Ciscos Group Encrypted Transport VPN – Eine kritische Analyse

Michael Rossberg · Guenter Schaefer

Fachgebiet Telematik/Rechnernetze
Technische Universität Ilmenau
[michael.rossberg, guenter.schaefer]@tu-ilmenau.de

Zusammenfassung

Der zunehmende Einsatz von öffentlichen Netzen zur Abwicklung der internen Kommunikation von Firmen und Behörden ermöglicht eine höhere Flexibilität bei gleichzeitigen Kostenersparnissen. Doch birgt dies auch Risiken in Bezug auf die IT-Sicherheit, die erst durch IPsec-VPN-Systeme tragbar werden. Die Firma Cisco möchte mit ihrer Group Encrypted Transport (GET) Lösung die, zurzeit relativ komplexe, IPsec-Verwaltung vereinfachen und setzt dazu ein Protokoll zur Verteilung von Gruppenschlüsseln ein. Dieser Artikel analysiert, wie durch diese Vereinfachungen fundamentale Sicherheitseigenschaften verändert werden und diskutiert anschießend Einsatzmöglichkeiten und Grenzen des Ansatzes.

IPsec zum Schutz von Kommunikationsinfrastrukturen

Der Betrieb von IPsec-Infrastrukturen zur Sicherung von organisationsinterner Kommunikation zieht heutzutage oft einen hohen Verwaltungsaufwand nach sich. Bei der manuellen Einrichtung sind zwischen allen beteiligten IPsec Gateways Sicherheitsrichtlinien zu konfigurieren. Da die Anzahl der zu wartenden Sicherheitsrichtlinien bei einer Vollvermaschung quadratisch mit der Anzahl der Gateways eines VPN wächst, kann der Aufwand schnell wachsen. Bereits das einfache Beispiel in Abbildung 1 muss ein Administrator 12 Einträge in der Security Policy Database (SPD) pflegen. Diese Komplexität ist ein oftmals bemängelter funktionaler Nachteil von IPsec. Er führt bei manueller Konfiguration aber unter Umständen auch zu Sicherheitsproblemen [FeSc00], da bei der manuellen Pflege der Einträge fehlerhafte Daten hinzugefügt oder ehemals korrekte nicht oder nicht vollständig entfernt werden.

Die Firma Cisco hat in ihre Router mit IOS Version 12.4(11)T ein System integriert, das die automatische IPsec-Einrichtung von virtuellen privaten Netzen (VPN) zur Vernetzung von Firmenstandorten verspricht. Dabei richtet der Group Encrypted Transport (GET) [Cisc07, Bhai08] genannte Ansatz mithilfe von zentralen Schlüssel-Servern Gruppenschlüssel in allen Routern ein, welche zum Verbund gehören. Diese können dann sowohl über Multicast als auch über Unicast direkt miteinander kommunizieren, da alle über dieselben Schlüssel und Sicherheitsbeziehungen (security association, SA) verfügen.

