IPSec (IP Security) authentications

IPSec: Mechanisms

- Security Associations (SA, RFC 4301)
  - Security policies, mechanisms and crypto parameters used to secure the communication between a pair of hosts
  - Security Parameter Index (SPI)
    - SA identifier
    - Indexes the SA that should be used to validate an IPSec datagram
- Extra optional fields for the IP header
  - Authentication Header (AH, RFC 4302)
    - Has an SPI
    - Keyed hash (MAC) of the whole IP datagram
  - Encapsulating Security Payload (ESP, RFC 4303)
    - Has an SPI
    - Authenticated cryptogram of the IP datagram payload

IPSec: SAD and SPD

- Security Association Database (SAD)
  - Repository of local SAs
  - An SA is mainly a bilateral peer agreement
    - A set of common rules to protect ID datagramas
    - But it only protects traffic in one direction!
- Security Policy Database (SPD)
  - Repository of local IPSec protection policies
  - A policy states a required IPSec protection
    - E.g. traffic with characteristics X and Y should be protected with mecanisms A and B

IPSec: Setup of SAs

- Manual
  - With console or graphical tools
  - With libraries
- Automatic with protocol
  - IKE v2 (Internet Key Exchange)

ISAKMP (Internet Security Association and Key Management Protocol, RFC 2408)

- Generic metaprotocol (or framework)
  - App-level protocol
- Allows key negotiations and peer authentications
  - Was created to handle SA negociations
    - For IPSec / IKEv1, but not exclusively
    - IKEv1 was just a Domain of Interpretation (DOI) of ISAKMP
- Initially independent of IPSec
  - Actually is totally intertwined with IKEv2

IKEv2 (Internet Key Exchange)

- Two-phase protocol
  - Setup of bilateral, host-to-host IKE SAs
  - Setup of IPsec SAs
    - aka child SAs
- The first phase is less frequent
- The second phases are more frequent
  - We may have numerous IPSec SAs between two hosts
  - These are unilateral

IKEv2 protocol phases: Initial exchanges

- SA_INIT request / response
  - Negotiate cryptographic algorithms
  - Exchange nonces
  - Diffie-Hellman key agreement
- SA_AUTH request / response
  - Authenticate the previous messages
  - Exchange identities and certificates
    - These are hidden from eavesdroppers
- At the end we have an IKE SA between two hosts
  - This SA is then used to protect the installation of IPSec SAs

IKEv2 protocol phases: Creation of child SAs

- CREATE_CHILD_SA request / response
  - To create a new IPSec SA
  - To rekey IKE SAs or IPSec Sas
- SA is rekeyed by creating a new SA
  - And then deleting the old one

IKEv2: Peer authentication

- Digital signatures and X.509 certificates
  - Distributed inline
- Pre-distributed public keys
- Pre-shared secret key