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

- Get WG feeling about the Problem and Applicability statement
- Initiate work on SPD/PAD/IKE extensions
- Update milestones into more realistic ones
- Other technical discussion, if time permits

Problem and applicability statement

Joe Touch

draft-ietf-btns-prob-and-applic-00.txt

Unauthenticated BITS implementation using IKE

Nico Willimas

draft-williams-btns-unauthenticated-bits-00.txt

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

- Whether upgrading to BTNS later is ok?
  - i.e., using cleartext until established
- What kind of phase 2 SAs are allowed?
  - Transport only?
  - Subject to local configuration?
  - Something else?

Other issues on 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

- When the problem and applicability statement could be ready for WG last call?
- First version of SPD/PAD extensions draft
- Update milestones as needed

Next milestones

- Jul 05 WGLC on problem and applicability statement
- Jul 05 First version of SPD and/or PAD extensions draft
- Aug 05 First version of IKE extensions draft (if needed)
- Sep 05 First version of IPsec interfaces draft
- Sep 05 Submit problem and applicability statement to IESG
- Oct 05 WG LC on IKE extensions
- Oct 05 WG LC on SPD and/or PAD extensions
- Nov 05 Submit IKE extensions to the IESG
- Nov 05 Submit SPD and/or PAD extensions to the IESG

Blue sheets ?