P. Horster (Hrsg.) · D.A.CH. security · syssec (2009) pp.

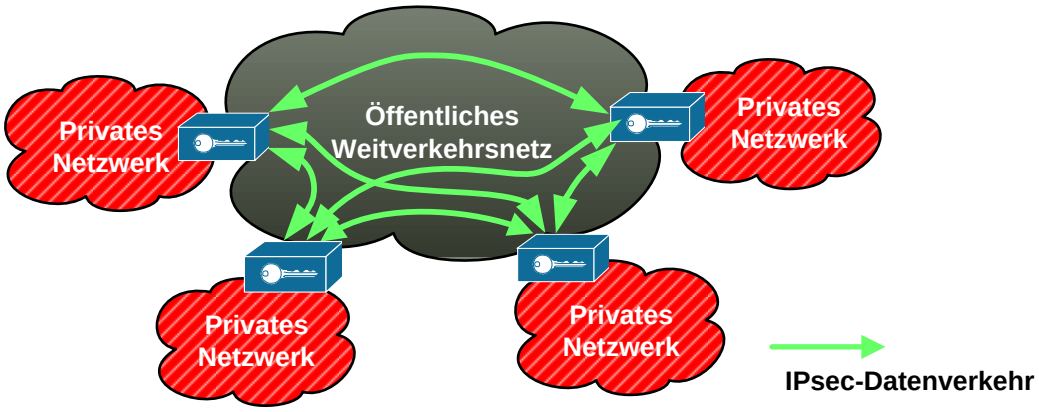

Abbildung 1 – Einfaches Beispiel einer IPsec-Infrastruktur mit Vollvermaschung

Neben dem Schlüsselaustausch verändert GET auch die Behandlung von IPsec-Datenpaketen. GET arbeitet zwar im IPsec-Tunnelmodus verwendet aber große Teile des inneren IP-Headers zur Konstruktion des äußeren. Dadurch wird auch das Differentiated-Services-Code-Point (DSCP) Feld kopiert und somit DiffServ unterstützt. Ferner wird der IPsec-Schutz gegen wiedereingespielte Pakete durch einen proprietären Zeitfenstermechanismus ersetzt, da die Sequenznummern des IPsec-Standards die mehrfache Verwendung einer SA nicht unterstützen.

Dieser Artikel stellt im Folgenden die umfangreichen Anforderungen zusammen, die im Allgemeinen an IPsec-Infrastrukturen gestellt werden, und analysiert Ciscos GET-Technologie. Dabei tritt eine schwerwiegende sicherheitstechnische Schwächung gegenüber der herkömmlichen manuellen IPsec-Konfiguration zu Tage, und es werden auf der Grundlage der Analyse Hinweise für den Einsatz von GET abgeleitet.

Anforderungen

Zu den Anforderungen an Systeme zur IPsec-Autokonfiguration gehören neben funktionalen Eigenschaften auch nicht-funktionale, zu denen auch die kritischen Sicherheitsanforderungen gehören. Anforderungen aller Bereiche werden in den folgenden drei Unterabschnitten angegeben und kurz erläutert.

Funktionale Anforderungen

Ein Autokonfigurationsmechanismus muss die folgenden funktionalen Anforderungen erfüllen, um einen möglichst großen Teil existierender IPsec-Infrastrukturen zu unterstützen:

- **Einfache Konfiguration und Rekonfiguration:** Das Einfügen, das Entfernen und das Bewegen von IPsec Gateways soll ohne umfangreiche manuelle Intervention erfolgen.
- **Geschachtelte Netzwerke:** Die zu konfigurierende IPsec-Infrastruktur besitzt unter Umständen IPsec Gateways, welche hinter anderen IPsec Gateways beispielsweise aus Sicherheitsgründen verborgen sind. Diese müssen erkannt werden und Datenpakete entsprechend geroutet werden.
- **Private IP-Adressbereiche:** Viele IPsec-Infrastrukturen nutzen intern private IP-Adressbereiche, da diese ohne vorherige Beantragung verfügbar sind. Pakete an diese

privaten IP-Adressbereiche müssen in der Regel von IPsec-Mechanismen geroutet und so anderen IPsec Gateways verfügbar gemacht werden.

- **Quality of Service (QoS):** Falls das Transportnetzwerk QoS unterstützt soll, je nach Sicherheitspolitik, diese Möglichkeit auch durch IPsec genutzt werden.
- **Keine Notwendigkeit von Multicast im Transportnetz:** Weite Teile der Internet-Infrastruktur unterstützen kein IP-Multicast, daher sollte ein automatisches System zur Einrichtung von IPsec-Netzen diese Eigenschaft nicht voraussetzen.
- **Multi-/Any-/Broadcast im VPN:** Spezielle Formen der Gruppenkommunikation sollten in den IPsec-Netzen unabhängig von der Transportnetzwerkunterstützung verfügbar sein.

Nicht-funktionale Anforderungen

Zusätzlich müssen eine Reihe nicht-funktionaler Anforderungen bestmöglich erfüllt werden:

- **Skalierbarkeit:** Das IPsec-Netzwerk muss über die Anzahl der IPsec Gateways skalieren. Insbesondere darf kein exponiertes System existieren, dass einen Flaschenhals darstellen kann.
- **Robustheit:** Das IPsec-Netz darf auch auf seltene Ereignisse nie unkontrolliert reagieren. Es darf beispielsweise kein Single Point of Failure (SPoF) existieren, und bei einer Netzwerkpartionierung müssen die entstandenen Teilnetzwerke unabhängig von einander einsatzfähig bleiben.
- **Agilität:** Mobile IPsec Gateways, beispielsweise Road-Warrior, sollen in der Lage sein schnell dem Verbund beizutreten und ihn schnell wieder zu verlassen.

