Zeitschrift: Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association suisse des électriciens, de l'Association des entreprises électriques suisses

Herausgeber: Schweizerischer Elektrotechnischer Verein ; Verband Schweizerischer Elektrizitätsunternehmen

Band: 87 (1996)

Heft: 3

Artikel: Sicherheitsaspekte im Internet : Firewalls, Packet Filter und IPv6

Autor: Lubich, Hannes P.

DOI: https://doi.org/10.5169/seals-902297

Obwohl das Internet als rein akademischer Netzverbund konzipiert wurde, hat es sich inzwischen zu einer Informationsquelle entwickelt, die auch für kommerzielle Zwecke von Interesse ist. Eine wachsende Zahl von Firmen betrachtet das Internet als wichtiges zukünftiges Geschäfts- und Werbeinstrument und versucht derzeit, die Möglichkeiten, aber auch die Grenzen des Internet kennenzulernen. Es bestehen jedoch unterschiedliche Sicherheitsbedürfnisse für die verschiedenen Anwender und Anwendungen, für die entsprechend skalierbare Schutzmechanismen bereitgestellt werden müssen. Da die meisten dieser Mechanismen schlecht in die Basis-Protokollarchitektur des Internet integriert sind, werden derzeit im Rahmen einer Neufassung der Internet-Protokolle auch Sicherheitsdienstelemente diskutiert. Im Rahmen dieses Beitrages sollen Stand und Trends im Bereich Sicherheit im Internet aufgezeigt werden.

Sicherheitsaspekte im Internet

Firewalls, Packet Filter und IPv6

■ Hannes P. Lubich

Sicherheitsaspekte beim Aufbau des Internet

In der heute allgemein verbreiteten Architektur des Internet wurde von der Annahme ausgegangen, dass «Sicherheit», das heisst das Verhindern des Mitlesens bzw. die Unverfälschbarkeit der übertragenen Benutzer- und Verwaltungsinformation sowie sicherheitsbezogene Funktionalität wie zum Beispiel der Beweis des Erhalts oder des Absendens einer Mitteilung, in einem reinen Forschungsnetz auf absehbare Zeit nicht benötigt werden würden. Demzufolge wurde beim Entwurf der Internet-Protokolle und -Anwendungen dieser Aspekt nicht berücksichtigt.

Bezüglich der Design-Kriterien für ein Datennetz, wie sie in Bild 1 gezeigt werden, muss das Internet also als System mit sehr guter Verfügbarkeit, das aber die Kriterien Integrität und Vertraulichkeit wenig beachtet, klassifiziert werden. Es wäre aber bei Betrachtung der ursprünglichen Anforderungen verfehlt, den ursprünglichen Erbauern und heutigen Betreibern den Vorwurf zu machen, ein nicht brauchbares Netz zu propagieren. Aufgrund des zunehmenden Gebrauchs des Internet für geschäftliche Zwecke sind jedoch in zunehmendem Masse Meldungen in der Presse zu finden, die sich auf Einbrüche in fremde Rechner, das Erschleichen von Leistungen über Datennetze usw. beziehen. Es ist demnach an der Zeit, das Internet bezüglich seiner Sicherheitsdienstelemente zu überarbeiten und

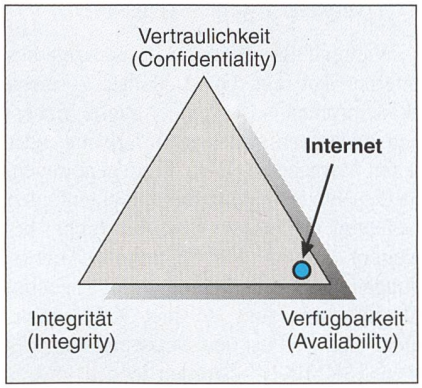

Bild 1 Das CIA-Dreieck des Netzwerkdesigns und die Position des Internet

Adresse des Autors:
PD Dr. *Hannes P. Lubich*, Switch-Geschäftsstelle, Limmatquai 138, 8001 Zürich.

zu modernisieren, wozu jedoch zunächst einmal Klarheit über die vorhandenen und demzufolge zu behebenden Mängel geschaffen werden muss. Aus heutiger Sicht umfasst die «Mängelliste» des Internet und seiner Anwendungen die folgenden Punkte:

