

Weshalb VPNs mit Preshared Keys nicht sicher sind

Autor: Dr. Andreas Anton Bloom, Product Marketing Manager

Version 1.1 vom 21. Januar 2004

Copyright © 2004 BinTec Access Networks GmbH, alle Rechte vorbehalten

Weshalb VPNs mit Preshared Keys nicht sicher sind	1
1 VPNs gewinnen immer grössere Bedeutung	2
2 VPNs benötigen Verschlüsselung	3
3 Was ist IPSec?	3
4 Die Kette bricht stets am schwächsten Glied	4
4.1 Preshared Keys und Zertifikate	4
4.2 Gefahren von Preshared Keys in der Praxis	5
5 Preshared Keys können geknackt werden!	6
6 Wie kann man sich schützen?	7

1 VPNs gewinnen immer grössere Bedeutung

So genannte Virtuelle Private Netzwerke (VPNs) zur sicheren Datenübertragung über das Internet kommen immer häufiger zum Einsatz. Neue Vernetzungen von Standorten oder Filialanbindungen werden heute in der Regel nicht mehr über traditionelle Festverbindungen, sondern auf Basis von VPNs realisiert. Darüber hinaus werden auch bestehende Festverbindungen zunehmend durch VPNs ersetzt. Hierbei wählen sich die Zugangsgeräte – sogenannte VPN Gateways – in das Internet ein und nutzen die bereits bestehende, weltweit verfügbare Infrastruktur.

Die Gründe für diesen deutlichen Trend liegen auf der Hand: In Zeiten knapper IT Budgets bietet sich hier eine Möglichkeit, den Anforderungen der Benutzer und Applikationen nach immer mehr Bandbreite gerecht zu werden und dabei gleichzeitig noch die Kosten spürbar zu reduzieren. So schlägt eine Festverbindung mit einer Bandbreite von 256 kBit/s auf einer Distanz von nur 30 km^[1] mit ca. 19.000 Euro pro Jahr zu Buche. Ein VPN hingegen bietet Datendurchsatzraten von 2,3 MBit/s – also fast der neunfachen Bandbreite – und kostet je nach Anbieter und Ausstattung (z. B. ISDN Backup) auf der gleichen Strecke nicht mal die Hälfte. Verdoppelt man die Distanz zwischen den Standorten, erhöhen sich die Kosten für eine traditionelle Festverbindung dementsprechend. Die Kosten für ein VPN jedoch bleiben gleich, da lediglich für die Einwahl beim nächsten „Point of Presence“ (POP) des Providers bezahlt wird. Wie groß die Distanz zwischen den beiden Standorten ist, spielt dabei keine Rolle. Die initialen Kosten für neue Geräte, Schulung der Mitarbeiter oder allgemeine Migrationskosten haben sich nach spätestens zwölf Monaten amortisiert.

2 VPNs benötigen Verschlüsselung

Die Vorteile von VPNs sind offensichtlich, die potenziellen Nachteile allerdings auch: Während Festverbindungen als sicher und zuverlässig gelten, da sie lediglich die eigenen Daten transportieren, teilt man sich bei einem VPN die Leitung im Internet mit Millionen anderen Nutzern. Und nicht alle Nutzer haben hehre Absichten.

^[1] Als Beispiel wurde die Strecke Dortmund – Hagen genommen.

Abgefangene, mitgelesene oder gar veränderte Daten stellen für jedes Unternehmen ein Sicherheitsrisiko dar.

Aus diesem Grunde werden die Daten, die über ein VPN verschickt werden, in der Regel verschlüsselt. Aus der Vielzahl möglicher Verschlüsselungsverfahren hat sich in den neunziger Jahren das Point to Point Tunneling Verfahren (PPTP) durchgesetzt, vor allem auch deshalb, weil es alle gebräuchlichen Windows-Versionen unterstützt. Es ist somit nahezu überall verfügbar und leicht zu administrieren.

Sicherheitslücken im Verfahren führten dennoch zur Ablösung des Verfahrens durch neuere Verfahren wie beispielsweise IPSec (Internet Protocol Security). Das Verfahren gilt als sicherer, da es auf einem ausgefeilteren Schlüsselmanagement beruht. Darüber hinaus ist seine Architektur flexibler und ermöglicht schnellere Reaktionen auf neue Angriffstaktiken der Hacker.

3 Was ist IPSec?

Als IPSec wird eine Vielzahl von Verfahren beschrieben, die sichere und verschlüsselte Datenkommunikation über öffentliche Netze wie das Internet erlauben. Diese Verfahren sind in einer Vielzahl von RFCs (Request for Comment) beschrieben – das erste stammt aus dem Jahr 1995 von R. Atkinson – und werden immer wieder erweitert sowie den Marktbedürfnissen angepasst. Dadurch bietet IPSec nicht nur ein hohes Maß an Sicherheit, sondern weist auch eine sehr hohe Praxisrelevanz auf.