Aufgrund ihres Umfanges und ausschlaggebenden Bedeutung werden die Sicherheitsanforderungen, die ebenfalls nicht-funktional sind, im folgenden eigenen Abschnitt diskutiert.

Sicherheitsanforderungen

Im Allgemeinen werden an Systeme die folgenden sicherheitsrelevanten Anforderungen gestellt (Kategorisierung teilweise aus [Scha03]):

- **Vertraulichkeit:** Neben der eigentlichen Vertraulichkeit der übertragenen Daten durch das unsichere Netzwerk sollen folgende Unterziele von VPN realisiert werden:
    - **Covert-Channel-Resistenz:** IPsec Gateways sorgen in VPN für die Durchsetzung von Sicherheitspolitiken, somit sollen Rechner, die sich hinter solchen befinden, nicht in der Lage sein über verdeckte Kanäle mit der Außenwelt zu kommunizieren. IPsec realisiert dies durch eine Zwangsverschlüsselung im Tunnel-Modus und gegebenenfalls Paddings, mit denen Pakete auf feste Längen gebracht werden. Aufgrund dieser Maßnahmen können weder im IP-Header noch mittels einer Variation der Paketlängen Informationen nach außen transportiert werden.
    - **Perfect Forward Secrecy (PFS):** Das Kompromittieren eines Schlüssels oder Zertifikates nach Ablauf der Kommunikation, darf nicht bewirken, dass die

Sitzungsschlüssel von Dritten wiederherzustellen und somit potenziell aufgezeichnete Kommunikationsvorgänge zu entschlüsseln sind.

- **Infrastructure Hiding:** Der Aufbau der Kommunikationsinfrastruktur, insbesondere solcher Teile, die sich hinter IPsec Gateways befinden, soll nicht durch Außenstehende zu erkennen sein, sodass Verkehrsflussanalysen erschwert werden. Insbesondere dürfen keine intern verwendeten IP-Adressen unverschlüsselt übertragen werden, da sonst eine Schätzung der Größe von Teilnetzen des VPN ermöglicht wird.

- **Zurechenbarkeit/Integrität:** Damit die ausgetauschten Daten zu jedem Zeitpunkt einer Partei zugeordnet werden können, müssen über das VPN versandte Daten über eine Signatur oder einen Message Authentication Code (MAC) verfügen. Letztere können in Multicast-Umgebungen allerdings oft nicht eingesetzt werden, da es sich um ein symmetrisches System handelt. Jede Partei, die ein Paket authentisieren kann, kann auch gültige MAC generieren, so dass der eigentliche Sender nicht genau identifiziert werden kann. Es kann mit einem MAC lediglich überprüft werden, ob ein Mitglied der Gruppe die Nachricht versandt hat.

  Zum Erreichen der Zurechenbarkeit ist ferner ein Replay-Protection-Mechanismus erforderlich, sodass keine alten Datenpakete erneut verarbeitet werden und Angreifer Kommunikationsvorgänge nicht zu späteren Zeitpunkten wieder verwenden kann.

- **Verfügbarkeit:** VPN müssen auf Angriffe robust reagieren, sodass die Auswirkungen des Angriffs auf die Kommunikation der Teilnetzwerke minimiert werden. Dazu existieren folgende Teilziele:

  - **Denial-of-Service (DoS) Resistenz:** Ein verfügbares VPN muss robust auf DoS-Angriffe reagieren. Dies impliziert in der Regel eine dezentrale Architektur, da zentrale Komponenten einen potenziellen SPoF darstellen.

  - **Graceful Degradation:** Ferner kann ein robustes Verhalten bei einem teilweise kompromittierten VPN gefordert sein, sodass bei Angriffen jeglicher Art in nicht direkt betroffenen Teilen des VPN alle Sicherheitsziele weiter erfüllt werden können.

- **Zugriffskontrolle:** Um die Datenvertraulichkeit sicherstellen zu können, muss in einem VPN die Entscheidung getroffen werden, welche Instanzen zu welchen Daten Zugriff erhalten dürfen. Beim Einsatz von Multicast-Protokollen schließt dies folgende Mechanismen [HaDo03] ein:

  - **Backward Access Control:** Werden neue VPN-Gateways dem Netz hinzugefügt, sollen diese nicht in der Lage sein vorher ausgetauschte Daten zu entschlüsseln. Dies bedeutet alle betroffenen Gruppenschlüssel des VPN müssen neu ausgehandelt werden.