- Die Basisdateneinheit des Internet, das heisst ein IP-Paket, ist in keiner Weise gegen Mitlesen, Verfälschung, Duplizierung usw. geschützt, die einfache Prüfsumme kann von entsprechend geschulten und ausgerüsteten Angreifern leicht neu berechnet werden.
- Die für den Betrieb des Internet lebenswichtigen Routing-Protokolle, mit deren Hilfe Router untereinander Erreichbarkeitsinformation über die angeschlossenen Netze austauschen, sind gegen Eindringlinge nicht geschützt. Diese können zum Beispiel ihren eigenen Router unter Angabe falscher Information im Netz so etablieren, dass fremder Datenverkehr über den eingeschleusten Router statt über die offizielle Route verläuft.
- Die Dateneinheiten der Transportschicht (TCP- und UDP-Segmente) sind nicht bzw. nur durch eine einfache Prüfsumme gegen Verfälschung usw. geschützt.
- Die für den Betrieb des Internet benötigten Hilfsprotokolle (insbesondere ICMP, DNS, ARP, BOOTP, TFTP) sind nicht bzw. nur unzureichend geschützt, so dass eine Attacke auf ein Netz bzw. einen Rechner durch «Maskieren» (Vorspiegelung einer falschen Rechneridentität) als anderer Partnerrechner möglich ist.
- Die Anwendungsprotokolle sind entweder nicht (SMTP, SNMP-1) oder nur durch einen einfachen Benutzername/Passwort-Mechanismus geschützt, der jedoch in seinem Wert stark durch die Tatsache vermindert wird, dass Benutzername und Passwort im Klartext vom Sender- zum Empfängersystem geleitet werden, das heisst mitgelesen und wiederverwendet werden können.

Während der gesamten Lebenszeit des Internet hat ein Grossteil der – meist akademischen – Anwender diese Sicherheitslücken entweder nicht erkannt oder deren Vorhandensein in Kauf genommen, da der Nutzen des Internet die potentiellen Gefahren für diese Benutzergruppe bei weitem aufwog. Für bestimmte Anwendungen – insbesondere solche neueren Datums, wie zum Beispiel X-Windows, elektronische Post und Netzwerk-Management (SNMP-2) – wurden jedoch jeweils spezifische Sicherheitsdienstelemente zur Verfügung gestellt, die gesicherte Kommunikation aber auf Partner beschränkt, welche die gleiche Anwendung (oft sogar des gleichen Herstellers) verwendeten. Dementsprechend sind solche Applikationen derzeit noch nicht sehr weit verbreitet. Heute wird jedoch durch die zunehmende kommerzielle Nutzung des Internet sowie durch den Wunsch nach Abrechenbarkeit von bezogenen Dienstleistungen der Ruf nach einheitlichen Sicherheitsdienstelementen immer lauter.

Heutige Lösungsansätze

Solange beide Endpunkte einer Kommunikationsbeziehung kontrolliert werden können, kann bereits seit langem bewährte, kommerziell erhältliche Chiffriertechnologie eingesetzt werden, wobei die Chiffrierung auf allen Protokollschichten, von der Datensicherungs- und Netzwerkschicht bis zur Anwendungsschicht, vorgenommen werden kann. Jedoch ergibt sich immer dann ein Problem, wenn der jeweils andere, organisationsexterne Endpunkt nicht der eigenen Kontrolle untersteht (also z. B. beim Abruf von Daten aus dem «öffentlichen» Internet, bei Kommunikation mit vorher nicht bekannten Partnern usw.). In diesem Fall kann das Netzwerk nicht mehr als ein – möglicherweise ungesichertes – Verbindungsmittel zwischen zwei gesicherten Endpunkten angesehen werden. Es entsteht eine asymmetrische Situation, in der Dienste von Unbekannten (z. B. bei Benutzung des WWW-Dienstes) bezogen werden und in der ein Eindringen (über die Verbindung des eigenen Netzes oder Rechners nach aussen) in den eigenen Rechner oder das firmeninterne Netz verhindert werden muss. Der einzige Punkt, an dem die eigene Infrastruktur und Informationen geschützt werden können, ist nun der Anschlusspunkt an das Internet. Bild 2 zeigt diesen Paradigmenwechsel von symmetrischen zu asymmetrischen Netzanschlüssen.

