

Sicher Surfen I: Das Internet

Georg Wagner

25. Mai 2001

1 Einleitung

Zum Verständnis der Sicherheitsprobleme bei der Benutzung des Internets, ist eine grundlegende Kenntnis der Technik des Internets nötig. Die verwendete Technik ist stark durch den ursprünglichen Verwendungszweck des Internets - militärische Forschung - geprägt.

1.1 Geschichtlicher Ueberblick

Nach dem Sputnik-Schock wurde die ARPA¹ als militärische Forschungseinrichtung gegründet. Diese beschäftigte sich schon früh mit der Frage der Vernetzung von Computern. Aus dieser Beschäftigung entstand der Vorläufer des heutigen Internet, das ARPANET. Folgende Ueberlegungen stehen hinter der Konzeption dieses Netzwerks:

- Was passiert wenn der zentrale Rechner eines Netzwerks bei einem feindlichen Angriff zerstört wird?
- Wie kann die sichere Zustellung von Nachrichten gewährleistet werden?

Diese Fragen wurden wie folgt beantwortet:

- Es gibt keinen zentralen Computer mehr, alle Computer im Netz sind gleichberechtigt.
- Die Nachrichten werden in einzelne Datenpakete zerlegt und suchen sich ihren Weg gewissermassen selbständig durch das Netz. Fällt auf dem Weg von einem Computer zu einem anderen einer aus, wird ein neuer Weg gesucht.

Die Umsetzung dieser Antworten in die Technik hat folgende Konsequenzen:

- Fällt einer der Computer aus, funktioniert das Netz weiterhin.

¹Advanced Research Projects Agency

- Es kann nicht vorhergesagt werden, welchen Weg ein Datenpaket im Netzwerk einschlägt.

Damals wurde davon ausgegangen, dass nur ein beschränkter Personenkreis - nämlich Militärs und militärische Forscher - an das Netz angeschlossen würden. Deshalb wurden keine Massnahmen getroffen, um die Vertraulichkeit der Nachrichten zu gewährleisten. Der Inhalt der Datenpakete geht also unverschlüsselt über das Netz. Jedes Paket ist problemlos lesbar. Das Hauptproblem beim Lesen einer Nachricht besteht im Zusammensetzen der einzelnen Datenpakete.

1.2 Der Wachstum des Internets

In der folgenden zeitlichen Uebersicht kann das Wachstum des Internets abgelesen werden:

- 1957: Der Sputnik-Schock führt zur Gründung der ARPA.
- 1969: Das ARPANET verbindet 4 Netzwerke miteinander.
- 1971: Verbund von ca. 24 Forschungs- und Regierungscomputer, dient als Werkzeug für Austausch von Forschungsdaten
- 1972: Email wird zur interessanten Anwendung im Netz.
- 1973: Erste internationale Verbindung, das ARPANET wird mit dem University College of London und der Royal Radar Establishment in Norwegen verbunden. FTP - File Transfer Protocol - zum Uebertragen von Dateien - wird entwickelt. Email macht 75% des Netzwerkverkehrs aus.
- 1975: Spezifikation des Transfer Control Protocol (TCP), heute Grundlage fast aller Datenübertragungen im Internet.
- 1978: Das Protokoll TCP wird in zwei Schichten aufgespalten: TCP und IP (TCP/IP)
- 1980: Totaler Netzausfall aufgrund eines Virus
- 1983: Mehr als 500 Computer angeschlossen. Der Name Server wird entwickelt, Benutzer des Netzes müssen nicht mehr die exakte (numerische) IP-Adresse eines Zielsystems kennen.
- 1984: Mehr als 1000 Computer angeschlossen. Einführung des Domain Name Systems DNS
- 1986: Mehr als 5000 Computer angeschlossen. Erster grösserer Sicherheitszwischenfall²

²siehe Clifford Stoll: The Cuckoo's Egg - Tracking a Spy Through the Maze of Computer Espionage

- 1987: Mehr als 10000 Computer angeschlossen.
- 1988: 88000 Computer sind am Netz angeschlossen. Der Internet-Wurm von Morris legt grosse Teile des Netzwerks lahm.
- 1989: Mehr als 100000 Computer sind angeschlossen. Das ARPANET wird zum Internet.
- 1990: 313000 Computer sind angeschlossen. Das ursprüngliche ARPANET existiert nicht mehr. Der Begriff World Wide Web (WWW) wird geprägt.
- 1991: 617000 Computer sind angeschlossen, Die ersten Browser (Vorfahren von Netscape oder Internet Explorer) werden entwickelt.
- 1992: 1136000 Computer angeschlossen, ca. 50 HTTP-Server existieren.
- 1993: 2056000 Computer sind angeschlossen, 200 HTTP-Server existieren, der MOSAIC-Browser ist für die wichtigsten Betriebssystem erhältlich. MS Windows lernt TCP/IP kennen.
- 1994: 3864000 Computer sind angeschlossen, Die Firma Netscape wird gegründet. Die erste Internet Bank wird eröffnet.
- 1995: 8200000 Computer sind angeschlossen Die amerikanische Regierung und der Vatikan gehen online.
- 1996: 16729000 Computer sind angeschlossen
- 1997: 26053000 Computer sind angeschlossen
- 1998: 36739000 Computer sind angeschlossen

2 Die Technik des Internets

2.1 Paket-orientierte Datenübertragung

Das Internet ist heute eine Sammlung tausender miteinander verbundener individueller Netzwerke. Das Herz des Internets besteht aus individuellen regionalen Netzwerken. Diese Netzwerke gehören Universitäten, Regierungsstellen, Online-Diensten und Privatfirmen und sind alle miteinander verbunden. Die meisten der Computer in einem Teilnetz (Subnet) sind im Internet nicht mit einer eigenen Adresse bekannt. Computer die netzweit bekannt sind, werden auch als Hosts bezeichnet. Sie können über ihre IP-Adresse eindeutig identifiziert werden.