Ursprünglich wurde das Verfahren für die Kommunikation zwischen Datennetzen mit festen IP-Adressen entwickelt (RFC 1825 vom August 1995). Das Verfahren wurde in den USA entwickelt, wo statische, also feste, IP-Adressen die Regel sind. IPSec arbeitete im so genannten Main Mode. Dabei bildeten die IP-Adressen einen wichtigen Teil der Identifikation und der Verschlüsselung. In der Praxis stellte sich jedoch heraus, dass feste IP-Adressen nicht immer vorhanden sind. Dies trifft beispielsweise auf mobile Mitarbeiter zu, die sich von unterwegs aus ins Internet

einwählen oder aber auch auf Home Offices oder kleinere Standorte, die aus Kostengründen mit einer dynamischen IP-Adresse ausgestattet sind. Dies ist in Deutschland die Regel.

Für die Kommunikation, in der zumindest einer der Partner keine feste IP-Adresse besitzt, wurde das Verfahren Aggressive Mode entwickelt. Während beim Main Mode im Verbindungsaufbau sechs Nachrichten ausgetauscht werden, reduziert sich diese Zahl im Aggressive Mode auf drei. Diese Nachrichten etablieren die Kommunikation durch Authentisierung der Gesprächspartner und durch Einigung auf eine Verschlüsselungsmethode. Diese Verschlüsselungsmethoden werden dem jeweiligen Stand der Technik angepasst. So galt das Verfahren DES (Data Encryption Standard) mit einer 56 Bit Verschlüsselung vor Jahren noch als sicher. Mittlerweile ist eine dreimal so lange Verschlüsselung Standard (3DES mit 168 Bit Verschlüsselung). Aktuellste VPN Geräte unterstützen bereits den Standard von morgen (AES = Advanced Encryption Standard) mit bis zu 256 Bit Verschlüsselung. Die Verschlüsselungsverfahren im IPSec können somit als sicher bezeichnet werden – sie halten mit der Entwicklung der Hackertechniken mühelos Schritt: Im Wettlauf zwischen Hackern und Kryptologen haben Letztere mit IPSec die Nase vorn.

4 Die Kette bricht stets am schwächsten Glied

Die Schwachstelle im IPSec sind viel weniger die Verschlüsselungsmethoden und die Schlüssellängen, als vielmehr die Schlüssel selbst: Die stärkste Verschlüsselung kann nichts ausrichten, kennt der Angreifer den passenden Schlüssel.