Zum Schutze dieses Anschlusspunktes werden heute verschiedene Lösungsansätze von verschiedenen Herstellern angeboten, die in ihrer Effektivität, aber auch im damit verbundenen Installations- und Betriebsaufwand stark variieren. Es muss jedoch bereits an dieser Stelle darauf hingewiesen werden, dass keine der diskutierten Methoden als beweisbar sicher gelten kann:

- *Packet Filter,* die – meist innerhalb eines Routers implementiert – auf IP-Paket-Ebene (Netzwerkschicht) die im Kopf des IP-Paketes vorhandene Information (IP-Adressen, benutzter Anwendungsdienst, verantwortliches Transportprotokoll usw.) auswerten und anhand von vordefinierten Filterregeln Pakete abweisen oder durch den Router hindurchlassen. Die meisten Router-Hersteller bieten heute diese zusätzliche Funktionalität an, jedoch sind Syntax und Semantik der Filterregeln meist sehr komplex. Zudem ist der Administrator beim Aufsetzen der Filterregeln meist an die «Filterlogik» gebunden, die der Ersteller der Filtersoftware als sinnvoll angesehen hat. Viele Packet Filter betrachten zusätzlich auch den Paketkopf des Transportprotokolls (meist TCP oder UDP), um weitere Filteroptionen (z. B. Portnummer, d. h. gewünschter Anwendungsdienst) zu ermöglichen.
- *Network Relays,* die den Packet Filter durch einen programmierbaren Überwachungsrechner ergänzen. Dieser überwacht den Packet Filter, erlaubt ein leichteres Konfigurieren der Filterregeln, protokolliert den Betrieb des Packet Filters und alarmiert gegebenenfalls auch einen Administrator, wenn Unregelmässigkeiten im Zustand des Packet Filters erkannt werden (Bild 3). Es ist zudem möglich, einen solchen Überwachungsrechner so mit dem Packet Filter zu koppeln, dass sich Anrufer

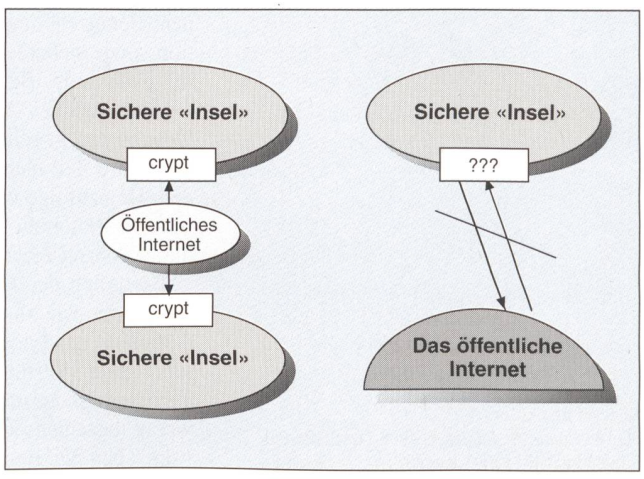

Bild 2 Paradigmenwechsel bei sicheren Netzverbunden

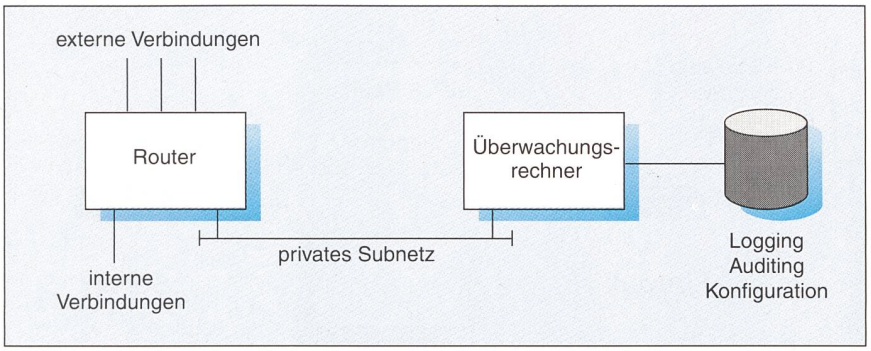

Bild 3 Aufbau eines Network Relay

zunächst beim Überwachungsrechner authentisieren müssen, bevor dieser dynamisch und zeitlich beschränkt den Packet Filter anweist, eine entsprechende Filterregel für den Anrufer in seinen Tabellen einzutragen. Der Vorteil dieser Methode liegt in der freien Programmierbarkeit des Überwachungsrechners. Entsprechende Software ist heute allerdings kaum kommerziell erhältlich, so dass diese von den Anwendern meist selbst erstellt und verwaltet wird.

