Better Than Nothing Sec
BTNS

IETF 65, March 20, 2006
Chairs: Love Hörnquist Åstrand and Pekka Nikander
mailing list: anonsec@postel.org
jabber: btns@rooms.jabber.ietf.org
audio feed: http://videolab.uoregon.edu/events/ietf/

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

• Document status (5 min)
• Goals review (5 min)
• Technical discussion
  • Problem statement (20 min)
  • Unauthenticated mode of IPsec (40 min)
    • including Connection latching
• Open issues (30 min)
• Next steps (10 min)
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

• Complete discussion on Problem statement and applicability statement
• Discussion on Nico’s proposal for a core document
• Update milestones
Problem and applicability statement

Joe Touch
draft-ietf-btns-prob-and-applic-02.txt
Unauthenticated mode of IPsec

IPsec Channels: Connection Latching

Nico Williams

draft-ietf-btns-core-00.txt
draft-ietf-btns-connection-latching-00.txt
Old but still open issues w.r.t. core document

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

Other issues on the table

• API document
• Volunteers?
• Opinions on basic approach(es)?
  • New API? Socket options? Use of Cryptographically Generated Address?
• One approach or multiple alternatives?
Next steps

• Re-spin PS/AS document, take to WG-LC
• Address comments on Nico’s drafts
• First IPsec interfaces draft
## Milestones

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sep 05</td>
<td>Done</td>
<td>First version of SPD and/or PAD extensions draft</td>
</tr>
<tr>
<td>Jan 06</td>
<td>May 06</td>
<td>WG LC on problem and applicability statement (a+b)</td>
</tr>
<tr>
<td>Jan 06</td>
<td>Done</td>
<td>First version of IKE extensions draft (if needed)</td>
</tr>
<tr>
<td>Feb 06</td>
<td>May 06</td>
<td>First version of IPsec interfaces draft (e)</td>
</tr>
<tr>
<td>Feb 06</td>
<td>May 06</td>
<td>Submit problem and applicability statement to IESG (a+b)</td>
</tr>
<tr>
<td>Mar 06</td>
<td>Aug 06</td>
<td>WG LC on IKE extensions (c)</td>
</tr>
<tr>
<td>Mar 06</td>
<td>Aug 06</td>
<td>WG LC on SPD and/or PAD extensions (d)</td>
</tr>
<tr>
<td>Apr 06</td>
<td>Sep 06</td>
<td>Submit IKE extensions to the IESG</td>
</tr>
<tr>
<td>Apr 06</td>
<td>Sep 06</td>
<td>Submit SPD and/or PAD extensions to the IESG</td>
</tr>
<tr>
<td>Jun 06</td>
<td>Nov 06</td>
<td>WG LC on IPsec interfaces draft</td>
</tr>
<tr>
<td>Jun 06</td>
<td>Nov 06</td>
<td>Submit IPsec interfaces draft to the IESG</td>
</tr>
<tr>
<td>Jun 06</td>
<td>Mar 06</td>
<td>Recharter or close the WG</td>
</tr>
</tbody>
</table>
Blue sheets?