



••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

Netzwerksicherheit

Virtual Private Networks und Network Address Translation

Dr. Christoph Busch
Dr. Stephen Wolthusen
Fraunhofer-IGD





Vertiefungsmöglichkeiten

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Diese Vorlesung kann nur einen Überblick über Verfahren und Probleme für VPN/NAT geben
- Parallelveranstaltung am Fachbereich:
W. Böhmer: Virtual Private Networks
(jeweils Wintersemester)





Gründe für Network Address Translation

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Zunehmende Verknappung des Adressraumes
 - Zumindestens keine Vergabe zusammenhängender „bequemer“ Adreßbereiche mehr (VLSM...)
- Aus historischen/administrativen Gründen eingeführte Adressen die nicht von Vergabestellen (ARIN, APNIC, RIPE) stammten
- Renumerierung schwierig
 - anwendungsspezifische Bindung an bestimmte Adressen (Server, Lizenzmanagement...)
 - erfordert Protokolle zur dynamischen Vergabe von Adressen und anderen Netzwerkinformationen (z.B. DHCP)





Rückwirkende Legalisierung: RFC 1597 (1994)

... department security technology ... department security technology ... department security technology ... department security technology ...

- Annahme: Nur wenige Hosts müssen mit Internet verbunden werden (SMTP,FTP,NNTP...)
 - Adreßbereiche 10.0.0.0/16, 172.16.0.0/20, 192.168.0.0/16
 - Filterung ausgehender Verbindung, Blockierung seitens ISPs
- Explizite Gegenposition in RFC 1627: Verletzung der IETF-Prinzipien (Sicherstellung von Ende-zu-Ende-Verbindungen...)
- Mit RFC 1918 wurde das Vorgehen dennoch als „Best Current Practice“ etabliert
 - Hauptgrund: Einführung des „Network Address Translators“ durch Tsuchiya und Eng





Grundlegende Annahmen bei NAT

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Zu einem gegebenen Zeitpunkt kommuniziert nur eine kleine Teilmenge der Hosts in einem Netzwerk mit der Außenwelt
 - Ermöglicht die dynamische Abbildung einer großen Anzahl von „internen“ Adressen auf eine geringe Anzahl „externer“ Adressen (von IANA vergeben)
 - Abbildung wird nach Beendigung der Verbindung gelöscht
- Vorschlag von Tsuchiya und Eng sah vor, dies über dynamische Modifikation von DNS vorzunehmen
 - Aufgrund praktischer Überlegungen verworfen





