Wie Interoperabel ist IPsec? Ein Erfahrungsbericht

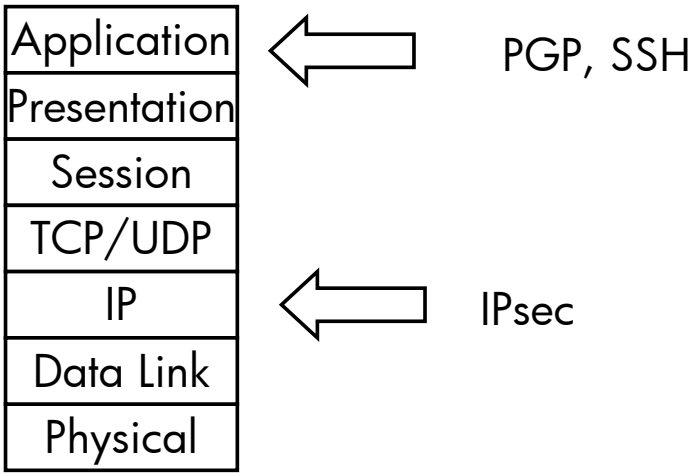
Arturo Lopez
Senior Consultant

März 2003

Agenda

- Security Associations
- Schlüsseltausch
  - IKE Internet Key Exchange
    - Automatischer Schlüsseltausch und Identitätsnachweis
  - Diffie-Hellman
    - Verfahren zum initialen Schlüsseltausch
  - ISAKMP (Internet Security Association and Management Protocol)
    - Festlegung der Security Association Parameter
- Sicherheitsprotokolle
  - ESP Encapsulating Security Payload
  - AH Authentication Header

- Internet Protokoll Security (IPsec) implementiert Sicherheit auf Layer 3 in OSI Modell



Ipsec Komponenten

- Security Associations
- Schlüsseltausch
  - Diffie-Hellman
    - Verfahren zum initialen Schlüsseltausch
  - IKE Internet Key Exchange
    - Automatischer Schlüsseltausch und Identitätsnachweis
  - ISAKMP (Internet Security Association and Management Protocol)
    - Festlegung der Security Association Parameter
- Sicherheitsprotokolle
  - ESP Encapsulating Security Payload
  - AH Authentication Header

- SA ist eine unidirektionale Festlegung von Parametern, die eine sichere Kommunikation ermöglichen sollen.
- Für bidirektionale Übertragung muss eine Inbound und eine Outbound Verbindung aufgebaut werden.
- Die sichere Kommunikationsverbindung in ESP, AH, IPComp und ISAKMP werden durch SA beschrieben.
- Protection Suite ist Menge aller möglichen Parameter für eine SA.
  - ESP z. B. DES, 3DES, AES
  - AH z. B. HMAC-MD5
  - ISAKMP z. B. Preshared Secrets oder SHA1

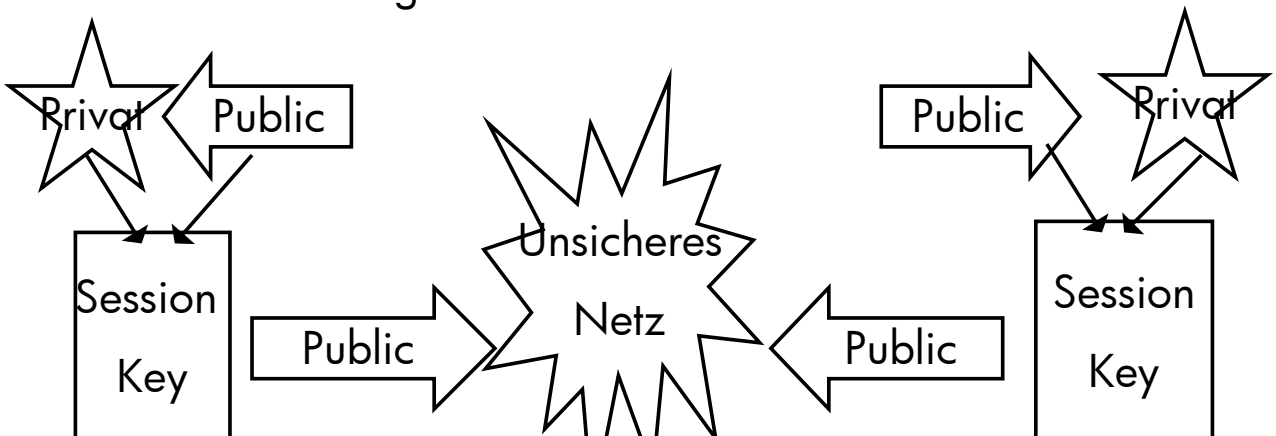
Am Anfang war der Schlüssel

- Authentifizierung des Partners
  - Pre-Shared-Key, der Authentifizierungsschlüssel ist ein Passwort
  - RSA-Keys=Private/Public Keys, der Authentifizierungsschlüssel wird mit Private/Public Key Paar generiert
  - RSA-Signaturen= Private/Public Keys auf digitalen Zertifikaten, der Authentifizierungsschlüssel wird mit digitalen Zertifikaten generiert.

