Proseminar Virtuelle Präsenz
Thema: Instant Messaging
Sommersemester 2005

Christina Nell
cn2@informatik.uni-ulm.de

Inhalt

1. Einleitung

Instant Messaging – zu deutsch „sofortige Nachrichtenübermittlung“ – ist definiert als ein Dienst, der es mit Hilfe eines Clients – des so genannten Instant Messengers – ermöglicht, über ein Netzwerk Nachrichten in Echtzeit auszutauschen. Hervorzuheben ist hierbei der Begriff „in Echtzeit“, denn anders als E-Mails, die ihren Empfänger oft mit einer Verzögerung von mehreren Minuten erreichen, beträgt diese Verzögerung beim Instant Messaging meist nur wenige Sekunden.
Seit seinen eher rudimentären Anfängen zu Beginn der 1970er Jahre hat sich Instant Messaging rasant weiterentwickelt. Inzwischen gibt es eine Vielzahl von Instant Messaging-Netzwerken und eine noch größere Anzahl an Instant Messengern.
Diese Ausarbeitung soll einen Überblick über die Entwicklung des Instant Messaging von den Anfängen bis zur Gegenwart geben, sowie die generelle Funktionsweise näher beleuchten.

2. Historischer Überblick

Die Geschichte des Instant Messaging beginnt 1973 auf der Plattform PLATO, der ersten größeren Onlinegemeinde, als Dave Andersen bekannt gab, dass PLATO mit der Option TERM-talk um die Fähigkeit zu einfachem Instant Messaging erweitert worden war[1]. Nach der Anmeldung im System konnte man eine Liste der Benutzer abrufen, die ebenfalls zu diesem Zeitpunkt online waren. Die Unterhaltung selbst fand mit Hilfe von zwei Eingabefeldern statt, in denen der eigene Text und der Text der anderen Person zu sehen waren.
Diese Idee eines einfachen Kommunikationstools wurde bei der Entwicklung der Unix-Distribution 4.2BSD wieder aufgegriffen. Als diese im August 1983 erschien, beinhaltete ihr Funktionsumfang auch den talk-Dämon, dessen Funktionalität der von TERM-talk stark ähnlich war. Beide Ansätze unterstützten jedoch nicht die Funktionalität einer Kontaktliste, wie man sie von modernen Instant Messaging-Programmen kennt.
Das änderte sich 1989, als AOL die erste Version des AOL Instant Messengers veröffentlichte. Dieses Datum gilt als die Geburtsstunde des modernen Instant Messaging, denn auch wenn Nachrichtenaustausch in Echtzeit bereits zuvor möglich war, so war doch die Möglichkeit, eine Liste mit seinen Bekannten zu führen etwas völlig Neues.
Bis ins Jahr 1996 hinein kamen jedoch nur die Mitglieder von AOL in den Genuss dieser bequemen Art der Kommunikation. Doch die Gründung der Firma Mirabilis durch die vier Israelis Yair Goldfinger, Arik Vardi, Sefi Vigiser und Amnon Amir im Juni dieses Jahres und das Erscheinen der ersten Version des Instant Messengers ICQ (kurz für: „I seek you“) im November revolutionierten das Internet. Denn im Gegensatz zum AOL Instant Messenger war ICQ für jedermann kostenlos verfügbar. Das Konzept ging auf – als Mirabilis 1998 von AOL für die Summe von 287 Millionen US-Dollar aufgekauft wurde, konnte das ICQ-Netzwerk bereits über 12 Millionen registrierte Nutzer verbuchen.
Nachdem ICQ erschienen war, explodierte die Zahl der Instant Messaging-Angebote förmlich. 1997 machte AOL seinen Instant Messaging-Dienst, der inzwischen AIM (kurz für AOL Instant Messenger) hieß, der breiten Öffentlichkeit zugänglich; die ersten Unix-Implementierungen für das ICQ-Netzwerk erschienen bereits 1998. Es folgten weitere

[1] Es ist davon auszugehen, dass TERM-talk zwar die erste überlieferte, aber nicht die erste Implementierung eines Instant Messaging-Systems überhaupt war; allerdings hat sich kein anderes System zuvor ähnlicher Beliebtheit erfreut.

Anbieter mit ihren jeweils eigenen Netzwerken, so z.B. Microsoft mit seinem MSN Messenger oder auch Yahoo! mit dem Yahoo! Messenger.
Im Dezember 2002 gab AOL Time Warner bekannt, dass der Tochtergesellschaft ICQ bereits im September desselben Jahres ein US-Patent auf Instant Messaging zugesprochen worden war – und damit auch die entsprechenden Rechte als Erfinder der dahinter stehenden Technologie. Während diese Entwicklung von Seiten der Konkurrenten als sehr bedenklich angesehen wurde, da AOL Time Warner mit diesem Patent seine Konkurrenten wegen Urheberrechtsverletzung auf hohe Millionenbeträge verklagen könnte, versicherte AOL Time Warner, von diesem Recht vorerst keinen Gebrauch zu machen.