Weitere Annahmen für NAT

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

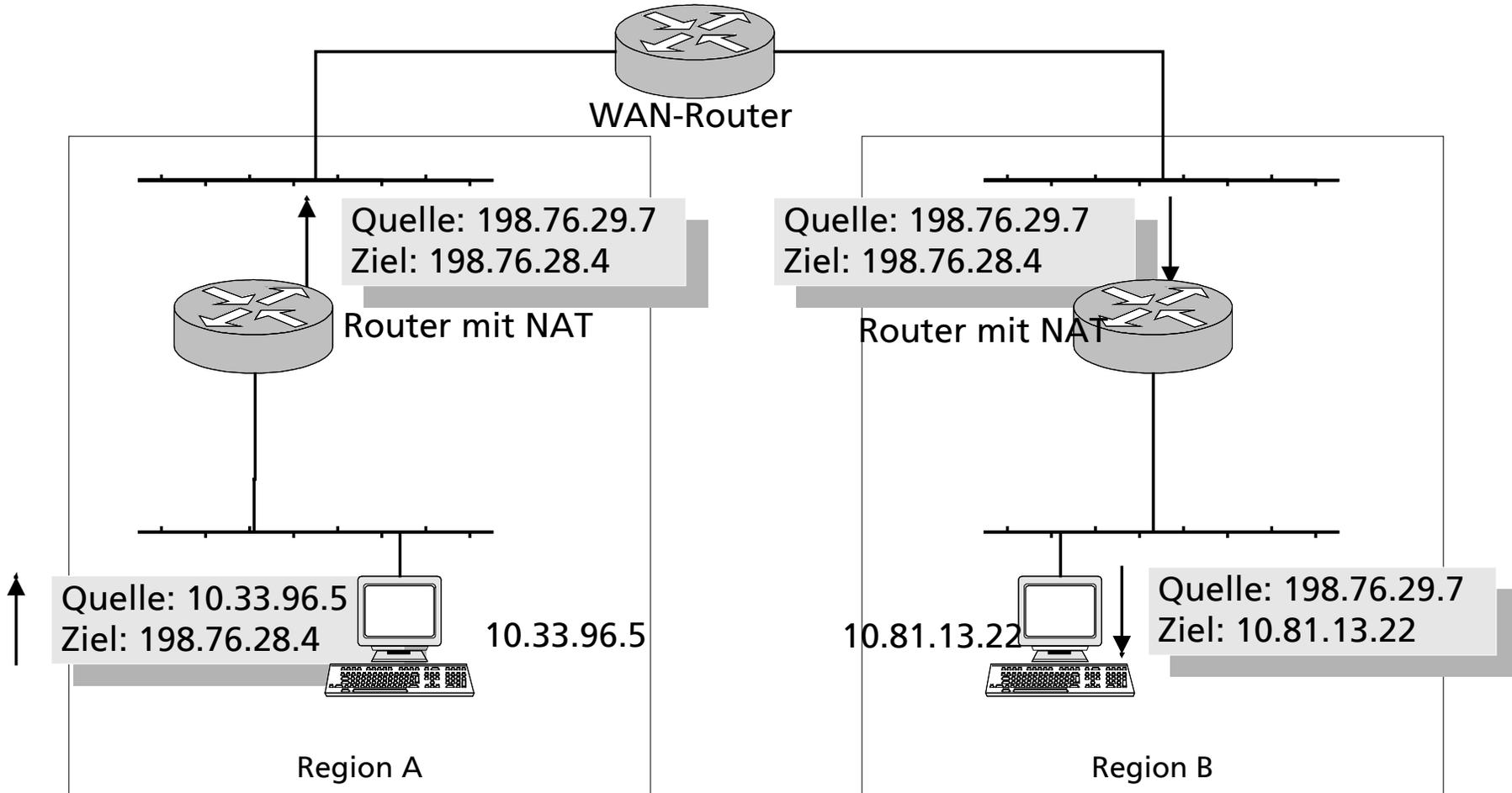
- Private Adressen dürfen ausschließlich in Regionen verwendet werden, deren einziger Übergangspunkt ein mit NAT ausgestatteter Knoten ist
 - Einfache Variante: Nur ausgehende (TCP) Verbindungen werden betrachtet - nur eine Tabelle
 - Problem: eingehende Verbindungen
 - ▲ Müssen nach außen hin semi-statisch/auflösbar sein
 - ▲ Übersetzung muß dann bidirektional erfolgen
 - ▲ Kooperation mit DNS und anderen Namensdiensten
 - ▲ Erfordert parallele Pflege zweier Tabellen





Network Address Translation bei Quell- und Zielnetz

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





Probleme von NAT

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Modifikation der IP-Header bewirkt Änderung von Prüfsummen
 - Partielle Neuberechnung (1er-Komplement-Eigenschaft)
 - Bewirkt Fehler in IPSec AH - Dan Harkin (Coautor IKE):
„**NAT is the kind of attack IPSec was designed to detect**“
 - AH erzwingt Verwerfen von Paketen deren Header modifiziert wurde; implizit ähnliches Problem mit ESP

- Die Verbreitungsgeschwindigkeit von NAT und IPSec war jeweils invers dem Wünschenswerten
 - Einrichtung einer IETF-NAT-Arbeitsgruppe (bis dahin nur herstellerepezifisch ad hoc)





IETF-Bemühungen um NAT

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Versuch einer Vereinheitlichung der Hersteller-Terminologie sowie Definition der Problemstellung (RFC 2663)
- Spezifikation des einfachen NAT in RFC 3022:
Festschreibung bestehender Praktiken, ohne eingehende Verbindungen
 - Definiert kein Verhalten bei Erschöpfung extern erreichbarer Adressen: Implementierungen ignorieren überzählige Verbindungen (auch bei Lizenzüberschreitung)
 - Abbildung soll bis zum Abbau der letzten Verbindung erhalten bleiben, neue Sitzungen erhalten alte Abbildung
 - Problem: Wann ist Verbindung wirklich beendet?