  - **Forward Access Control:** Analog dürfen Gruppenschlüssel nicht mehr verwendet werden, wenn ein Teilnehmer die Gruppe verlässt, da das ehemalige Mitglied sonst in der Lage ist Verkehr weiterhin zu entschlüsseln und zu generieren.

  Somit müssen Gruppenschlüssel mit jeder Veränderung des VPN-Verbundes sicher erneuert werden.

- **Secure-By-Default**: Um eine Fehlkonfiguration zu vermeiden, sollen alle VPN- Konfigurationseinstellungen werksseitig das höchste Sicherheitsniveau garantieren und nicht auf umfangreiche manuelle Eingriffe angewiesen sein.

Mit Ausnahme der Secure-By-Default-Eigenschaft können alle diese Sicherheitsziele durch eine sorgfältige, manuelle IPsec-Konfiguration erreicht werden.

Nach dem Ableiten der umfangreichen Anforderungen an einen IPsec-Autokonfigurationsmechanismus wird im Folgenden Ciscos GET Ansatz erläutert.

Cisco GET-VPN

Zentraler Ansatzpunkt von GET ist der Einsatz von Verschlüsselungsmechanismen, welche ursprünglich für die Gruppenkommunikation (Multicast) entwickelt wurden. Dabei werden Unicast-Pakete lediglich als ein Spezialfall der many-to-many Kommunikation betrachtet.

Die IPsec Gateways kontaktieren dazu beim Beitritt zum IPsec-Verbund einen zentralen Schlüssel-Server (siehe Abbildung 2), der statisch in jedem Gateway konfiguriert werden muss. Mit dem Schlüssel-Server wird zunächst eine normale IKE Phase-1-Aushandlung ausgeführt. Während im Normalfall in der anschließenden Phase-2-Aushandlung jedoch eine SA zwischen den kommunizierenden Parteien eingerichtet wird, werden in GET vom Schlüssel-Server zum IPsec Gateway mit Hilfe von GDOI [BWHH03] zwei gruppenweit gültige symmetrische Schlüssel versandt.

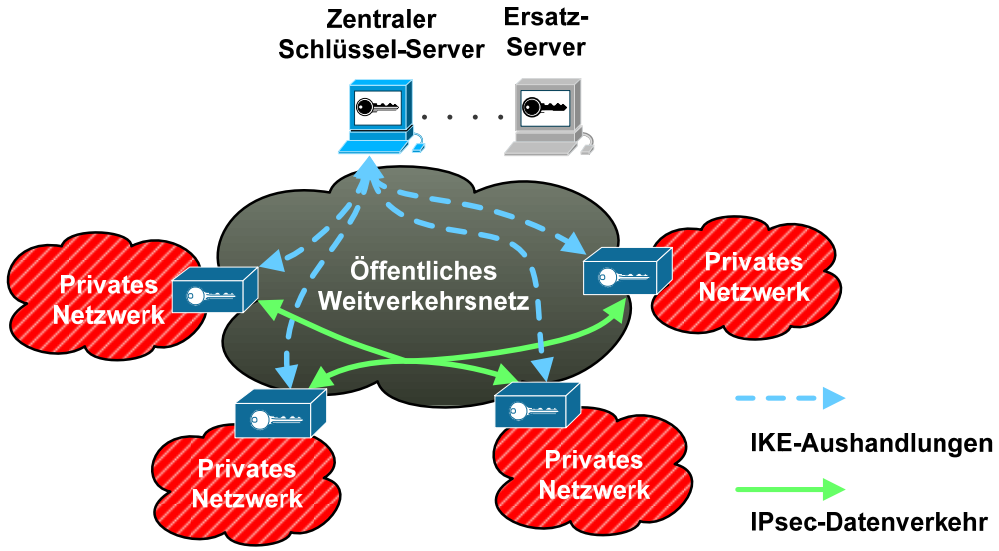

Abbildung 2 – Beispiel eines GET-VPN-Einsatzszenarios

Einer dieser Schlüssel wird zum Verschlüsseln sämtlicher Daten, die über das öffentliche Netzwerk übermittelt werden, verwendet. Der andere Schlüssel dient dem Schutz periodischer Schlüsselaustausche, die vom Schlüssel-Server zu den Sicherheits-Gateways gesendet werden. Die Übertragung geschieht wahlweise über eine Unicast-Nachricht zu jedem Sicherheits-Gateway oder via einer Multicast-Nachricht. Um eine gewisse Ausfallsicherheit zu bieten werden bis zu 7 Ersatz-Server unterstützt, welche bei Störungen die Aufgaben des Schlüssel-Servers übernehmen können. Eine Load-Balancing-Funktion zwischen den Schlüssel-Servern ist nicht vorgesehen.