Heute ist Instant Messaging das am schnellsten wachsende Segment des Internets. Nach einer Studie von Nielsen//NetRatings ist Instant Messaging mittlerweile zu einem ernsthaften Konkurrenten für die zahlreichen kostenlosen E-Mail-Angebote geworden. Im direkten Vergleich zwischen dem E-Mail- und dem Instant Messaging-Angebot des gleichen Anbieters gewinnt Instant Messaging zunehmend an Marktanteilen. Besonders deutlich ist dies bei MSN zu beobachten, wo das Instant Messaging-Angebot MSN Messenger bereits mehr Benutzer hat als das E-Mail-Angebot MSN Hotmail. Doch auch bei anderen Anbietern wie z.B. Yahoo! zeichnet sich eine ähnliche Entwicklung ab. Der Marktforscher Tom Ewing begründet dies damit, dass „[...] das Senden einer Instant-Nachricht viel leichter und einfacher sein [kann] als das Versenden einer kurzen eMail“.
Die Instant Messaging-Netzwerke verzeichnen insgesamt über eine halbe Milliarde registrierter Benutzer; die Zahl der aktiven Nutzer ist allerdings niedriger einzuschätzen – sie liegt bei etwa 250 Millionen.

3. Der Präsenzbegriff im Instant Messaging

Das wesentliche Merkmal, welches die modernen Instant Messaging-Systeme von ihren Vorgängern wie TERM-talk unterscheidet, ist zweifellos die Präsenzfähigkeit. Dazu muss man wissen, dass Präsenz im Instant Messaging als Onlinestatus definiert ist, der anderen mitteilt, ob der jeweilige Kontakt nun erreichbar, beschäftigt oder abwesend ist. Die Fähigkeit eines Systems, Informationen über diesen Onlinestatus zu geben und auf der anderen Seite Meldungen über eine Änderung dieses Onlinestatus richtig interpretieren zu können, bezeichnen wir als Präsenzfähigkeit.
Um Präsenzfähigkeit realisieren zu können, muss jeder Benutzer durch einen eindeutigen Namen identifizierbar sein. Darüber hinaus pflegt jeder Benutzer eine so genannte Kontaktliste, welche die Namen – und je nach Anbieter auch zusätzliche Informationen wie z.B. Alter, Geschlecht oder auch ein Bild – von Bekannten enthält, mit denen man sich auf regelmäßiger Basis unterhalten möchte. In dieser Kontaktliste wird nun der Onlinestatus durch ein Statusicon symbolisiert, das möglichst selbsterklärend darstellt, welcher Onlinestatus gewählt worden ist.
Wenn man nun von Präsenz spricht, ist häufig die zugrunde liegende Technologie gemeint, die es ermöglicht, auf einen Blick zu sehen, welche der Bekannten auf der Kontaktliste gerade für eine Unterhaltung zur Verfügung stehen. Die virtuelle Präsenz im eigentlichen Sinne ist jedoch vielmehr die Menge an Informationen, die man anderen durch seinen Onlinestatus mitteilen kann. Bereits die frühen Instant Messaging-Systeme kannten die Unterscheidung zwischen zwei Status, nämlich online und offline. Heutzutage haben Benutzer wesentlich mehr Möglichkeiten für die Wahl ihres Status, so kann unter anderem zwischen „beschäftigt“,

„nicht erreichbar“ und „gesprächsbereit“ gewählt werden, die allesamt ein Indikator für Stimmung, Ort oder Situation sein können, in denen sich der entsprechende Kontakt befindet.

4. Netzwerkarchitektur

4.1. Protokolle

Fast jeder Anbieter verwendet für sein Netzwerk ein eigenes Protokoll, das wiederum zu den Protokollen anderer Anbieter inkompatibel ist. Diese Protokolle werden als proprietäre Protokolle bezeichnet, da sie keinen allgemeinen oder offenen Standards entsprechen, sondern eigene Entwicklungen der jeweiligen Anbieter sind. Da es deshalb nicht möglich ist, Nachrichten zwischen zwei verschiedenen Netzwerken auszutauschen – mit Ausnahme der Netzwerke von AIM und ICQ, die beide das gleiche Protokoll verwenden – spricht man auch von fehlender Interoperabilität.
Mittlerweile unterstützen jedoch fast alle Protokolle die gleichen Features wie z.B. Stimm- und Bildübertragungen, so dass sie sich in ihrer Funktionalität kaum noch unterscheiden. Dennoch soll im Folgenden auf die Protokolle drei verschiedener Anbieter näher eingegangen und auch eine logische Konsequenz dieser fortschreitenden Annäherung der Protokolle, nämlich die Entwicklung eines Standards für Instant Messaging-Protokolle, diskutiert werden.

