

# IEEE Key Management Summit 2008

## IETF Key Management Standards

Russ Housley

IETF Chair

Founder of Vigil Security, LLC

# IETF Key Management Protocols

## Completed:

- IKE and IKEv2
- CMS
- TLS
- EAP-TLS, EAP-TTLS, ...

## Under development:

- KeyProv
- Key Management for TCP-AO

## Key Management for TCP Authentication Option (TCP-AO)

- TCP-AO is a replacement for TCP-MD5
- Meet needs of TCP-AO, and a bit more
- Manage tables of keys for the peers
- Table includes key identifiers, algorithm, protocol, usage period, and the key derivation key (KDK)
- Traffic key derived from protocol information and the KDK in the table