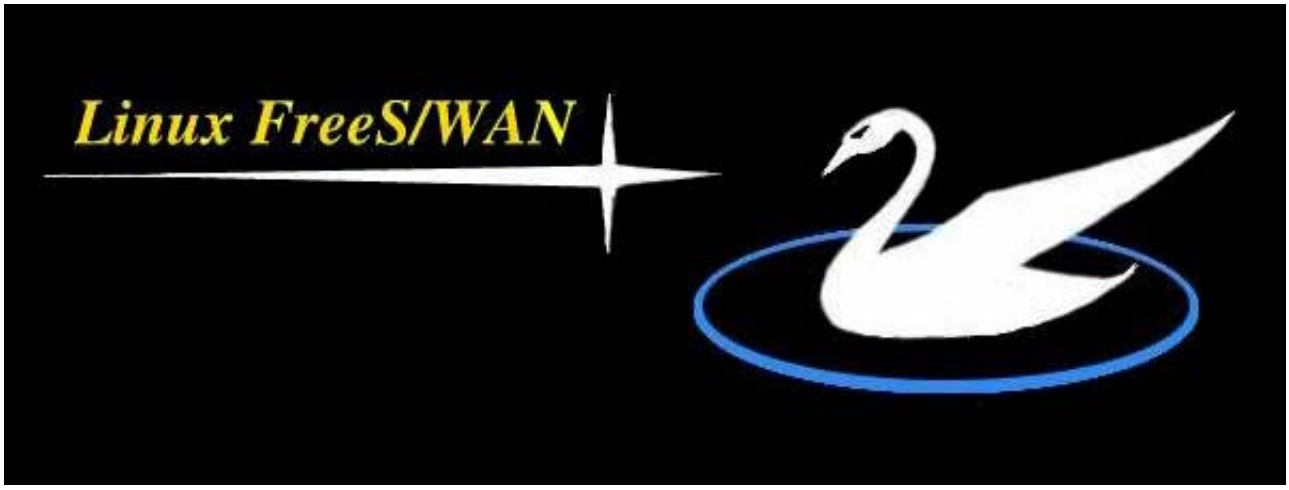
IPsec als Beispiel für symetrische und asymetrische Verschlüsslungsverfahren



Referat im Fach
Management von Informationssicherheit
am 9. Januar 2003

Referent:
Gerald Able, I7W

Gliederung:

1. Einführung eines Virtual Private Networks

Das zweite Praktikumssemester verbrachte ich bei der Firma OneVision Software AG in Regensburg. OneVision erstellt Software für die Druckvorstufe und konnte mit einigen Produkten die Position als Marktführer erreichen. Während die Programme in Regensburg und Hannover entwickelt werden, werden sie weltweit über mehrere Vertriebsniederlassungen und Tochterfirmen vertrieben.

1.1. Beweggründe für die Einführung

Zu Beginn meines Praktikums war die Kommunikation zwischen den Fillialen sehr schwierig und teilweise chaotisch. So wurde z. B. das firmenweite Intranet in Regensburg entwickelt und per CD auf dem Postweg in die Aussenstellen versandt. Abhilfe sollte ein Virtual Private Network (VPN) bieten. Das VPN würde die Aussenstellen über die ohnehin schon vorhandenen Internetleitungen permanent verbinden. Dabei kommen Leitungen unterschiedlicher Qualität von 1-Kanal-ISDN mit 64 kb/s bis X.25-Standleitungen mit 2 Mb/s zum Einsatz.

1.2. Anforderungen an die Lösung

Wichtig war die Auswahl der optimalen Lösung für die Firma. Als entscheidende Kriterien kristallisierten sich folgende Punkte heraus:

- absolute Diskretion über Art und Inhalt der übertragenen Daten

Da über das VPN auch geschäftskritische, vertrauliche Daten wie z. B. Quellcode verschickt werden sollte, war es entscheidend diese vor dem Abhören zu schützen.Auch ein unbemerktes Verändern der Daten wäre fatal.

- Verlässlichkeit der neu zu schaffenden Infrastruktur

Es war abzusehen, dass das neue VPN viele Dienste massgeblich unterstützen würde. Ein zuverlässiges Funktionieren der Lösung war unabdingbar, da viele Geschäftsprozesse darauf basieren sollten. Denial-of-Service (DoS) Angriffe gegen das VPN sollten nur schwer möglich sein.