4.1.1. OSCAR/ TOC

Das Open System for Communication in Realtime (OSCAR) ist das Instant Messaging-Protokoll von AOL für dessen zwei Netzwerke AIM und ICQ. ICQ hatte zuvor sein eigenes Protokoll genutzt, das jedoch nach der Übernahme von Mirabilis durch AOL zugunsten von OSCAR aufgegeben wurde. OSCAR unterstützt Dateitransfer und darüber hinaus das Einbinden von Musik- und Bilddateien direkt in die Unterhaltung.
Nachdem AOL Einzelheiten von OSCAR veröffentlicht hatte, um es z.B. den Entwicklern von Instant Messengern unter Linux zu ermöglichen das AIM-Netzwerk zu nutzen, implementierten auch Konkurrenten wie Microsoft und Yahoo! diese Möglichkeit in ihren Clients. Daraufhin nahm AOL Änderungen am Protokoll vor, um die Konkurrenten auszuschließen. Dies stellte jedoch keine langfristige Lösung dar, weil die Clients der Konkurrenten schon nach kurzer Zeit wieder eine Verbindung in das AIM-Netzwerk herstellen konnten.
Nach diesen negativen Erfahrungen veröffentlichte AOL schließlich im Jahre 1998 das Protokoll TOC (kurz für Talk to OSCAR), das wie OSCAR in der Lage ist, eine Verbindung zum AIM-Netzwerk herzustellen. Dadurch dass TOC völlig offen und für jeden zugänglich war, erhoffte sich AOL ein Ende der Entschlüsselungsversuche bezüglich OSCAR. TOC wurde jedoch sehr schlecht angenommen, da sich die Fähigkeiten des Protokolls auf reinen Chat beschränken, also keine weiteren Funktionen von OSCAR wie z.B. Dateitransfer unterstützt werden, und zudem die Paketgröße auf 1024 Bytes beschränkt ist, was zur Folge hat, dass längere Nachrichten unter Umständen auf mehrere Pakete verteilt werden müssen.

4.1.2. MSNP

Das Mobile Status Notification Protocol (MSNP) ist das Protokoll, das dem .NET Messenger Service von Microsoft zugrunde liegt. Dieser Service ist die Basis von Microsofts Internetplattform MSN. Zusammen mit dem Microsoft Passport-System ermöglicht er die

Nutzung vieler verschiedener Angebote von Microsoft mit einem universellen Benutzeraccount. Die offiziellen Instant Messaging-Clients des MSN-Netzwerks sind der MSN Messenger, dessen erste Version im Juli 1999 erschien, und der in das Betriebssystem Windows XP integrierte Windows Messenger, die beide sowohl Stimm- als auch Video- und Bildübertragungen unterstützen.
Wie auch AOL machte Microsoft 1999 sein Protokoll in der damals aktuellen Version 2 der Öffentlichkeit zugänglich, um so die Entwicklung von Linux-Clients für das MSN-Netzwerk zu ermöglichen. Die folgenden Versionen 8, 9, 10 und auch die aktuelle Version 11 wurden nicht veröffentlicht – diese Versionen sind jedoch die einzigen, die die MSN-Server momentan akzeptieren.

4.1.3. YMSG

Das Netzwerk des Yahoo! Messengers, des Instant Messengers von Yahoo!, verwendet ein Protokoll namens YMSG. Im Gegensatz zu den vorher genannten Protokollen haben diese 4 Buchstaben jedoch keine tiefere Bedeutung. YMSG unterstützt unter anderem Dateitransfer, Stimm-, Bild- und Videoübertragungen sowie die Möglichkeit, sich einen eigenen Avatar zu erschaffen und diesen nach Belieben zu konfigurieren. Zur Authentifizierung innerhalb des Netzwerks dient ein allgemeingültiger Benutzeraccount, die so genannte Yahoo! ID, der auch Zugang zu anderen Angeboten von Yahoo! bietet, wie z.B. Yahoo! Mail.
Trotzdem liegt der Marktanteil des Yahoo! Messengers in Europa bei lediglich etwa 3,0% - im Vergleich zu 22,9%, die der MSN Messenger erreicht[2]. Vermutlich ist das ein Grund dafür, dass es im Bereich des Instant Messaging schon seit dem Erscheinen der ersten Version des Yahoo! Messengers im Juni 1999 auffällig still um den Internetriesen ist. Dennoch liegt auch YMSG mittlerweile in der Version 11 vor, die vom Yahoo! Messenger 6.0 verwendet wird.

