Thinking About BTNS

Nicolas.Williams@sun.com

Basics

- Forget what I have in my -00 individual submission I-D on BTNS...
- Just do IKE with bare public key as CERT and new ID type to assert the bare public key as the ID
  - (or no asserted ID, whatever)
- And add a bit of PAD to allow for rules that say "any BTNS peer can use IP addresses from these ranges"
  - And, if anyone cared, a "this bare public key can use this address

Properties

- No real authentication
- Protects against passive attackers
- Protects against off-path injection attacks
- Active attackers that can take over a victim's IP can negotiate new SAs and go from there
  - But it can't take over existing connections
  - This is only slightly worse than plain IPsec in that at least in plain IPsec one can tie non-mobile devices' IDs to their static IP address; not so easy for BTNS

IPsec APIs: Connection Latching

- Latch all packets sent/received by a transport (e.g., TCP) for a given connection to all SAs with same algs/IDs/etc...
  - Record algs/IDs of SA negotiated and used for the first packet sent or received for a connection
  - Subsequently send or accept only packets protected with similar SAs
- In KAME, Solaris, a socket option
- Adds a more protection against active attackers

IPsec APIs: Connection Latching

- Even UDP datagrams can be latched, though without a UDP “connection” you probably only want to bind each datagram (and its fragments) to a single SA

IPsec APIs: Retrieve IDs/CERTs for Latched Connection

- If apps can latch connections then apps could ask the transports for information about the ends of the connection
  - Latched IDs, CERTs and cert chain used in cert validation for initial connection packet
- Then...

IPsec Channels and Channel Bindings

- Connection latching -> IPsec channels
- Latched IDs -> channel bindings
  - Because IKE sees to it that the SAs authenticate the SA's peers' IDs
    - Even in BTNS case, the peers, having bare keys are “authenticated” by signing with the private keys that correspond to their asserted public keys
  - So the IDs help identify IPsec channels
- Of course, you have to have authentication at a higher layer to use channel bindings to lower layers

IPsec Channels and Channel Bindings

- Much more protection against active attackers
  - As strong as upper layer authentication, against early active attacks
  - As strong as the session crypto in the lower layer, against active (or passive) attacks later in session