- Security Associations
- Schlüsseltausch
  - Diffie-Hellman
    - Verfahren zum initialen Schlüsseltausch
  - IKE Internet Key Exchange
    - Automatischer Schlüsseltausch und Identitätsnachweis
  - ISAKMP (Internet Security Association and Management Protocol)
    - Festlegung der Security Association Parameter
- Sicherheitsprotokolle
  - ESP Encapsulating Security Payload
  - AH Authentication Header
  - Ipcomp IP Payload Compression Protocoll

Diffie-Hellmann (RFC 2631)

- Mit Diffie-Hellman wird der Sitzungsschlüssel erzeugt
- Basiert auf asymmetrischer Verschlüsselung
- Der Sitzungsschlüssel muss durch Authentifizierung des Partners bestätigt werden



- Algorithmus
  - Shared_Secret entspricht Session Key in IPsec
  - Basiert auf der Berechnung von Primzahlen
  - $A_{pub} = g^{Apriv} \bmod p$
  - $Bpub = g^{Bpriv} \bmod p$

  $Shared\_S = (B_{pub})^{Apriv} \bmod P = (A_{pub})^{Bpriv} \bmod P = g^{Apriv * Bpriv} \bmod P$

Ipsec Komponenten

- Security Associations
- Schlüsseltausch
  - Diffie-Hellman
    - Verfahren zum initialen Schlüsseltausch
  - IKE Internet Key Exchange
    - Automatischer Schlüsseltausch und Identitätsnachweis
  - ISAKMP (Internet Security Association and Management Protocol)
    - Festlegung der Security Association Parameter
- Sicherheitsprotokolle
  - ESP Encapsulating Security Payload
  - AH Authentication Header

- ISAKMP
  - Definiert Prozeduren und Paketformate für den Aufbau und zum Management von Security Associations
  - Es ist nicht spezifisch für IPsec
  - Phase 1: Main Mode oder aggresive Mode Exchange
    - Schutz die ISAKMP Nachrichten durch eine Security Association
  - Phase 2: Quick Mode
    - Schutz die Benutzerdaten durch IPsec
  - Austausch von Verschlüsselungsschlüssel wird in IKE festgelegt

Internet Key Exchange (IKE) RFC 2409

- IKE
  - Authentifizierte Austausch von Verschlüsselungsschlüsseln innerhalb von IPsec
  - OAKLEY and SCHEME sind zwei Methoden für den Aufbau von authentifizierten Verbindungen für den Austausch von Schlüsseln.

- Security Associations
- Schlüsseltausch
  - Diffie-Hellman
    - Verfahren zum initialen Schlüsseltausch
  - IKE Internet Key Exchange
    - Automatischer Schlüsseltausch und Identitätsnachweis
  - ISAKMP (Internet Security Association and Management Protocol)
    - Festlegung der Security Association Parameter
- Sicherheitsprotokolle
  - ESP Encapsulating Security Payload
  - AH Authentication Header

Encapsulating Security Payload (ESP) RFC2406

- Ermöglicht Vertraulichkeit, Authentizität und Integrität der Nutzdaten (Payload)
- Vertraulichkeit durch symmetrische Verschlüsselung der Nutzdaten während der Übertragung z. B. mit DES oder 3DES
- Authentizität und Integrität über den ESP Header

- Ermöglicht Integrität und Authentifizierung des Absenders für ein IP Datagram
- Kann in Kombination zu ESP eingesetzt werden
- AH schützt die IP Header Felder. ESP den Payload.
- Basiert auf Hash Digest or Fingerprints. Eingesetzt werden z. B. MD5 oder SHA-1
- Hash-based Message Authentication Code (HMAC) ist die Authentifizierte Prüfsumme oder Message Digest, der an die Nachricht angehäng wird.

Erfahrungen aus den Tests

- Getestete Plattformen
  - Redhat LINUX FreeSwan
  - Checkpoint NG
  - Symantec Enterprise Firewall
  - Windows 2000
- Meistens Probleme hatten wir beim Aufbau der SA in der Phase 1. Probleme haben wir gelöst, in dem wir mit dem kleinsten gemeinsamen Nenner konfiguriert haben
- Nach anfänglichen Konfigurationsproblemen hatten wir eine gut funktionierende Infrastruktur im Testlabor aufgebaut
- Ipcomp war kein Bestandteil der Tests

- Fazit:
  - Auf den getesteten Plattformen funktionierte IPsec Reibungslos.