btns-prob-and-applic-03

Joe Touch, USC/ISI

David Black, EMC

Yu-Shun Wang, USC/ISI

Outline

- Changes & Issues Addressed
  - In Section order
- Non-Issues (No Actions)
- Remaining Issues
- Status

IPsec/IKE Overhead

- [Pekka Savola] BTNS brings extra overhead, not suitable in some scenarios.
- Summary:
  - Note the extra overhead in Section 4 before 4.1
  - BTNS-IPsec will have the same overhead as IPsec/IKE, thus unsuitable in situations where IPsec/IKE are unsuitable.

Security Considerations

- Section 5 - Rewritten & Reorganized
  - Streamline duplicate items
  - Added/Expanded sub-sections to address each security issue
  - Addressed old issue #12

CB-BTNS & Passwords

- [Pekka Savola/Nico] CB-BTNS could expose password-related materials to MITM, even if detected
- Summary:
  - Text: Section 5.3
  - Depends on the upper layer authentication. If the upper layer auth expose sensitive info, then the attacker can get something useful even though it will be detected (because the auth will fail).
  - Must not use ULP auth that may expose sensitive info

ICMP Protections

- [Pekka Savola] ICMP Protection with BTNS
- Summary
  - New text: Section 5.6 ICMP Attacks
  - BTNS-IPsec does not change the existing IPsec guideline on how to handle incoming ICMP packets.

Leap of Faith

- [Old Issue #14] Leap of Faith
- Summary
  - New text: Section 5.7 “Leap of Faith and Cached Credentials”
  - BTNS vs. SSH/SSL (next slide)
    - Similar motivations & mechanisms
  - Separate two mechanisms:
    - Accept unauthenticated credentials (BTNS, SSH/L)
    - Cache unauth credentials for future refs (SSH/L)

(LoF) BTNS vs. SSH/SSL

	SSH/SSL	BTNS
Accept unauth credentials	Yes	Yes
Options/Warnings to reject unauth credential	Yes	No
Cache unauth credential for future refs	Yes	No/?

Cached Credentials

- SSH/SSL
  - Trust cached credentials as if authenticated
  - “Upgrade” status of unauth credentials
  - (SSL) “Accept permanently”
- BTNS
  - Possible Options
    - SAB - No upgrade, still unauth even cached
    - CBB - Can/May upgrade if CB succeeds
  - ???

NAT Traversal

- [Pekka Savola] Should address NAT Traversal
- Summary
  - New text: Section 6.1 (adapted from Nico's email on 5/8/06)
  - Mostly orthogonal - BTNS focus on (relaxing) peer authentication in IPsec/IKE policy
  - BTNS with Channel Binding may cause problems with NAT if the IDs are tied to addresses at the application layer.
  - NOT specific to BTNS, but to the design of generic IPsec Channel Binding APIs.

Non-Issues / No Actions

- [Old #9] IKE vs. CBB => vulnerability, level of protection
  - Removed mis-leading text (IKE stronger than CB) in Section 3.3 since -01
  - CB & IKE are orthogonal
    - Different layers (transport & above vs. net)
    - Crypto strength of CB depends on upper layer auth protocols

Non-Issues / No Actions

- [Pekka Savola] Benefits + Transition Strategy
  - Benefits focus on BTNS
  - Transition strategy out of scope
- [Pekka Savola] Text re: pki4ipsec
  - No-Op: No better suggestions
- [Pekka Savola] Normative Refs
  - Can change if RFC Editor complains

Remaining Issues

- [1] Remove Asymmetric CBB
  - Currently prefer to leave this in as unresolved but suspect, recommend avoidance
- [2] Separate AS for SAB & CBB
  - (need to recheck)
- [3] Connection Latching
  - To be wrapped based on email discussion