Heuristiken für Feststellung von Verbindungsabbau

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- ICMP-Nachrichten erfordern virtuelle Verbindungen, mehrere Verhaltensmuster sind denkbar
 - Lediglich ein Datagramm als Antwort
 - Unbegrenzte Anzahl von Antworten
 - Es wird nie eine Antwort erhalten
 - NAT muß eigene Heuristik (Fristen etc.) anwenden um Verbindung für beendet zu erklären
 - ▲ diese bewirken neue, nicht vorherzusehende Fehlverhaltensmuster
- NAT müßte eigentlich auch ICMP-Inhalte modifizieren...





UDP und NAT

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Ähnliche Problematik wie bei ICMP: Verbindungsloses Protokoll
- Sitzungsdauer bei UDP prinzipiell unbegrenzt
 - Videokonferenzen etc.
- Intervall zwischen Datagrammen der Sitzung ist beliebig
 - Jede Heuristik wird legitime Verbindungen abbrechen
 - ▲ ALGWs können helfen, sind aber zu kostspielig
- Interaktionen mit Firewalling (DNS-Anfragen) können dafür sorgen, daß Pakete bei längerer Antwortzeit verloren gehen, **exponential backoff** kann beliebig lange Wartezeiten verursachen





TCP und NAT

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Heuristik muß halboffene Verbindungen (nur SYN) berücksichtigen - wann darf eine Adreßabbildung wieder gelöscht werden?
- Verbindungsabbau erfolgt nicht immer über FIN-Handshake
 - Beendung der Sitzung ohne Nachricht, mit RST
 - Es muß mindestens 2MSL gewartet werden, anderenfalls werden FIN-Segmente übersehen
- Auch TCP-Sitzungen können über Stunden inaktiv sein
 - Blockierung kleiner Adreßräume bei einfachem NAT fast unvermeidlich





Port Address Translation (PAT)

... department security technology ... department security technology ... department security technology ... department security technology ...

- Adreßabbildung umfaßt bei TCP, UDP Adresse und Portnummer
 - eine globale Adresse kann so bis zu 65535 TCP- und UDP-Verbindungen abbilden
 - Extern erreichbare Dienste müssen statisch abgebildet werden

- Fragmentierung und PAT
 - Zuordnung der Fragmente erfolgt über ID im 1. IP-Fragment „Fragment Identification“. Weitere Fragmente enthalten keine Portnummern
 - Verbindungen von 2 Interne Knoten auf denselben Host: Host kann Fragmente nicht unterscheiden





Weitere Probleme von NAT und PAT

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Einige Anwendungsprotokolle (RealAudio...) fügen Adressen in Nutzlast ein: Erfordern ALGWs
 - Bei Schutz durch IPSec nicht möglich
- Sitzungsorientierte Protokolle mit getrennten Datenverbindungen (FTP...) tauschen im Kontrollkanal Adressen und Ports aus: Erfordern ALGWs
- P2P-Protokolle benötigen meistens Server-Adressen
- Lösungen über DNS-Modifikation sind meist unbefriedigend
 - Caching sorgt für Inkonsistenzen bei schneller Änderung der DNS-Abbildung





Virtual Private Networks (VPN)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Private Network: Komponenten stehen nur einer Organisation zur Verfügung (also auch gemietete Standleitungen)
- VPNs sollen Merkmale von Private Networks über öffentliche Netzwerke anbieten
 - Verwendung nicht zulässiger Adressierungsschemata
 - Nutzung „fremder“ Netzwerkprotokolle
 - Vertraulichkeit, Integrität, Verfügbarkeit
- Hauptmotivation: Kostenersparnis
 - Bandbreite von Private Network muß sich an Spitzenlasten orientieren, VPN kann dynamisch Ressourcen verwenden





VPN auf Basis von IPSec

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- IPSec kann in zwei Modi betrieben werden
- Transport Mode
 - Ende-zu-Ende Verbindung
 - ▲ Beide Endpunkte müssen IPSec beherrschen
 - ▲ Nur Nutzlast (IPv4/IPv6) wird mit ESP, AH bearbeitet
- Tunnel Mode
 - Einer oder beide Endpunkte müssen IPSec nicht beherrschen
 - Komplette „innere“ IP-Pakete werden in „äußeren“ Pakete verpackt