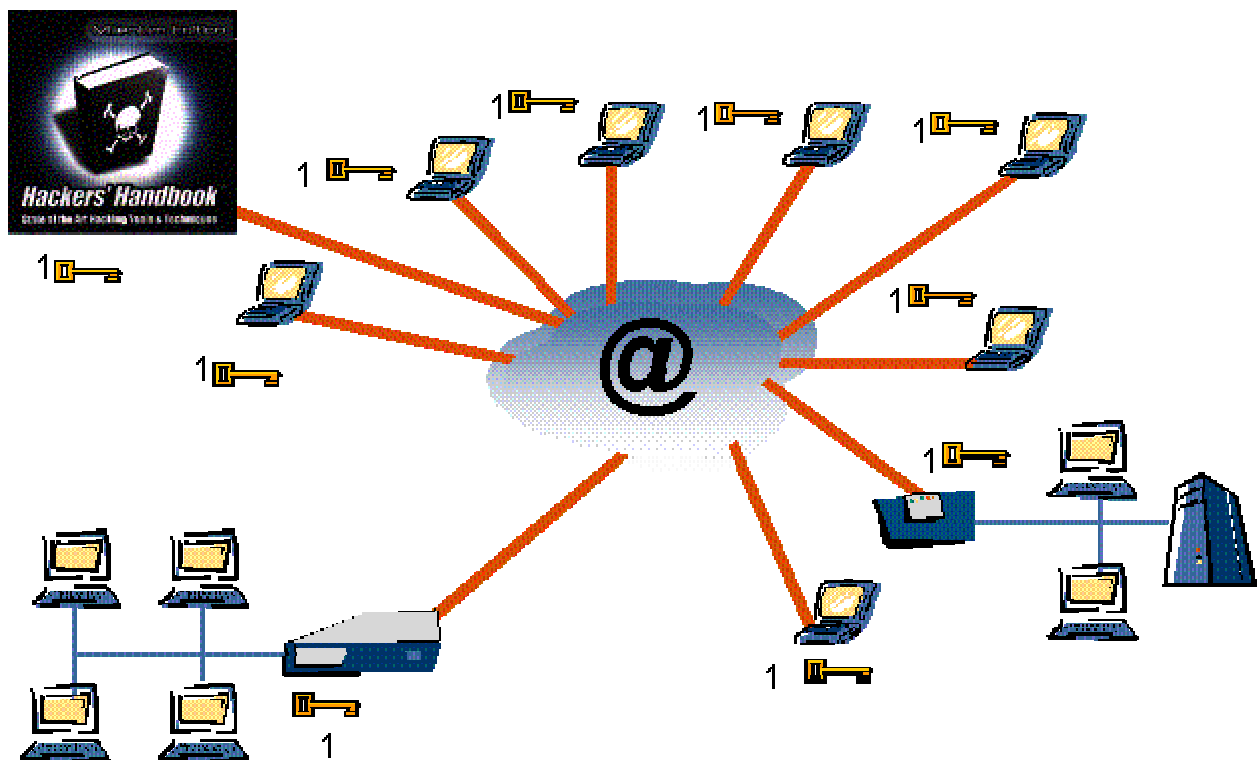
4.1 Preshared Keys und Zertifikate

Im IPSec unterscheidet man grundsätzlich zwei Arten von Schlüsseln: Preshared Keys und Zertifikate.

Während Zertifikate als sicher gelten, können Preshared Keys eine Schwachstelle darstellen und Angreifern unter Umständen Zugang zu geschützten Daten ermöglichen.

4.2 Gefahren von Preshared Keys in der Praxis

Preshared Keys sind im Grunde nichts anderes als Passwörter, die beiden Kommunikationspartnern für die Ver- und Entschlüsselung bekannt sein müssen. Sie sind vor der Kommunikation bekannt (Preshared) und müssen auf beiden Seiten übereinstimmen. Diese Passwörter werden in die Geräte eingetragen. Aus Sicherheitsgründen sollte jede Verbindung mit eigenen Passwörtern abgesichert sein. Da dies jedoch umständlich und häufig auch fehleranfällig ist, arbeiten viele VPNs sogar im Falle von mehreren Standorten nur mit einem einzigen Schlüssel. Dies erleichtert die Administration ungemein, und nicht selten behält ein einmal eingetragener Preshared Key seine Gültigkeit über Jahre hinweg, da Änderungen an allen Standorten manuell vorgenommen werden müssten.



Wird nun aber bei einem VPN-Szenario mit Preshared Keys und etwa fünfzig Außenstellen sowie Außendienstmitarbeitern ein Endgerät gestohlen (z. B. das Notebook aus Hotel, Zug oder Auto), so ist eine sichere Datenkommunikation keinesfalls mehr gewährleistet. Um diese wieder herzustellen, müsste in allen fünfzig

Standorten der Preshared Key manuell ersetzt werden – mit erheblichem logistischen und personellen Aufwand. Das gleiche gilt selbstverständlich auch für die Notebooks der Außendienstmitarbeiter: Solange der Preshared Key nicht manuell geändert wurde, ist die Kommunikation über das VPN nicht mehr sicher. Die sichere Übertragung unternehmenskritischer Daten ist nicht mehr möglich und das Unternehmen verliert bares Geld. Das VPN erfüllt seinen Zweck nicht mehr.

Noch gravierender ist es, wenn die Entschlüsselung des Preshared Key seitens der Verantwortlichen unbemerkt bleibt und die gesamte Unternehmenskommunikation über Monate oder Jahre hinweg abgehört wird.

5 Preshared Keys können geknackt werden

Um an den Preshared Key zu gelangen, muss unter Umständen ein Endgerät gar nicht erst entwendet werden.

Im IPSec unterscheidet man wie bereits oben erwähnt zwischen Main Mode und Aggressive Mode. Während der Main Mode die IP-Adresse als einen Teil der Verschlüsselungsverfahren heranzieht, gilt dies im Aggressive Mode nicht. Diese Tatsache bildet die Voraussetzung für einen erfolgreichen Hackerangriff auf ein VPN mit Preshared Keys.

Heutige VPN Gateways unterstützen beide Verfahren. Wählt sich nun ein Außendienstmitarbeiter bzw. das Gateway mit einer dynamischen IP-Adressen in ein anderes VPN Gateway ein, so schlägt es das Aggressive Mode-Verfahren vor, da die dynamische IP-Adresse dem zentralen Gateway nicht bekannt sein kann und damit auch nicht Grundlage der Authentifizierung sein darf. Da im Aggressive Mode nur drei Botschaften ausgetauscht werden, enthält die erste Botschaft die Aufforderung, im Aggressive Mode zu arbeiten. Darüber hinaus werden fast alle notwendigen Parameter übergeben, um eine sinnvolle Kommunikation zu ermöglichen.