- geringer Overhead bei der Übertragung

Die Fillialen werden von ihren Internet Service Providern teilweise volumenbasiert abgerechnet. So sollte die Einführung eines VPN den Traffic möglichst wenig erhöhen, um laufende Kosten zu sparen.

- gute Wartbarkeit und Einfachkeit für die Mitarbeiter

Die Wartung der Lösung sollte zentral in Regensburg erfolgen. Dabei sollte dem Personal in der IT-Abteilung eine einfache Administrationsumgebung für das VPN zur Hand gestellt werden. Die anderen Mitarbeiter des Unternehmens sollten die Vorteile des VPN nach vorheriger Klärung der Umstände mit der IT-Abteilung nutzen und davon ohne große Einarbeitungszeit provitieren können.

- Flexibilität und Erweiterbarkeit

Da zum Zeitpunkt der Einführung die Anwendungsmöglichkeiten noch unabsehbar waren, war es wichtig eine flexible Lösung zu finden, die später um weitere Möglichkeiten erweitert werden konnte. Relativ bald war z. B. die Notwendigkeit der Anbindung von sog.

Road Warriors. Das sind Kundenberater mit Firmen-Laptops unter Windows in (potentiell unsicheren) Netzwerken der Kunden oder mit Modemverbindungen.

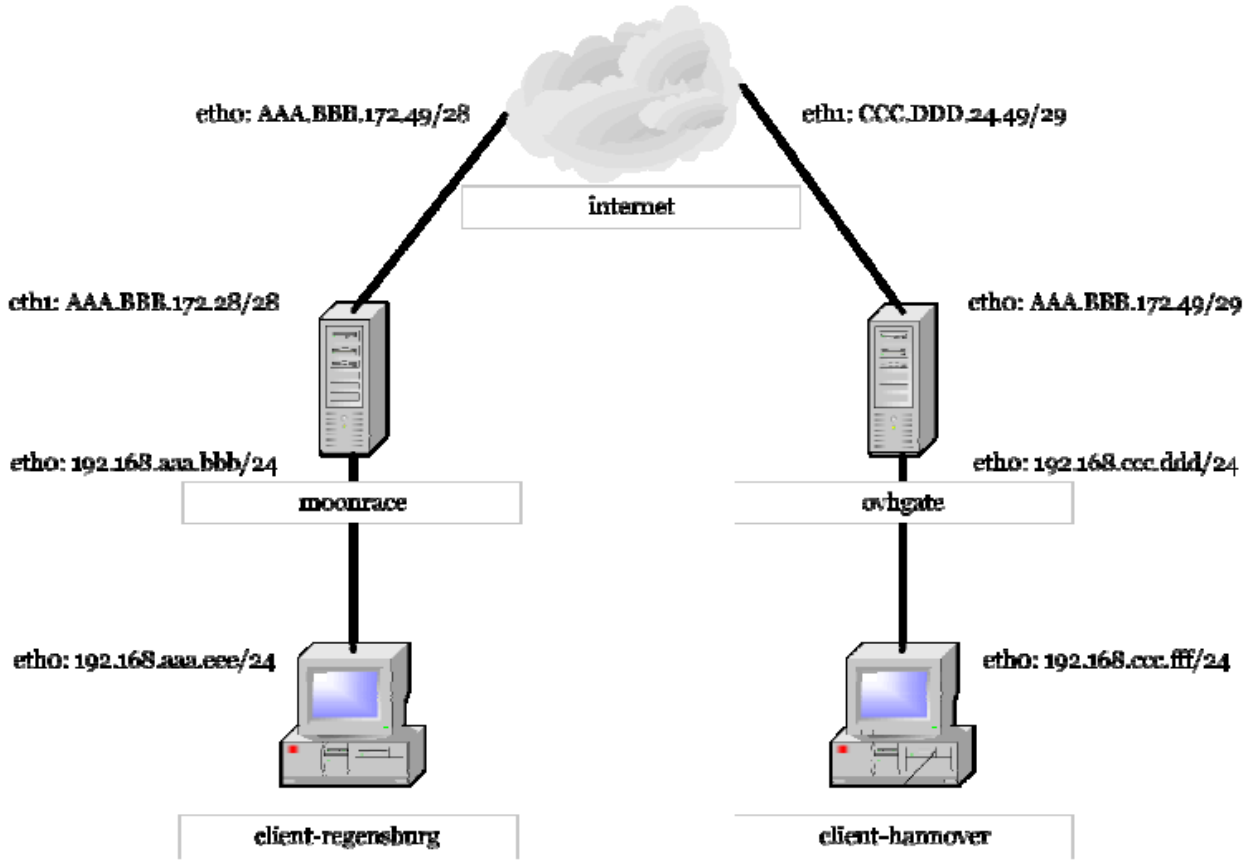
1.3. Alternativen und Entscheidung für eine Lösung