Schlüsselaustausch in IPSec

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Schlüsselaustausch ist unabhängig von Transportsicherung
 - Verknüpfung erfolgt erst über SPD/SAD
- Einfachste Variante:
Vorvereinbarte symmetrische Schlüssel
 - Aufwand n^2 der beteiligten Knoten, kein Re-Keying
 - Vorverteilen von Zertifikaten und Zertifikatsketten beseitigt nur Re-Keying-Problem
- Einsatz von Zertifikaten bedingt meist das Vorhandensein einer Public Key Infrastructure (PKI)
 - Aufwand wird meist unterschätzt: In größeren Firmen kann die Einführung mehrere Jahre und MEUR kosten





Gemeinsamkeiten von Schlüsselaustauschverfahren

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Alle Verfahren verwenden

- zur Geheimnisvereinbarung den Algorithmus von Diffie und Hellman
- zur Vermeidung von DoS-Angriffen auf die Schlüsselgenerierung einen Cookie-Mechanismus

■ Kategorien von Verfahren:

- Rahmenprotokolle zur Festlegung von Verfahren (z.B. Oakley)
- Explizite Verfahren (IKE, SKIP, Photuris)
- Mischprotokolle, die mehrere Verfahren vereinen (ISAKMP)





- Meta-Protokoll, das Verfahren, Datenstrukturen, Protokolle für Aushandlung von Security Associations definiert
 - Ursprünglich für mehr als IPSec (z.B. TLS) geplant
 - erfordert starke Authentisierung mittels digitaler Signatur
 - ▲ Algorithmen, Zertifikate sind nicht spezifiziert
 - erfordert authentisierten Mechanismus für Schlüsselaustausch
 - Details müssen in „Domain of Interpretation“ Dokument festgelegt werden. Darin enthalten:
 - ▲ Repräsentation von Datenstrukturen, Sicherheitsmechanismen, Syntax für Spezifikation, Benennung





Phasen von ISAKMP

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Primäre Phase

- Aushandlung von SAs zwischen je 2 ISAKMP-Instanzen
 - ▲ Es können mehrere SAs für Paare von Systemen existieren
 - ▲ (Neu-) Verhandlungen über sekundäre SAs werden über primäre SAs geführt
 - ▲ Erfordert Einsatz von Cookies
(Verifikation einfacher als als Diffie-Hellman)

■ Sekundäre Phase/SAs

- Sicherheitsmechanismen für Nutzdaten-Protokolle
- Benötigen keine asymmetrischen Verfahren: schnell





Austauschmechanismen in ISAKMP (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Base Exchange

- Sender erzeugt Proposal mit Zufallswert (Schutz vor Wiedereinspielung)
- Empfänger reagiert mit Nachricht der akzeptierten Verfahren, mit Zufallswert
- Bei Schnittmenge: 2 weitere Nachrichten für Aufbau eines gemeinsamen Geheimnisses, Identitäten der Parteien
 - ▲ Identifikation erst jetzt möglich da Authentisierungsfunktion erst ausgehandelt werden mußte
 - ▲ Kostspielig: 4 Nachrichten, evtl. asymmetrische Operation





Austauschmechanismen in ISAKMP (2)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Identity Protection Exchange

- Ermöglicht Austausch von Schlüsselmaterial ohne daß dafür die Identität der Parteien von Dritten mitgelesen werden kann
- Schritte 1+2 analog zu Base Exchange
- 2 weitere Nachrichten: Austausch von D-H Teilschlüsseln, Zufallswerten
- 2 weitere Nachrichten für Austausch der Identitäten und Authentisierung unter Schutz des zuvor vereinbarten gemeinsamen Geheimnisses





Austauschmechanismen in ISAKMP (3)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Authentication Only Exchange

- Soll eingesetzt werden wenn kein Schlüsselmateriale ausgehandelt werden muß
- Benötigt nur drei Nachrichten
- 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





Austauschmechanismen in ISAKMP (4)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Aggressive Exchange

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





Oakley

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Als Implementierung von ISAKMP vorgesehen

- Kernverfahren basieren auf Station-to-Station-Protokoll von Diffie, van Oorschot und Wiener
- Cookies zur Vermeidung von DoS-Angriffen und zur Benennung von Schlüsseln: 64 Bit Zufallszahlen
 - ▲ Sender und Empfänger generieren je 1 Cookie, Schlüssel wird durch Verknüpfung identifiziert
- Wechselseitige Aushandlung von Verschlüsselungs- und Authentisierungsalgorithmen: Zertifizierte, unzertifizierte oder vorvereinbarte Schlüssel
- Aushandlung von Sitzungsschlüsseln





Authentisierung von Schlüsseln in Oakley

... department security technology ... department security technology ... department security technology ... department security technology ...

