IPsec ISAKMP

Internet Security Association and Key Management Protocol (RFC 2408)

Vortrag in der Vorlesung „Sicherheit in Netzen“

Jens Mahnke

ISAKMP - Allgemein

- Meta-Protokoll definiert (RFC 2408):
  - Verfahren
  - Datenstrukturen
  - Protokolle
  - zur Aushandlung der SA mit vier Modi
- Erfordernisse:
  - Starke Authentisierung (digitale Signatur)
  - Authentisierten Mechanismus zum Schlüsseltausch
  - Definition Randbedingung in „Domain of Interpretation“
- Begriffe IKE und ISAKMP heute oft gleich

ISAKMP - Phasen

- Primäre Phase:
  - Aushandlung SA (zw. 2 Instanzen)
  - Einsatz von Cookies (einfacher als Diffie-Hellman)
  - ISAKMP-SA etabliert
- Sekundäre Phase SAs:
  - Nutzung Phase 1 als sicherer Kanal
  - Sicherheitsmechanismen für Nutzdaten
  - Keine asymmetrischen Verfahren (schneller)

$\Rightarrow$ 4 Austauschmechanismen im ISAKMP

ISAKMP Phasen und IPSec

ISAKMP Phase 1: Noch keine SA zur Verschlüsselung

ISAKMP Phase 2: ISAKMP zur Verschlüsselung

IPSec: IPSec-SA zur Verschlüsselung

ISAKMP - Base Exchange (1/4)

- Ablauf:
  - Sender erzeugt Proposal mit Zufallszahl
  - Empfänger sendet unterstützte Verfahren und Zufallszahl zurück
    - Voraussetzung: Schnittmenge (Sender/Empfänger) unterstützter Verfahren
  - Aufbau gemeinsames Geheimnis und Identität
    - Identifikation erst nach aushandeln der Algorithmen
    - Kostspielig: 4 Nachrichten werden gesendet
    - Evtl. mit asymmetrischer Verschlüssellung

ISAKMP - Identity Protection Exchange (2/4)

- Austausch von Schlüsselmaterial
  - Identität der Parteien kann nicht von Dritten mitgelesen werden
- Start analog zu Base Exchange (Proposal)
- 2 weitere Nachrichten:
  - Austausch von Teilschlüsseln und
  - Zufallswerten
- Nochmals 2 weitere Nachrichten:
  - Austausch der Identitäten
  - Authentisierung unter Schutz des zuvor vereinbarten gemeinsamen Geheimnisses

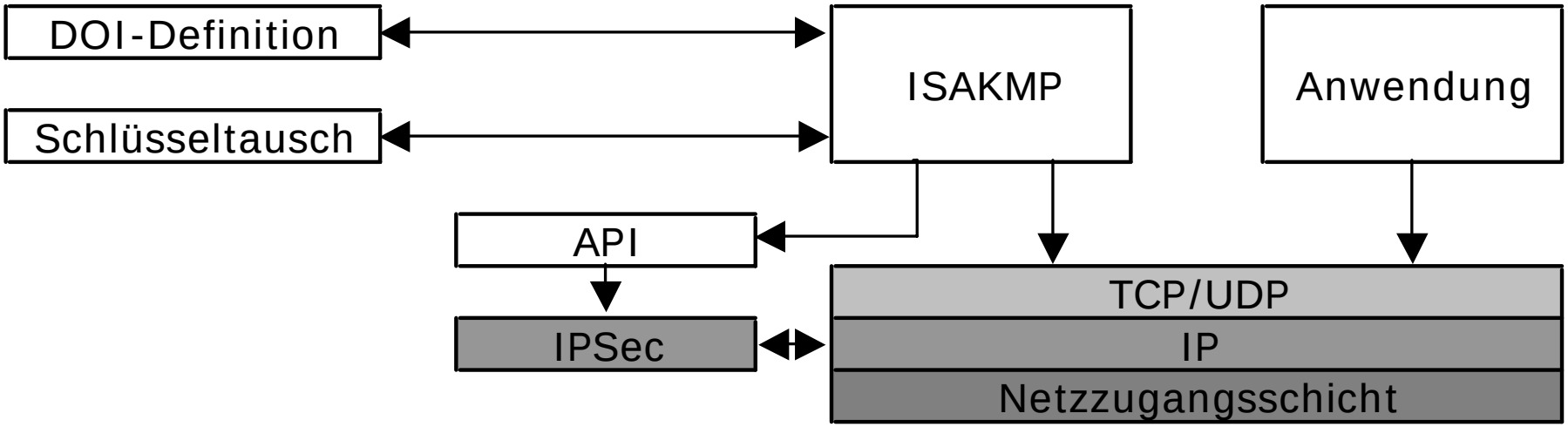
ISAKMP - Authentication Only Exchange (3/4)

- Einsatz wenn kein Schlüsselmaterial ausgehandelt werden muss
- Nur drei Nachrichten werden gesendet:
  - Proposal enthält:
    - Chiffren,
    - Schlüssellängen wie bei Base Exchange,
    - Zufallswert als Schutz vor Wiedereinspielen
  - Empfänger reagiert mit:
    - Proposal-Schnittmenge,
    - Zufallswert
  - In dritter Nachricht sendet Empfänger Identität unter Schutz der Authentisierungsfunktion

ISAKMP - Aggressive Exchange (4/4)

- SA, Key Exchange und Authentication werden zusammen übertragen
- Vorteil: Reduktion auf drei Nachrichten
- Nachteil: Identitäten der Beteiligten als Klartext
- Es wird genau ein Proposal und eine TransformPayload übertragen
  - Sofern Empfänger damit nichts anfangen kann muss auf anderen Austauschmechanismus zurückgefallen werden

ISAKMP - Kommunikationsarchitektur



ISAKMP - Header

Initiator Cookie				
Responder Cookie				
Next Payload	MjVer	MnVer	Exchange Type	Flags
Message ID				
Length				

Payload

MjVer = Major Version (ISAKMP)
MnVer = Minor Version (ISAKMP)
ExchangeType = Nachricht verschlüsselt, authentifiziert oder nicht

Literatur

D. Maughan (National Security Agency), M. Schertler (Securify, Inc.), M. Schneider (National Security Agency), J. Turner (RABA Technologies, Inc.): *Internet Security Association and Key Management Protocol (ISAKMP).* Request for Comments: 2408, Network Working Group, November 1998. http://www.ietf.org/rfc/rfc2408.txt (22.05.2005)

Stephen Wolthusen (FhG): *Netzwerksicherheit - Virtual Private Networks und Network Adress Translation.* Fraunhofer Gesellschaft - Institut Grafische Datenverarbeitung, 2003. http://www.wolthusen.com/books/Netzwerksicherheit/slides/11_VPNNAT.pdf (22.05.2005).

J. Schwenk: *IPSec - Internet Protocol Security*. Lehrstuhl für Netz- und Datensicherheit an der Ruhr-Universität Bochum. Vorlesung Systemsicherheit. http://www.nds.ruhr-uni-bochum.de/lehre/vorlesungen/systemsicherheit/ (22.05.2005).