Da alle Gateways nach einer erfolgreichen IKE-Aushandlung dieselben kryptographischen Schlüssel besitzen, können sie untereinander beliebige, verschlüsselte Nachrichten austauschen. Sofern der Netzbetreiber des öffentlichen Netzes es erlaubt, können auch Multicast-Nachrichten zwischen den privaten Netzen ausgetauscht werden.

Optional kann dabei in GET ein Cisco-proprietärer Mechanismus zum Einsatz kommen, um das Duplizieren von verschlüsselten Paketen durch Angreifer zu erkennen. Das Verfahren basiert auf Zeitstempeln und erlaubt Pakete nur in einem konfigurierbaren Zeitfenster von 1 bis 100 Sekunden.

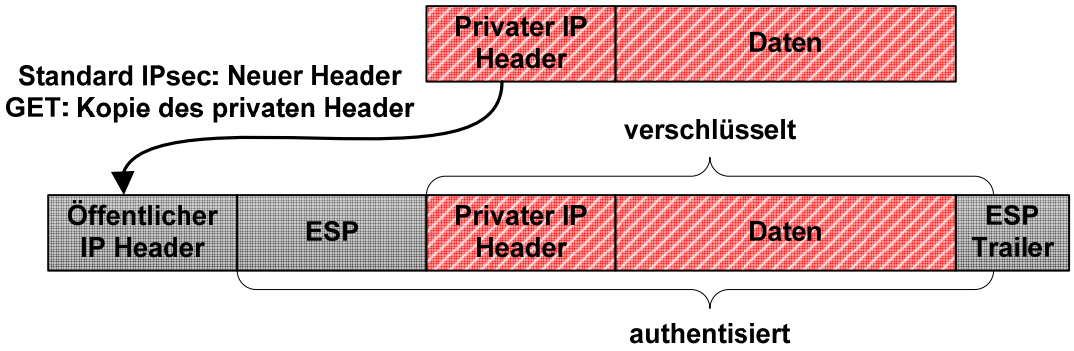

Abbildung 3 – IPsec-Verarbeitung im ESP-Tunnelmodus (Eingabepaket oben, Ausgabe unten), GET übermittelt vormals private Daten im öffentlichen Teil des IPsec-Paketes

Eine weitere Besonderheit von GET ist der „tunnellose“ Arbeitsmodus (siehe Abbildung 3). Hierbei wird IPsec zwar im Tunnelmodus betrieben, allerdings wird zum Bilden des äußeren, nicht kryptographisch geschützten Headers der Original-Header kopiert. Dies spart zunächst die relativ aufwendige Abbildung von inneren IP-Headern auf vom Administrator zu konfigurierende äußere. Ferner möchte Cisco so eine Quality-of-Service-Unterstützung ermöglichen, da auch das Type-of-Service- beziehungsweise Differentiated-Services-Code-Point-Feld vom Paket des Rechners im privaten Netz übernommen wird.

Analyse

Die im Folgenden gegebene Untersuchung des GET-Ansatzes gliedert sich analog zur Strukturierung der Anforderungen in drei Unterabschnitte.

Erfüllung der funktionalen Eigenschaften

- **Einfache Konfiguration und Rekonfiguration:** GET ermöglicht es auf einfache Weise IPsec Gateways dem Verbund hinzuzufügen. Dazu müssen die Gateways lediglich mit einem Zertifikat oder Passwort, sowie den IP-Adressen der Schlüssel-Server ausgestattet werden. Das Entfernen oder Bewegen eines Gateways erfordert keine manuelle Interaktion. Dennoch kann ein erheblicher Konfigurationsaufwand entstehen, wenn beispielsweise ein Backup-Server hinzugefügt werden soll. In diesem Fall müssen alle IPsec Gateways manuell rekonfiguriert werden. Ganz ähnlich verhält es sich wenn die Schlüssel-Server während eines DoS-Angriffes oder Provider-Wechsels neue IP-Adressen erhalten sollen.