- Vorvereinbarte Schlüssel
- DNSSEC-Erweiterungen (Schlüssel, Zertifikate im DNS)
- Nicht zertifizierte RSA-Schlüssel, Verfahren analog zu „web of trust“ in PGP
- Zertifizierte RSA-Schlüssel
- Zertifizierte DSS-Schlüssel
 - Fast alles ist optional, genaue Verfahren sind nicht spezifiziert
 - Quelle für fast beliebige Kompatibilitätsprobleme





Schlüsselerneuerung in Oakley

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Nach Ablauf einer bestimmten Zeitspanne oder nach Austausch einer bestimmten Datenmenge:
Neuverhandlung der SA-Schlüssel
 - Angreifer steht weniger Zeit zur Verfügung um Chiffre (z.B. durch Brute Force) zu brechen
 - Die Menge an Chiffretext (evtl. auch Klartext/Chiffretext-Paare) unter einem Schlüssel wird begrenzt

- Parteien tauschen unter bestehender Sitzung **Nonces** aus die zum neuen Schlüssel verknüpft werden





Internet Key Exchange (IKE)

... department security technology ... department security technology ... department security technology ... department security technology ...

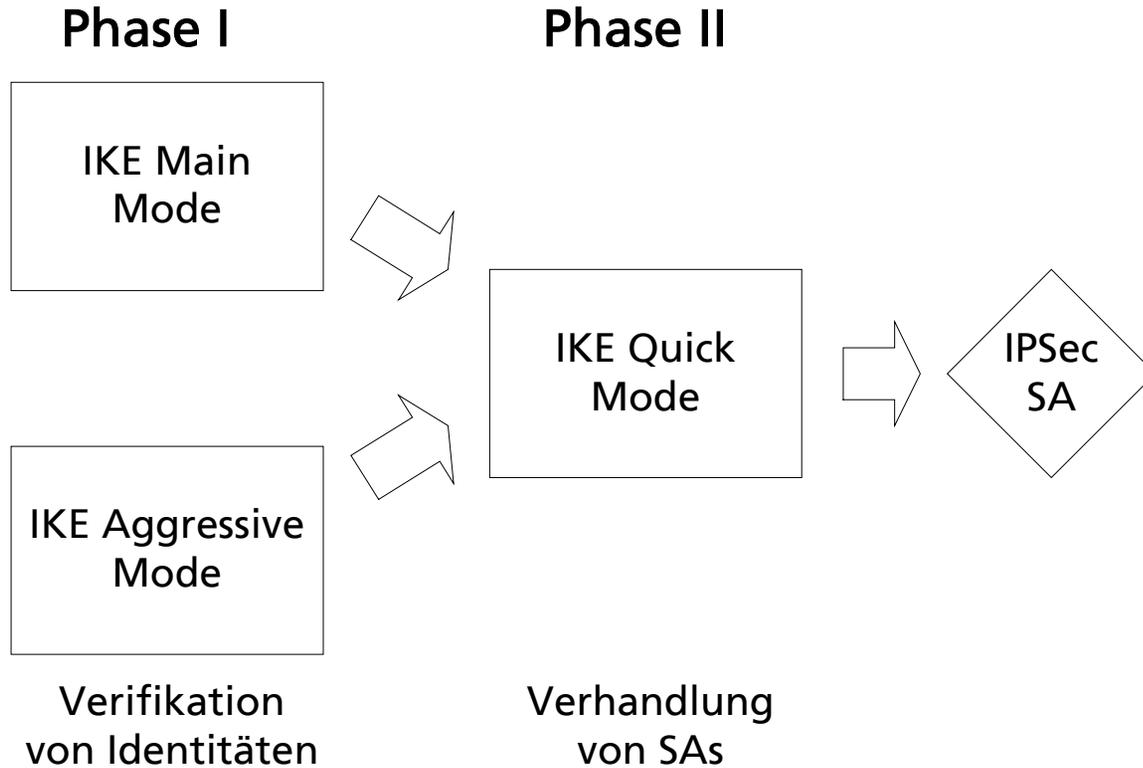
- Hybrid aus ISAKMP und Oakley mit Anleihen bei SKEME, erlaubt Bestimmung von
 - Verschlüsselungsalgorithmus
 - Hash-Algorithmus
 - Authentisierungsmethode
 - Parameter für Diffie-Hellman-Schlüsselvereinbarung
- IKE verwendet Terminologie von ISAKMP (Unterteilung in zwei Phasen)
- Austausch auf 500/udp: Quell- **und** Zieladresse