Wenn Sie Informationen durch das Internet verschicken, werden diese durch das Transmission Control Protocol TCP in einzelne Datenpakete³ zerlegt. Um

³Im Fachjargon des TCP werden diese Datenpakete als Segmente bezeichnet.

diese später wieder zusammensetzen zu können, werden die Pakete mit einer fortlaufenden Sequenznummer versehen.

Diese Datenpakete werden nun vom Internet Protocol mit einem Absenderadresse und einer Empfängeradresse versehen. Diese Adressen werden als IP-Adressen bezeichnet. Eine IP-Adresse oder IP-Nummer besteht aus 4 Zahlen, die durch Punkte voneinander getrennt werden.

Danach werden die Pakete an den nächstgelegenen Router gesandt. Router sind spezielle Computer, die entweder die Adresse des Empfänger-Computers direkt kennen oder einen weiteren Router in der Nähe des Empfänger-Computers. Die Pakete werden also von Router zu Router weitergereicht. Am Bestimmungsort angekommen, wird von TCP auf dem Empfängercomputer die ursprüngliche Nachricht aus den einzelnen Paketen wieder zusammengesetzt. Da die Router von Paket zu Paket entscheiden, über welchen Weg sie ein Paket weiterreichen, kann nicht sicher vorhergesagt werden, welchen Weg ein einzelnes Datenpaket nimmt.

2.2 Adressen im Internet

Das Internetprotokoll IP verwendet Adressen, die aus vier mit Punkten abgetrennten Zahlen bestehen, also 198.232.40.1⁴ wäre eine gültige IP-Adresse. Da sich Menschen meistens Namen besser merken können, werden stattdessen Adressen verwendet, die aus Namen und Buchstaben bestehen. Diese Adressen bestehen aus mehreren Gruppen, den sogenannten Domänen. Der ganz rechts stehende Teil bezeichnet die höchste Domäne: In der Adresse computer.organisation.ch wäre also das Kürzel ch die höchste Domäne.⁵ Diese Domänenorientierten Adressen werden von speziellen Dienstcomputern im Netz - den sogenannten Domain Name Servern - in die numerische IP-Adresse umgesetzt.

2.3 Dienste des Internets

Aufsetzend auf dem Basisprotokoll TCP/IP existieren verschiedene Dienste, die wiederum eigene höherwertige Protokolle verwenden. Die bekanntesten Dienste sind:

- Email (SMTP, POP und IMAP): Dient zum Versenden elektronischer Post. Email-Programme - gibt es als Standalone Programme wie z.B. Eudora, Pegasus, Outlook Express oder integriert in einem Browser wie Netscape.
- FTP: Das File Transfer Protocol ermöglicht das direkte Senden und Empfangen von Dateien von rsp. zu anderen Computern. Der Computer von

⁴Keine der Zahlen kann grösser als 255 sein.

⁵In den USA sind für die höchsten Domänen - den Top Level Domains - folgende Kürzel üblich: com für commercial, edu für Bildungsinstitute, gov für Regierungstellen und Behörden, mil für Militär, net für Netzwerk-Organisationen und org für andere Organisationen oder Vereine. Ausserhalb der USA werden oft nur zwei Buchstaben - nämlich die Landeskennung - für die Top Level Domain verwendet.

dem eine Datei geholt werden soll, muss einen entsprechenden Datei-versandservice anbieten; er muss also als FTP-Server dienen. Auf dem abrufenden Computer muss ein entsprechendes FTP-Programm, also ein FTP-Client, gestartet werden. Diese Clients sind in Browsern wie Netscape oder Internet Explorer enthalten.

- WWW oder HTTP: Dieser Dienst hat das Internet bei der breiten Öffentlichkeit bekanntgemacht. Es handelt sich um das Hypertext Transfer Protocol. Es ermöglicht Texte⁶, die auf verschiedenen Computern⁷ der Welt liegen, anzusehen. Hypertext deswegen, weil sich in diesen Texten aktive Stellen - die sogenannten Links - befinden, über die Sie per Mausklick von einem Text zum nächsten springen können. Programme, mit denen Sie solche Texte durchforsten können, werden als Browser bezeichnet. Die bekanntesten Browser sind Netscape und der Internet Explorer.
- Telnet: Ermöglicht das Absetzen von Befehlen auf weit entfernten Rechnern. Wird oft auch von Bibliotheken verwendet.
- NNTP oder News(groups): Dieser Service besteht aus grossen elektronischen Anschlagbrettern, den Newsgroups. Jeder kann Nachrichten in einer Newsgroup veröffentlichen oder lesen. Newsgroups gibt es zu jedem denkbaren Interessenbereich.

2.3.1 Sicherheit der Dienste

Da fast alle Dienste auf TCP/IP aufsetzen, gelten hier ähnliche Überlegungen. Alle beschriebenen Dienste transportieren ihre Daten unverschlüsselt über das Netz. Das hat folgende Konsequenzen:

- Passwörter gehen unverschlüsselt über das Netz (Email, telnet)
- Email kann in Bezug auf Vertraulichkeit mit einer offen lesbaren Postkarte verglichen werden.
- Absender sind der jeweilig anderen Seite bekannt⁸ (IP-Adresse).

⁶Eine Ansammlung solcher Texte wird auch als Homepage oder Website bezeichnet.

⁷Den HTTP-Servern

⁸Dies ist bei Email meist erwünscht, aber beim Besuch einer Homepage bleiben die meisten Benutzer lieber anonym.