- **Geschachtelte Netzwerke:** Da GET keinen neuen äußeren IP-Header konstruiert und lediglich den inneren IP-Header kopiert, verliert IPsec durch GET seine Routing-Funktion. Die Umsetzung geschachtelter Netzwerke ist somit nicht möglich.
- **Private IP-Adressbereiche:** Auch wenn Cisco immer wieder private IP-Adressbereiche in den Konfigurationsbeispielen verwendet, so erfordert dies ein Routing dieser IP-Adressen durch das öffentliche Weitverkehrsnetz und entsprechende Abkommen mit einem Internet-Provider. Im Allgemeinen ist der Einsatz privater IP-Adressbereiche nicht möglich.
- **Quality of Service (QoS):** Durch das Kopieren des inneren IP-Headers kann GET DiffServ auf einfache Weise umsetzen (eine entsprechende Unterstützung durch das Weitverkehrsnetz vorausgesetzt). Das weitaus mächtigere IntServ-Verfahren ist nicht vorgesehen.
- **Keine Notwendigkeit von Multicast im Transportnetz:** GET benötigt zunächst kein Multicast im Weitverkehrsnetz. Der Schlüssel-Server kann prinzipiell Schlüssel über Unicast an alle IPsec Gateways verteilen. In diesem Fall steigt seine Kommunikationsbelastung allerdings linear mit der Anzahl der Teilnetze.
- **Multi-/Any-/Broadcast im VPN:** Geräte in den privaten Netzen können lediglich Multicast innerhalb des VPN nutzen, und dies auch nur wenn das Weitverkehrsnetzwerk es unterstützt. Eine Unabhängigkeit ist nicht gegeben.

Die Analyse der funktionalen Eigenschaften zeigt deutlich, dass Cisco mit GET viele Probleme gelöst hat, indem die Umsetzung aus der IPsec-Implementierung in die Routing-Funktionalität des Weitverkehrsnetzwerkes verschoben wird. Dadurch wird die Sicherheitsarchitektur sehr schlank. Allerdings wird eine sehr enge Bindung an den Internet-Provider erwartet.

Nicht-funktionale Eigenschaften

Die nicht-funktionalen Anforderungen werden von GET wie folgt erfüllt:

- **Skalierbarkeit:** Durch das Einrichten einer einzigen Sicherheitsbeziehung in den IPsec Gateways skaliert GET an dieser Stelle sehr gut über die Anzahl der Teilnetze. Beim Einsatz von Multicast skaliert das System auch sehr gut bei der periodischen Verteilung von Schlüsseln, da der Schlüssel-Server nur eine Nachricht versendet und alle IPsec Gateways eine Nachricht empfangen.
  Dennoch bildet der zentrale Schlüssel-Server unter Umständen einen Flaschenhals, da er als einzige Instanz neue Gateways dem Netz hinzufügen kann. Insbesondere bei hohen Fluktuationsraten bei sehr vielen mobilen Gateways oder aber nach einem Ausfall kann dies zu Skalierbarkeitsproblemen führen. Unter Umständen verschlimmert sich das Problem: wenn kein Multicast verfügbar ist, und mit jedem neuen IPsec Gateway der Gruppenschlüssel verändert werden soll (Gewährleistung von Backward Access Control), muss mit jedem hinzugefügten Gateway jedes andere kontaktiert werden. Nach einem zentralen Ausfall würden so $O(n^2)$ Nachrichten vom Schlüssel-Server versandt werden müssen.
- **Robustheit:** Trotz der Möglichkeit sieben Backup-Server einzurichten, bleibt der zentrale Schlüssel-Server in GET ein logischer SPoF. Insbesondere bei Netzwerkparti-

tionierungen können Teilnetze unter Umständen nicht unabhängig von einander operieren. Nur wenn in jedem Teilnetzwerk ein Schlüssel-Server verbleibt ist ein unabhängiger Betrieb möglich.

- **Agilität:** Mobile IPsec Gateways können in GET dem Verbund schnell beitreten oder diesen verlassen, solange der Schlüssel-Server die verursachte Last verarbeiten kann. Wenn neue IPsec Gateways einen Schlüsselwechsel verursachen, steigen die an alle anderen IPsec Gateways verteilten Nachrichten entsprechend an.

Insgesamt kann GET die nicht-funktionalen Anforderungen gut erfüllen, solange Multicast eingesetzt werden kann und keine zu große Dynamik in der Netztopologie vorhanden ist. Unter ungünstigen Beispielen kann sich allerdings der zentrale Ansatz negativ auswirken.