Phasenmodell bei IKE

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





Phasen in IKE

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Phase I: Zufallsdaten und Identitätsmerkmale (Public Key-Zertifikate) werden unter asymmetrischer Verschlüsselung ausgetauscht
 - Diffie-Hellman-Schlüsselaustausch wird parallel ausgetauscht
 - Beweis der Identität erfolgt über
 - ▲ Hash-Wert der entschlüsselten Daten oder
 - ▲ Daten (insb. Zufallswerte), mit symmetrischer Chiffre verschlüsselt

- Phase II: Schlüsselerzeugung und Austausch der SA-Parameter





Beliebte Probleme in der Praxis

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Lebensdauer von SAs kann an Endpunkten konfiguriert werden
 - Eine Seite bricht ohne Neuverhandlung einfach ab

- Path MTU Discovery
 - IPSec bewirkt insbesondere bei Tunnel Mode Verringerung der PMTU - Implementierungen müssen darauf reagieren
 - Es kann günstig sein, die MTU manuell niedriger zu setzen: Fragmentierung sorgt für katastrophale Geschwindigkeit

- Cisco-Spezialität (IOS 12.0.(x)):
 - Automatische IKE Key Renegotiation findet nicht statt sobald Lebensdauer der Schlüssel abläuft...





Generelle IPSec-Probleme

... department security technology ... department security technology ... department security technology ... department security technology ...

- IPSec selbst ist vergleichsweise einfach zu implementieren
- Spezifikation von Schlüsselaustauschmechanismen umfangreich, komplex, ungenau spezifiziert
 - Bestrebungen für vereinfachte Version von IKE existieren, Erfolgsaussichten für tatsächliche Vereinfachung eher fraglich
- IKE etc. erfordern erheblichen Implementierungs-Overhead: PKIX, X.509, X.68x, LDAP bzw. X.500, OCSP... und eine funktionstüchtige PKI





Generic Routing Encapsulation Protocol (GRE)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Entwicklung immer neuer spezieller Protokolle für das Tunneln von Protokoll X in Protokoll Y
 - GRE sollte allgemeinen Mechanismus bieten, um OSI Layer 3 Protokolle zu tunneln

- Pakete bestehen aus drei Komponenten:
 - Delivery Header: Protokollspezifischer Header des äußeren Protokolls für den Nutzlasttransport
 - GRE Header: Gibt zu tunnelnden Protokolltyp an sowie Zusatzinformationen zur Nutzlast (optional)
 - Payload Packet: Pakete des „inneren“ Protokolls





Der GRE-Header (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Flags und Versionsnummer: 2 Bytes mit Bit-Flags

- Bit 0: „Checksum Present“
- Bit 1: „Routing Present“ (Routing und Offset-Felder)
- Bit 2: „Key“-Feld vorhanden
- Bit 3: Sequenznummer gesetzt
- Bit 4: Strict Source Routing
- Bits 5-7: Maximale Rekursionstiefe für Tunneling
- Bits 8-12: Reserviert, muß 0 sein
- Bits 13-15: Versionsnummer als Ganzzahl: Muß nach RFC 1701 0 sein.





Der GRE-Header (2)

... department security technology ... department security technology ... department security technology ... department security technology ...

- Protocol Type: 2 Bytes, nach IEEE 802.3/1H (z.B. 2048 für IP)
- Offset: 2 Bytes: Beginn des aktiven Routing-Eintrags
- Prüfsumme: 2 Bytes, analog zu IP-Prüfsumme
- Key: 4 Bytes frei zwischen Parteien zu definierend
- Sequenznummer: 4 Bytes, vorzeichenlose Ganzzahl, wird von Absender eingetragen. Keine Vorgaben seitens GRE über den Inhalt
- Routing: Variable Länge, Einträge aus 4 Feldern: Address Family, Source Routing Entry Offset, SRE Length, Routing-Daten. Semantik ist von RFC 1701 ebenfalls undefiniert.





Verwendung von GRE

... department security technology ... department security technology ... department security technology ... department security technology ...