– *Sichtbare Firewall-Systeme,* die nicht End-zu-End-basierte Anwendungsdienste terminieren und asynchron nach aussen/innen weiterleiten können (z. B. DNS, elektronische Post). Benutzer, welche Internet-Dienste in Anspruch nehmen wollen, müssen auf dem Firewall-System einen Benutzerbereich (mit entsprechend guter Autorisierung bei der Anmeldung) haben. Diese Methode ist relativ leicht zu implementieren, bietet jedoch sehr wenig Benutzungskomfort. So müssen zum Beispiel Anwender Daten, die sie aus dem Internet abholen wollen, zunächst auf das Firewall-System kopieren, bevor sie diese in einem zweiten Schritt auf den eigenen Rechner kopieren können. Die Verwendung von interaktiven End-zu-End-Diensten (Terminalemulation, X-Windows, WWW) wird auf diese Weise fast unmöglich und sehr unkomfortabel.

– *«Unsichtbare» Firewall-Systeme,* welche sich dynamisch und (für den Benutzer) nicht sichtbar zwischen die beiden kommunizierenden Endsysteme schalten und den Datenverkehr mit der Kenntnis und im Kontext der Anwendung überwachen können (wenn z. B. die Syntax der Passwortdatei im Anwendungskontext «Dateitransfer» oder «Terminalemulation» erkannt wird, kann die Verbindung abgebrochen werden). Diese Methode ist die eleganteste der bisher vorgestellten, fällt jedoch trotz der Verfügbarkeit entsprechender Software-Umgebungen noch immer in den Bereich der angewandten Forschung. Die existierenden Firewall-Produkte sind zudem noch zu neu, um bereits abschliessend bezüglich ihrer Qualität beurteilt zu werden, insbesondere dann, wenn sie auf einem handelsüblichen Betriebssystem mit seinen eigenen Sicherheitslücken zur Verfügung gestellt werden.

– *Schutz einzelner Anwendungen* durch End-zu-End-Verschlüsselung, Leisten digitaler Unterschriften, gesicherte Prüfsummen usw. Diese Methoden sind in verschiedenster Form (PEM und PGP für elektronische Post, Kerberos usw.) im Internet im Einsatz, skalieren sich jedoch in ihrer heutigen Form und Verfügbarkeit nicht auf den potentiell sehr grossen Nutzerkreis. Zudem werden in vielen Anwendungen parallel und meist unkoordiniert Sicherheitsdienstelemente implementiert, die ein Zusammenspiel zwischen verschiedenen Anwendungen, die Verwendung eines gemeinsamen Schlüssels usw. unmöglich machen.

Mit den beschriebenen Methoden bzw. Kombinationen davon (und unter der Annahme einer ausreichenden physikalischen Sicherheit von Netzkabeln, Rechnern usw.) kann nun bereits ein Grossteil der Attacken im Internet vermieden werden, ähnlich dem Abschliessen der Autotür auf einem öffentlichen Parkplatz. Auch das Türschloss des Autos bietet ja keinen vollkommenen Schutz vor Einbruch; es hält aber diejenigen Personen davon ab, das Auto zu stehlen, die nur probieren, ob sich die Tür öffnen lässt, und die bei Misserfolg sofort weitergehen, um nicht aufzufallen. Für das verbleibende Restrisiko basiert die Abwehrstrategie meist auf der Hoffnung, dass der Eindringling (wie beim Aufbrechen des Autos) so viel Lärm (bzw. Logging-Information) verursacht, dass der Versuch wenn schon nicht verhindert, so doch detektiert werden kann (analog zur Autoalarmanlage). Besonders im Hinblick auf die nicht zu unterschätzenden Kosten für den Aufbau und den Betrieb eines solchen Schutzmechanismus sind die meisten heute am Internet angeschlossenen Organisationen mit einer solchen oder ähnlichen Lösung zufrieden. Es muss jedoch darauf hingewiesen werden, dass in keinem Fall eine Garantie besteht, dass nicht externe Angreifer eine Kommunikationsbeziehung von oder nach aussen verhindern oder stören können (denial of service).

