Security and IPv6

Steven M. Bellovin
smb@research.att.com
http://www.research.att.com/~smb

Areas of Improvement

- IPsec
- No NATs
- Address privacy
- Availability

IPsec

- Protects all upper-layer protocols.
- Requires no modifications to applications.
  - But smart applications can take advantage of it.
- Useful for host-to-host, host to gateway, and gateway-to-gateway.
  - Latter two used to build VPNs.

Doesn't IPsec work with IPv4?

- Yes, but…

- It isn't standard with v4.
- Few implementations support host-to-host mode.
  - Even fewer applications can take advantage of it.

No NATs

- NATs break IPsec, especially in host-to-host mode.
- With no NATs needed, fewer obstacles to use of IPsec.
- Note carefully: NATs provide no more security than an application-level firewall.

Address Switching

- Hosts can pick new addresses frequently.
  - Prevents tracking of usage.
- Using separate IP address per process group can simplify firewalls.

Availability

- Multiple addresses per host help with multihoming.
- Autorenumbering permits switching providers without downtime.
- Autoconfiguration helps prevent mistakes.

Conclusions

- IPv6 gives a noticeable -- though not dramatic -- improvement in security.
- Much of the improvement comes from standard, usable, IPsec.
- The very large address space may provide for other, innovative security mechanisms.