In Frage kamen nur Lösungen die entweder auf IPsec oder dem Layer-2-Tunneling-Protocol (L2TP) basierten. Letzteres tauchte in dieser Zeit öfters in den Schlagzeilen auf, weil die L2TP-Implementierung von Microsoft mehrmals gebrochen wurde und damit die auf L2TP-VPNs übertragenen Daten leicht kompromittiert werden konnten. Obwohl auch UNIX-Implementierungen des Protokolls verfügbar waren entschied man sich für IPsec, auch weil IPsec ein verpflichtender Bestandteil von IPv6 wird und damit die Zukunft des Protokolls langfristig gesichert ist. Zudem war aufgrund der Verschlüsslungstechniken sichergestellt, dass die Sicherheit gewährleistet war. Optionale Komprimierungsalgorithmen sorgen für eine Minimierung der zu übertragenden Datenmenge.

Des weiteren stellte sich die Frage, ob es sinnvoll sei ein Komplettpaket aus Hard- und Software (eine sog. "Appliance") zu kaufen oder das VPN selbst zu implementieren. Letzteres versprach eine größere Flexibilität in der Umsetzung und war zudem um ein Vielfaches billiger. So entschied man sich das Open Source Produkt FreeS/WAN auf den SuSE Linux Gateways der Fillialen und in Regensburg zu installieren.

2. technische Abläufe bei IPsec

Zentrale Elemente bei der Umsetzung sind die Gateway-Rechner der Fillialen und der Regensburger Hauptstelle des Unternehmens. Auf ihnen war eigentlich nur die Paketfilter-Firewall iptables bzw. ipchains installiert, die zudem das notwendige Masquerading und Network Adress Translation (NAT) für das dahinterliegende LAN bewerkstelligte. Nun wurde, nachdem die Umsetzung zuvor umfassend in einem vom Internet getrennten Testnetz (siehe Grafik) evaluiert wurde, zusätzlich FreeS/WAN installiert und konfiguriert. Auch die Firewall-Regeln mussten angepasst werden, um der neuen Sicherheitslage zu genügen.



2.1. Schlüsselaustausch über asymetische Verfahren

Um den Rechenaufwand bei der Kommunikation zwischen zwei IPsec Endpunkten gering zu halten wird folgendes Verfahren angewendet:

Zuerst werden in einem (rechenintensiven) asymetrischen Verfahren Verbindungsparameter und Grundlagen für eine spätere symetrische Verschlüsslung ausgehandelt. Das sog. ISAKMP Protokoll sorgt hierbei für eine Authentifizierung der Kommunikationspartner, die sich mit Pre-Shared-Keys nach dem RSA-Standard, digitalen Signaturen oder wie bei OneVision mit X.509-Zertifikaten ausweisen müssen. Die entstehende logische Verbindung hat bidirektionalen Charakter und wird als ISAKMP SA (Security Association) bezeichnet. Sie verwendet als kryptographisches Verfahren Triple-DES und kann über Tage bestehen bleiben. Auch andere Algorithmen sind möglich, abhängig von der Standardkonformität der Implementierung. So haben sich die FreeS/WAN-Entwickler beispielsweise entschieden Single-DES nicht zu unterstützen, weil es schon gebrochen wurde und damit nur eine Pseudosicherheit verspricht.

In der zweiten Phase des ISAKMP Protokolls wird ein Sitzungsschlüssel ausgehandelt, mit dem die IPsec SA aufgebaut wird.

2.2. Verschlüsslung der Nutzdaten über symetrische Schlüssel

Die IPsec SA gilt nur für eine Richtung, d. h. für einen funktionierenden Informationsfluss müssen zwei IPsec SAs ausgehandelt werden. Die symetrische Verschlüsslung mit dem Sitzungsschlüssel benötigt wesentlich weniger Rechenleistung und wird aus Sicherheitsgründen periodisch neu verhandelt und eingerichtet.

