Lecture 27 (IKE)

1 IKE

Authentication can happen using a Pre-Shared Key (PSK) or using PKI

1.1 PSK

Both sides start with secret and then run IKE to authenticate each other and generate IPsec SAs

1.2 PKI

1. Both sides start with public/private key pair and certificate
2. Run IKE to authenticate each other and obtain IPsec SAs
3. Similar to handshake in SSL