Sicherheit im «neuen Internet»

Im Rahmen der derzeit vorgenommenen Überarbeitung des IP-Protokolls wurde – nach der Vergrösserung des Adressraums (von jetzt 32 auf zukünftig 128 Bit) – als zweitwichtigste Anforderung der Wunsch nach Sicherheitsdienstelementen genannt, die für alle Anwendungen sowie die für den Betrieb des Internet notwendigen Protokolle (Routing usw.) nutzbar sein sollten. Demzufolge werden derzeit zwei verschiedene Sicherheitsmechanismen diskutiert, die im neuen IP-Protokoll (IP Version 6, oft auch als IPng oder SIPP bezeichnet) bereitgestellt werden sollen:

– *Authentication Header:* Dieser geplante Mechanismus basiert auf der Verwendung von Prüfsummen in Kombination mit

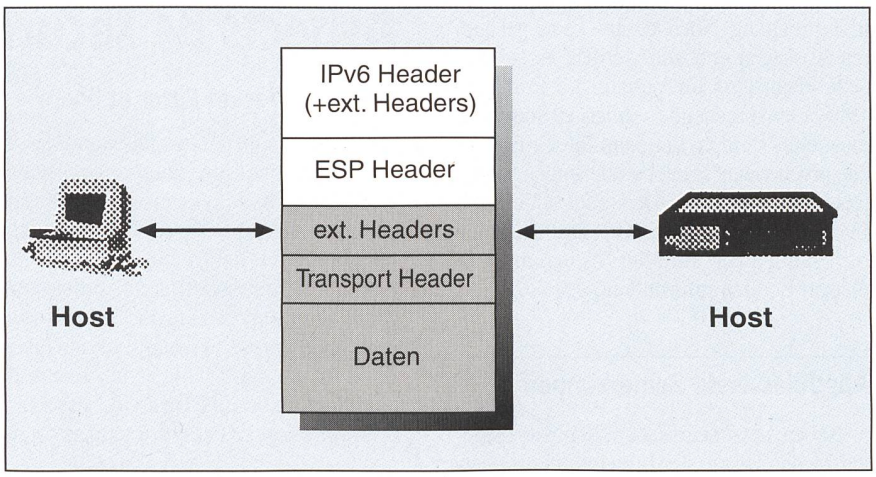

Bild 4 Transportmodus ESP

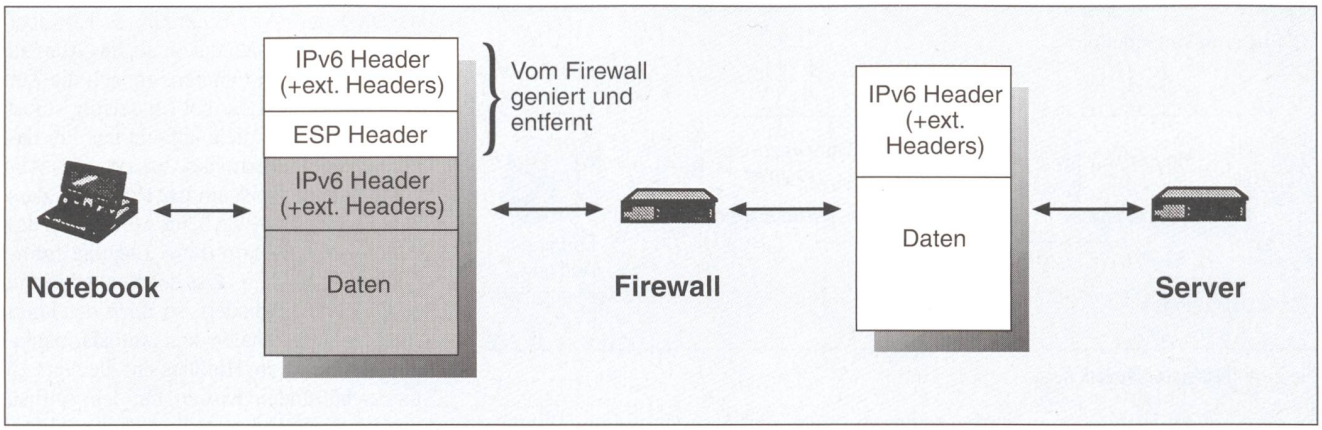

Bild 5 Tunnelmodus ESP

einem öffentlichen Chiffrierverfahren, bei dem beliebige Information vom Absender mit seinem geheimen Schlüssel chiffriert wird. Jeder Empfänger solcher Information kann dann mit dem öffentlichen Schlüssel des Senders prüfen, ob die Information intakt ist und ob sie tatsächlich vom angegebenen Absender stammt.