Im Testnetz wurde der Traffic mit Sicherheitstools wie tcpdump und ethereal abgehört. Dabei konnte kein Zusammenhang zwischen übertragenen und beobachteten Daten beobachtet werden. Zu sehen waren nur IPsec-Pakete. Das sind IP Pakete, die Huckepack ein ESP (Encapsulated Security Payload)-Paket tragen. In diesem sind ein 32 Bit langer Index und eine eben so lange Sequenznummer und Authentifizierungsdaten zu finden. Natürlich enthält ein ESP-Paket auch die verschlüsselten Nutzdaten und ebenfalls verschlüsselt den Datentyp der Nutzdaten.

Als nettes Zusatzfeature ist es möglich zwischen IPsec Endpunkten unter Linux und *BSD die Nutzdaten transparent zu komprimieren. Die IPsec Implementierung von Windows 2000 unterstützt diese Möglichkeit leider nicht. Der Kommunikationsoverhead betrug ca. 60 %, was zwar höher lag als erwartet, aber sich mit der Implementierung aktueller Kompressionsalgorithmen in Zukunft verbessern wird. Die Geschwindigkeitsobergrenze im Testnetz betrug, abhängig von der verwendeten MTU bis zu 5 Mb/s. Begrenzender Faktor war offensichtlich ein veralteter Rechner (Pentium-166). Doch auch diese Geschwindigkeit hätte die Anforderungen in dieser Hinsicht schon übererfüllt.

3. Erweiterungen und Ausblick

Als die Lösung im Testnetz erfolgreich angetestet wurde, wurden weitere Gegebenheiten bekannt, die in das VPN eingepflegt werden sollten.

3.1. Einbindung von Road Warriors

Nachdem in der ersten Phase der Umsetzung noch auf ausgehandelte RSA-Schlüssel gebaut wurde, stellte sich schnell heraus, dass für eine Integration von Windows-Laptops die Verwendung von X.509-Zertifikaten unerlässlich ist. So musste eine firmeneigene einfache Public Key Infrastructure (PKI) aufgebaut werden. Ein dedizierter Rechner wurde als Certificate Authority (CA) auserkoren und sehr restriktiv abgesichert. Mittels einer Open Source Lösung (VPN Package) konnten Windows 2000 Rechner ähnlich FreeS/WAN konfiguriert werden. Eine Klickorgie, wie Microsoft sie für die Konfiguration vorsieht konnte so vermieden werden. Auch die Anbindung von Windows-Rechnern, die sich per Modem über einen seperaten ISP einwählten konnte erfolgreich getestet und umgesetzt werden.

3.2. auf das VPN aufsetzende Lösungen

Mit dem realisierten VPN konnten viele Abläufe im Unternehmen verbessert werden. Die Codeentwicklung funktioniert wegen der direkten Verfügbarkeit aller Quellen nun reibungslos zwischen den Standorten. Anwendern im Ausland, die auf Probleme mit der Bedienung der Rechner stossen kann direkt geholfen werden, indem ihre Windows-Rechner über das VPN und die Fernadministrationssoftware TightVNC ferngesteuert werden.
Erste Tests für die teilweise Umstellung des Telefonverkehrs auf Voice over IP sind bereits mit durchaus befriedigenden Ergebnissen erfolgt. Verwaltungsinformationen im Unternehmen sind nun zentral in Regensburg verfügbar. Es ist angedacht auch die Authorisierung für alle Dienste zentral zu steuern und somit eine Single Sign On-Lösung zu schaffen.

3.3. Probleme bei der Umsetzung und Fazit

Da die Materie für mich und meinen Praktikumsbetreuer relativ neu war, hatten wir anfangs mit Verständnisschwierigkeiten zu kämpfen. Als diese beseitigt waren und die ersten Versuche im Testnetz problemlos verliefen war die Zeit bis zum Einsatz im Produktionssystem erstaunlich kurz. Das VPN hat sich als verlässliche Hilfe im Arbeitsleben der Firma etabliert. Zudem konnte ich bei der Realisierung mein Wissen über UNIX, Netzwerktechnik und Kryptographie stark erweitern.

4. Literaturangaben

Andreas Pinkert, Interoperabilität von IPSecure Implementierungen:
http://www.tu-ilmenau.de/~pinkert/IPSec.pdf

Gerald Able, Praktikumsbericht OneVision Software AG:
http://gerald-able.de/common/studies/ps2/report_ps2.pdf

diverse RFCs zum Themenkomplex IPsec:
http://www.antioffline.com/ipsec/rfc/