Betrachtung der Sicherheitseigenschaften

Durch die GET-Architektur ergeben sich folgende Einschränkungen in Bezug auf die erreichbaren VPN-Sicherheitseigenschaften:

- **Vertraulichkeit:** Die Realisierung der Vertraulichkeit ist in GET prinzipiell möglich, sie hängt von der Einhaltung einer Reihe von Rahmenbedingungen ab. Insbesondere ist das System durch den Einsatz von Gruppenschlüsseln auf vertrauenswürdige Gateways angewiesen. Ein einziges kompromittiertes Gateway, beispielsweise in einer Außenstelle, ermöglicht das Entschlüsseln aller Kommunikationsvorgänge im VPN vom Zeitpunkt des Kompromittierens an.
    - **Covert-Channel-Resistenz:** Durch das Kopieren des inneren IP-Headers in den äußeren, unverschlüsselten Header können Klienten pro Paket einige Bytes an der IPsec-Zwangsverschlüsselung vorbei übertragen und so einen verdeckten Kanal nach außen erzeugen.
    - **Perfect Forward Secrecy (PFS):** Aus dem Time-Sequence-Diagramm in [Cisc07] geht hervor, dass die GDOI-Implementierung von GET kein PFS unterstützt. Somit ermöglicht das Dechiffrieren eines einzigen Rekeying-Paketes (beispielsweise durch Bruteforce-Angriffe), ein Entschlüsseln aller folgender Kommunikationsvorgänge [WwRo07].
    - **Infrastructure Hiding:** Durch das Offenlegen des inneren IP-Headers, können externe Beobachter die innere Struktur des VPN erkennen und genaue Verkehrsanalysen durchführen. Ferner ist es auch für externe Beobachter sehr einfach, den aktiven Schlüssel-Server zu entdecken, da sämtlicher IKE-Verkehr an ihn gerichtet ist.
- **Zurechenbarkeit/Integrität:** Auch die Zurechenbarkeit und Integrität der im GET-VPN ausgetauschten Daten hängt von der Integrität aller IPsec Gateways vor und zum Zeitpunkt der Übertragung ab. Ein kompromittiertes IPsec Gateway kann Pakete mit beliebigen Quelladressen erzeugen, sodass die IP-Adressbereiche verschiedener Teilnetzwerke in GET-VPN nicht zur Identifikation genutzt werden können. Somit ist beispielsweise eine weitere Zugriffskontrolle durch Firewalls wirkungslos.
  Ferner ist es, im Unterschied zum Standard-IPsec, möglich wenigstens innerhalb des konfigurierten Zeitfensters beliebige Pakete wieder einzuspielen. Die Auswirkungen dieses Angriffs hängen von der jeweiligen Anwendung ab.

- **Verfügbarkeit:** Die Verfügbarkeit der VPN-Infrastruktur hängt klar von dem zentralen Schlüssel-Server und seinen Ersatz-Servern ab.
    - **Denial-of-Service (DoS) Resistenz:** Durch die einfach Identifikation dieser Komponenten und die feste Beschränkung auf 7 Ersatz-Server, welche a priori in allen IPsec Gateways mit ihren IP-Adressen eingetragen werden müssen, kann ein Angreifer vergleichsweise einfach Denial-of-Service-Angriffe mit Auswirkungen auf die gesamte Infrastruktur durchführen.
      Aus Sicht eines Angreifers könnte es ferner interessant sein die Kommunikation zwischen Schlüssel-Server und einigen IPsec Gateways zu stören. Eine logische Partitionierung des Gesamtnetzes wäre die Folge, da die entsprechenden Backup-Server nur teilweise neue kryptographische Schlüssel verteilen würden.
    - **Graceful Degradation:** Mit dem Kompromittieren einer beliebigen IPsec-Komponente im VPN kann ein Angreifer das Erreichen sämtlicher Sicherheitsziele verhindern, sodass die Graceful-Degradation-Eigenschaft in keiner Weise garantiert werden kann.
- **Zugriffskontrolle:** GET authentifiziert IPsec Gateways primär durch den initialen IKE-Austausch, der ein gültiges Zertifikat oder Passwort erfordert. Da GET einen Gruppenschlüssel vergibt, muss dieser bei Gruppenveränderungen aktuell gehalten werden:
    - **Backward Access Control:** Bei dem initialen Vorgang können auch die Schlüssel im gesamten VPN durch den Server gewechselt werden, so dass in diesem Fall eine Backward Access Control gewährleistet wird. Wie bereits erwähnt erfordert dieser Wechsel jedoch ein VPN mit wenigen Gateways oder ein Multicast-fähiges Transportnetz, da sonst die entstehende Netzwerkbelastung am Schlüssel-Server sehr groß werden kann.
    - **Forward Access Control** kann von GET, zumindest im vorgesehenen Multicast-Rekeying-Modus, überhaupt nicht realisiert werden, sodass einmal eingebundene Gateways alle zukünftigen Nachrichten entschlüsseln können. Dies bedeutet auch, dass die Integrität des VPN nicht durch Entfernen der kompromittierter IPsec Gateways wiederhergestellt werden kann.
- **Secure-By-Default:** In der GET-Implementierung sind beispielsweise der Schutz vor Replay-Angriffen und Backward-Access-Control-Mechanismen durch mehrere Kommandos explizit zu aktivieren. Ferner setzen alle Konfigurationsbeispiele Passwortauthentifikation ein, obwohl Cisco selbst einen Einsatz von Zertifikaten empfiehlt [Cisc08], so dass die Secure-By-Default Eigenschaft nicht erfüllt ist.

