Further Work on IP-layer Security
A Personal Opinion

Steven M. Bellovin

`smb@research.att.com`

973-360-8656

AT&T Labs Research

Florham Park, NJ 07932

Remaining Work Items

- Critical path — must have for **ipsec** to progress and be deployed.
- Useful — will make **ipsec** nicer or better.
- Hard — large amount of work, or very unclear how to implement.

Critical Path

- Architecture — *Mostly done*
- ESP and AH — *Mostly done*
- Base transforms — *Mostly done*
- MIB — must have per IESG requirements — *Under way*
- IANA registration guidelines for ISAKMP DOI — ???

Useful

- ICMP messages (TTL exceeded, port/host unreachable, admin denied, ipsec-specific).
- PMTU (Path MTU) for tunnels
- Other key exchange protocols
- Other encryption algorithms
- Simple and advanced crypto API
- Crypto gateway discovery — KX records? ICMP messages? Something else?
- Dynamic discovery of complex **ipsec** topologies.

Hard — Multicast

- What type of multicast? Private conference? HBO-style broadcast? Broadcast with **ipsec**-mediated uplink?
- Key management protocol
- Group access control

My Suggestions

- Critical path items remain in **ipsec** group.
- New group (**ipsecond**?) for useful items.
- Separate group for multicast security.