- Mit RFC 1702 wurde IP als „äußeres“ Protokoll definiert (IP-Protokoll 47), umgekehrt ist GRE-Protokollfeld 2048.
- Vereinfachung mit RFC 2784 im März 2000, eine Reihe von Feldern wurden als „unerwünscht“ definiert (Routing, Key,...)
 - Aufgrund weiter Verbreitung von GRE/RFC1701 müssen Implementierung immer noch diese Optionen unterstützen
- GRE verfügt über keine eigenen Sicherheitsmechanismen
- Problem: Erhöhung der Nutzlast-Größe von Paketen bei Tunnelung (MTU)
 - Einige Implementierungen sind damit wohl überfordert...





Layer Two Tunneling Protocol (L2TP)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Point to Point Protocol (PPP) bietet einen Transportmechanismus auf OSI-Ebene 2 für Punkt-zu-Punkt-Verbindungen
 - Vor Verbindungsaufbau findet Authentisierungsphase statt
- L2TP erweitert PPP: Endpunkte von Verbindungen können auf beliebigen Knoten eines verbindungslosen Netzwerkes liegen
 - Anwendungsbeispiel: Einwahl über Dienstleister-Netz vor Ort in entferntes Firmennetz (Kostensparnis)
 - Anders als z.B. bei PPPoE wird kein spezielles Trägerprotokoll vorausgesetzt





Nachrichtentypen in L2TP

... department security technology ... department security technology ... department security technology ... department security technology ...

■ Kontrollnachrichten

- Für Aufbau, Modifikation, Abbau von Tunneln und Verbindungen
- L2TP stellt Zuverlässigkeit von Kontrollkanal durch eigenes Protokoll sicher

■ Datennachrichten

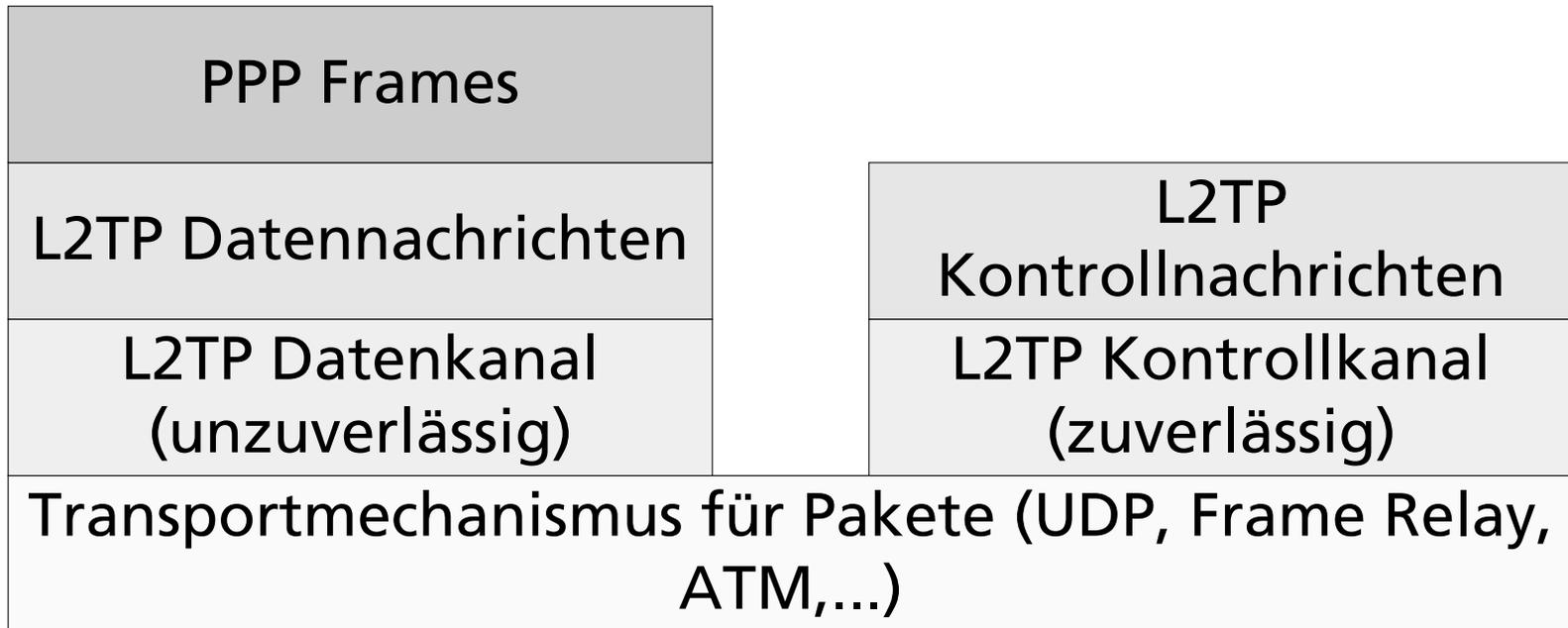
- kapseln PPP-Frames innerhalb von Tunneln
- Datenkanal wird als unzuverlässig modelliert: L2TP versendet selbst keine verlorenen / verfälschten Pakete erneut