Durch die Verlagerung des Routings aus der IPsec-Implementierung in das Weitverkehrsnetzwerk können unter Umständen von Angreifern noch weitere Schwächen ausgenutzt werden, da Internet-Provider beispielsweise eine kryptographisch gesicherten Protokolle für das Multicast-Routing einsetzen. Diese Schwachstellen sind zwar nicht GET an sich anzulasten sind, aber sie stellen dennoch eine direkte Folge des Ansatzes dar.

Schlussfolgerungen

Insgesamt führt ein Einsatz der GET-VPN Lösung zu einer deutlichen Reduzierung der mit IPsec realisierbaren Sicherheitseigenschaften, da in unnötiger Weise Gruppenkommunikationsmechanismen auch für Unicast-Verkehr eingesetzt werden. Aufgrund der Verfügbarkeitseigenschaften und der hohen Anforderungen an die Integrität der Gateways ist der Einsatz nur in vollständig kontrollierten Umgebungen sicher möglich, sodass der Einsatz einer VPN-Lösung nur einen geringen tatsächlichen Sicherheitsgewinn bringen kann.

Der einzige funktionale Vorteil, den GET gegenüber anderen IPsec-Konfigurationsmechanismen wie Tunnel End-Point Discovery (TED) bietet, ist die Unterstützung von Multicast. Hierbei sollten vor einer Entscheidung für GET Alternativen evaluiert werden, wie beispielsweise der Einsatz von Application Layer Multicast Systemen. Insbesondere wenn Multicast-Daten nur von einer Quelle ausgehen, ist beispielsweise ein einfacher Replay-Schutz möglich. Ferner könnte beispielsweise für Unicast-Verkehr eine herkömmliche VPN-Konfiguration zum Einsatz kommen, und GET nur für Multicast-Kommunikation verwendet werden. Für große Organisationen kann auch eine Einrichtung verschiedener GET-Gruppen sinnvoll sein, so dass die Auswirkungen eines kompromittieren Gateways lokal innerhalb einer Tochterorganisation oder eines Landes bleiben.

[Bhai08] Y. Bhaiji: Network Security Technologies and Solutions, Cisco Press, 2008.

[BWHH03] M. Baugher; B. Weis; T. Hardjono; H. Harney: The Group Domain of Interpretation, RFC 3547 (Proposed Standard), 2003.

[Cisc07] Cisco Inc.: Cisco Group Encrypted Transport VPN, 2007. http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htgetvpn.pdf

[Cisc08] Cisco Inc.: Group Encrypted Transport VPN Security Analysis, 2008. http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps7180/white_paper_c11-471053.pdf

[FeSc00] N. Ferguson; B. Schneier: A Cryptographic Evaluation of IPsec, Technical Report, 2000. http://www.counterpane.com/ipsec.pdf

[HaDo03] T. Hardjono; L. Dondeti: Multicast and Group Security, Artech House, 2003.

[Scha03] G. Schaefer: Netzsicherheit Algorithmische Grundlagen und Protokolle, dpunkt.verlag, 2003.

[WwRo07] B. Weis; S. Rowles: Updates to the Group Domain of Interpretation (GDOI), Expired Internet Draft, 2007.