EIDs, IPsec, and HostNAT

Steven M. Bellovin

smb@research.att.com

973-360-8656

AT&T Labs Research

Florham Park, NJ 07932

Endpoint Identifiers

- Provide a *name* for a host.
- Distinguish the name from a *locator* – the way you find the host.
- Today, IP addresses fill both roles.
- This has caused problems for mobility, process migration, renumbering, etc. EIDs help resolve many of these issues.

$\Rightarrow$ But – EIDs make packet headers larger.

IPsec

- Set up secure communication path between two hosts.
- Actually, the path is between two certificate holders – users, hosts, or gateways.
- A *security association*, identified by a receiver-assigned number (the SPI), points to the crypographic algorithms, certificate name, IP address, etc.

Security Associations *Are* EIDs

- If you're using IPsec, you already have strong assurance of who your peer is.
- The IP address is irrelevant, except as a locator.
- You don't need an explicit EID in the packet – it is implicit in the security association.
- Conclusion: with IPsec, we have EIDs, as long as implementations aren't too picky about the IP addresses on incoming packets.

Implications for NAT

- If IP addresses don’t matter, we can change them on the fly.
- We still have issues with the TCP pseudo-header – but see Huitema’s draft.
- And there’s always the embedded address problem.

HostNAT

- Must NAT take place at the border?
- The host knows about its protocols, embedded addresses, etc.
- Use TCP renumbering, encapsulation, IPsec, etc., to let the changes to the outside address be done at the endpoint. Perhaps we have a virtual interface, with a dynamic outside address.
- IPsec EIDs handle circuit association; locators (for use by the NAT gateway) are the remaining issue.

References

EIDs

http://users.exis.net/~jnc/tech/endpoints.txt
(Noel Chiappa)

TCP Address Change

http://www.chem.ucla.edu/~beichuan/etcp/
(Christian Huitema)