Struktur des L2TP-Protokolls

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





Der L2TP-Header

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

T	L			S		O	P					Version	Length
Tunnel ID												Session ID	
Ns												Nr	
Offset Size												Offset Padding	

- T: Typ (0 = Datennachricht)
- L: Längenfeld vorhanden
- S: Sequenznummer vorhanden
- O: Offset-Feld vorhanden
- P: Priority (nur für Datennachrichten)





Sitzungsaufbau

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Aufbau einer Kontrollverbindung

- Darin geschachtelt: „Verbindungen“ zwischen Endpunkten
 - ▲ Darin geschachtelt: „Sitzungen“
 - ▲ Tunnel 0 / Sitzung 0 ist reserviert für Aufbau neuer Tunnel und Sitzungen
- Feststellung von Protokollversion, optionale Charakteristika
- Identifizierung und Authentisierung
 - ▲ Protokoll ist optional (von PPP/CHAP abgeleitet)
 - ▲ Für L2TP über IP existiert seit RFC 3193 eine I&A-Anbindung an IPSec





Nutzdaten

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Nachrichten werden in erweiterbarem innerem Protokoll übertragen: 2-Tupel mit Header
 - Unterteilt in notwendige und optionale Elemente
 - Identifikation der Tupel über Vendor-ID (von IANA vergeben, eindeutig), darin werden „Attribute Types“ vergeben
- Nutzlast ist variabel, folgt dem Attribute Type.
- RFC 2661 definiert nur wenige Basis-Tupel, ansonsten frei erweiterbar





Point to Point Tunneling Protocol

... department security technology ... department security technology ... department security technology ... department security technology ...

- Von Microsoft in Konkurrenz zu L2TP definiertes Protokoll
 - entstand aus nicht abwärtskompatibler Modifikation an GRE
 - nur für TCP/IP als „äußeres“ Protokoll definiert
- Aushandlung von Tunneln, Sitzungen erfolgt out of band auf Port 1723/tcp
 - Kontrollnachrichten haben feste Länge:
 - ▲ 2 Bytes Gesamtlänge, 2 Bytes Typ, Magic Cookie (0x1A2B3C4D), 2 Bytes Kontrollnachricht-Typ, 2 Bytes reserviert, 2 Bytes Protokollversion
 - Datennachrichtung: modifizierter GRE-Header





Authentisierung in PPTP (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Drei Authentisierungsmethoden

- Klartext-Paßwort
- Hash-Paßwort
 - ▲ Einfaches Hashing entspricht „LAN Manager Hash“
 - ▲ Paßwort wird auf 14 Bytes gebracht, zu Großbuchstaben konvertiert, in 2 Hälften zu 7 Bytes gespalten, jede Hälfte wird als einzelner DES-Schlüssel verwendet um eine Konstante zu verschlüsseln. Verkettete Ergebnisse sind Hashwert
 - ▲ Kein Salt, entspricht Stärke von 1x DES, Wörterbuch...
 - △ Kuriose Sammlung von Anfängerfehlern
 - △ Wunsch nach Abwärtskompatibilität erhält dieses Protokoll in heterogenen Windows-Umgebungen noch länger am Leben





Authentisierung in PPTP (2)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Challenge/Response

- Ebenfalls beschränkt auf 14 Zeichen (durch Paßwort-Dialog: Algorithmus verkraftet bis 128 Zeichen!)
- Vollständiges Paßwort wird mit MD4 gehasht
 - ▲ MD4 ist verwundbar, Salt wird auch hier nicht verwendet

■ MS Point-to-Point Encryption

- Realisiert als Option in PPP Compression (!)
- Auch in aktueller Fassung (RFC 3078) gefährlicher Schwachpunkt: Schlüssel leitet sich aus Paßwort ab
 - ▲ keine Integritätssicherung