Als Antwort erhält das externe VPN Gerät vom zentralen Gateway eine ausführliche Botschaft – die einzige, die das zentrale Gateway zum Aufbau der Verbindung

sendet. Unter anderem enthält diese Nachricht einen Wert, der aus dem Preshared Key berechnet wurde. Dieser wird unverschlüsselt übertragen. Da der Preshared Key des externen Gateways nicht mit dem des zentralen Gateways übereinstimmt, kommt keine Kommunikation zu Stande. Der Angreifer hat sein Ziel verfehlt und IPsec die Sicherheit des VPNs unter Beweis gestellt. Der Administrator erkennt in seinen Analyse-Tools, dass ein Verbindungsaufbau abgelehnt wurde.

Doch der Schein trügt: Denn der Hacker hatte nicht die Absicht, mit dieser ersten Kontaktaufnahme die Kommunikation zu etablieren. Ihm ging es um den Hash-Wert, den das zentrale Gateway aus dem Preshared Key errechnet und dann unverschlüsselt übertragen hat. Der Wert wurde mit Hilfe von Tools wie Windump (Version 3.6.2) oder tcpdump mitgeschnitten. In einem zweiten Schritt versucht der Hacker nun, mit Hilfe von Hacker Tools (z. B. IKECrack, erhältlich unter <http://ikecrack.sourceforge.net>), den Preshared Key offline zu ermitteln. Gelingt ihm dies, gelangt er gewissermaßen offiziell über die Vordertür in das Unternehmensnetzwerk und hat Zugriff auf alle Daten des Unternehmens.

Ob ihm dies tatsächlich gelingt, hängt hierbei stark von der Beschaffenheit des Preshared Keys ab. Sehr lange und komplexe Preshared Keys stellen eine wesentlich höhere Hürde dar als simple Ziffernfolgen. Da allerdings einfache Tools zum Knacken der Passworte überall erhältlich sind (und diese auch noch auf mehreren Rechnern gleichzeitig am selben Key arbeiten können), ist die Gefahr nicht von der Hand zu weisen. Beschrieben wurde diese theoretische Möglichkeit erstmals im Oktober 1999 (<http://www.securityfocus.com/bid/7423/info/>). Und dass sie tatsächlich funktioniert, wurde seitdem Dutzende Male unter Beweis gestellt.

6 Wie kann man sich schützen?

Wie bereits oben erwähnt, funktioniert der Angriff nur in der Kombination Aggressive Mode und Preshared Keys. Häufig lässt sich der Aggressive Mode gar nicht vermeiden, da Filialen oder Außendienstmitarbeiter mit dynamischen IP-Adressen arbeiten.

Um jedoch wirklich sicher zu sein, sollten VPNs Stand heute mit Zertifikaten arbeiten. Dies ist zwar initial etwas aufwändiger und verlangt dem Administrator ein höheres Know how ab, bietet aber die notwendige Sicherheit. Bei einem VPN auf Basis von Zertifikaten besitzt jeder Kommunikationspartner sein jeweils eigenes Zertifikat und ist damit eindeutig identifiziert. Die Zertifikate haben nur eine bestimmte Gültigkeit und lassen sich an zentraler Stelle sperren, sollte doch einmal ein Notebook abhanden kommen. Die übrigen Bereiche innerhalb des VPNs können ungehindert weiter arbeiten.

Bis heute ist weder eine theoretische noch gar praktische Arbeit bekannt, die einen erfolgreichen Angriff auf ein zertifikatsbasiertes VPN beschreibt.

Ist man dennoch nicht gewillt oder in der Lage, sein VPN auf Zertifikate umzustellen (z. B. weil an der falschen Stelle gespart wurde und die installierten VPN Gateways keine Zertifikate beherrschen), oder aber ist der Umstieg auf Zertifikate erst für die Zukunft geplant, sollte man unbedingt die folgenden Vorsichtsmassnahmen beachten:

- -Der Preshared Key sollte für jede Verbindung ein anderer sein.
- - Man sollte VPN Geräte wählen, die lange Preshared Keys zulassen (z. B. mit bis zu 255 Zeichen).
- - Der Preshared Key sollte komplex sein, viele Zeichen umfassen und am besten durch einen Zufallsgenerator erstellt werden.
- - Der Preshared Key sollte mit Hilfe der gängigen Hackertools überprüft werden – und dabei der Überprüfung standhalten.