– *Encapsulating Security Payload (ESP):* Dieser Mechanismus soll Vertraulichkeit und Integrität der transportierten Daten sichern. Im Transportmodus (Bild 4) wird nur die Transportprotokoll-Dateneinheit verschlüsselt, während im Tunnelmodus (Bild 3) das ursprüngliche IP-Paket verschlüsselt und in einem umgebenden IP-Paket verpackt wird. Während die erste Methode «nur» den Inhalt des Paketes sichert, können mit der zweiten Methode auch der Absender und der Empfänger des Paketes verborgen werden. Die zweite Methode kann, wie in Bild 5 gezeigt, auch verwendet werden, um einen mobilen Rechner auf sichere Weise über einen Firewall mit IPv6-Software an ein Basisnetz anzuschliessen.

Die beiden beschriebenen Mechanismen und deren Details (Methode der Chiffrierung, Art der Schlüsselvergabe und -verwaltung usw.) sind derzeit im Internet in Bearbeitung. Noch können keine genaueren Aussagen gemacht werden, es ist aber abzusehen, dass im Verlauf des Frühjahrs 1996 entsprechende Internet-Standards existieren werden, die dann die Grundlage entsprechender Implementierungen durch Router- und Rechner-Hersteller bilden. Die Internet-Anbieter werden ihre Kunden rechtzeitig über allfällige Neuerungen in diesem Bereich informieren.

Abschliessende Bemerkungen

Neben den technischen Aspekten spielen in der Diskussion um Internet-Sicherheit auch einige organisatorische Elemente eine Rolle, wie zum Beispiel strafrechtliche Konsequenzen des Missbrauchs von Computern, legislative Massnahmen im Umgang mit chiffrierter Information und von Chiffrier-Soft- und -Hardware, aber auch der Aufbau einer Infrastruktur, welche die Erstellung von sicheren Kontexten in weltweiten Datennetzen überhaupt erlaubt (z. B. eine stabile, weltweite Verzeichnisdienst-Struktur zur Schlüsselverwaltung). Abschliessend ist festzuhalten, dass aufgrund der starken kommerziellen Ausrichtung des Internet der Druck wächst, allgemein verfügbare und genügend gute Sicherheitsmechanismen zur Verfügung zu stellen. Kurzfristig werden Packet Filter und Firewalls den asymmetrischen Zugangsschutz übernehmen, während mittelfristig modifizierte Netzwerkprotokolle wie IPv6 für die Basissicherheit sorgen werden. Längerfristig wird jedoch Sicherheit im Kontext des Benutzers bzw. einzelner Anwendungen wichtig werden, da sich zum Beispiel Sicherheitsanforderungen dynamisch im Lauf einer Interaktion mit einem oder mehreren Partnern ändern können. Persönliche, das heisst an die Person oder einen Rechner gebundene Sicherheitsmechanismen (Smart Cards, biometrische Technologien) werden dann eine wichtige Rolle spielen, während die eigentlichen Datennetze und Netzverbunde ihre Verarbeitungskapazität wieder stärker auf den Transport von Benutzerdaten ausrichten können.

Informationsquellen

[1] *W. Cheswick, S. Bellovin:* Firewalls and Internet Security, Addison-Wesley, 1994.
[2] *D. Curry:* UNIX System Security, Addison-Wesley, 1993.
[3] *S. Garfinkel, G. Spafford:* Practical UNIX Security, O'Reilly, 1991.
[4] *C. Kaufman, R. Perlman, M. Speciner:* Network Security, Prentice Hall, 1995.
[5] *W. Stallings:* Network and Internetwork Security, Prentice Hall, 1995.
[6] NetNews: comp.security.announce, comp.security.unix, alt.security
[7] WWW:http://www.switch.ch/switch/cert/SWITCH-CERT.html
[8] FTP: ftp://www.switch.ch/mirror/security

Aspects de sécurité dans l'Internet

Firewalls, Packet Filter et IPv6

Bien que conçu à des fins purement académiques, le réseau interconnecté Internet s'est développé entre-temps en une source d'informations pouvant aussi intéresser le commerce. Un nombre croissant de firmes considère l'Internet comme un instrument d'avenir et important pour les affaires et la publicité, et elles sondent actuellement les possibilités et limites de l'Internet. Il existe néanmoins des besoins de sécurité divergents pour les différents utilisateurs et applications, auxquels il faudra mettre à disposition des mécanismes de protection ajustables en conséquence. Comme la plupart de ces mécanismes sont mal intégrés dans l'architecture des protocoles de base de l'Internet, on discute actuellement, dans le cadre d'une refonte des protocoles de l'Internet, aussi d'éléments de services de sécurité. Dans le cadre de cet article, on présente l'état actuel et les tendances au niveau de la sécurité dans l'Internet.