4.1.4. Standards

Wie man sieht, unterscheiden sich die drei hier vorgestellten Protokolle im Wesentlichen nur noch durch den Namen des Netzwerkes, in dem sie verwendet werden, an Interoperabilität ist hierbei dennoch nicht zu denken. Da man Interoperabilität aber mit Fug und Recht als „heiligen Gral des Instant Messaging“ bezeichnen kann, wie es auf der Internetseite bigblueball.com zu lesen ist, hat die Internet Engineering Task Force (IETF) immer wieder versucht, einen gemeinsamen Standard für Instant Messaging-Protokolle zu etablieren. Besonders hervorzuheben wären hierbei wohl das Instant Messaging and Presence Protocol (IMPP) sowie SIP[3] for Instant Messaging and Presence Leveraging Extensions (SIMPLE). Obwohl beide Protokolle über die gleiche Funktionalität verfügen, nämlich sowohl den Nachrichtenaustausch zwischen zwei oder mehr Teilnehmern unterstützen als auch die Fähigkeit besitzen, Informationen über Präsenz zu geben bzw. den Benutzer zu benachrichtigen, wenn ein Kontakt seinen Status ändert, sind sie ansonsten kaum miteinander zu vergleichen. Denn während IMPP ein von Grund auf neu entwickeltes Protokoll ist, ist SIMPLE lediglich eine Erweiterung des bereits bestehenden SIP-Protokolls. Abgesehen davon unterscheidet die beiden Protokolle auch die Tatsache, dass das IMPP bereits als Standard verabschiedet wurde, während SIMPLE noch in Arbeit ist – auch wenn mittlerweile einige Teile standardisiert und schon erste Implementierungen vorhanden sind.

[2] Diese Zahlen stammen aus der bereits angesprochenen Studie von Nielsen//NetRatings vom März 2004.
[3] SIP = Session Initiation Protocol; ein weiterer Standard der IETF, der jedoch hauptsächlich in der IP-Telefonie Verwendung findet

Trotz aller Versuche seitens der IETF ist es bisher jedoch nicht gelungen, die großen Anbieter wie AOL und Microsoft dazu zu bewegen, einen dieser Standards anzunehmen. Aus diesem Grund wurden seit etwa Anfang 2000 mehr und mehr so genannte Multiprotokoll-Clients entwickelt, die in der Lage sind, Verbindungen zu mehreren Netzwerken gleichzeitig herzustellen und dem Benutzer so die Installation vieler separater Instant Messenger ersparen. Diese Multiprotokoll-Clients stehen jedoch vor dem Problem, dass die großen Anbieter alles unternehmen, um sie aus ihren Netzwerken auszusperren und deshalb immer wieder Kleinigkeiten an ihren Protokollen ändern, so dass sich auch die Entwickler der entsprechenden Multiprotokoll-Clients gezwungen sehen, ihre Programme zu überarbeiten.
Darüber hinaus stellen die Multiprotokoll-Clients auch keine Lösung für das Problem der fehlenden Interoperabilität dar, weil sie es dem Benutzer lediglich ermöglichen, in mehreren Netzwerken gleichzeitig online zu sein ohne jedoch die jeweiligen Clients dieser Netzwerke parallel laufen zu lassen. Denn auch wenn der Benutzer so in zwei voneinander verschiedenen Netzwerken kommunizieren kann, ist es ihm nicht möglich, von einem Netzwerk aus eine Nachricht in ein anderes Netzwerk zu schicken.

4.2. Beispiel einer Nachrichtensitzung

Im folgenden soll dargestellt werden, wie eine typische Nachrichtensitzung zwischen zwei Benutzern eines Instant Messaging-Netzwerkes abläuft. Diese Darstellung lässt sich problemlos auf so gut wie alle Netzwerke übertragen, der Vollständigkeit halber sollte jedoch angemerkt werden, dass diese Beschreibung auf den Abläufen innerhalb des ICQ-Netzwerkes basiert.

4.2.1. Anmelden

Bevor eine Nachrichtensitzung gestartet werden kann, muss sich der Benutzer im Netzwerk mit seinem Namen und seinem Passwort authentifizieren. Dies geschieht, nachdem der Client des Benutzers zum ersten Mal versucht hat, eine Verbindung zum jeweiligen Server herzustellen. Der Server sendet daraufhin einen zufälligen String an den Client, den der Client an das vom Benutzer eingegebene Passwort anhängt. Mittels eines Hash-Verfahrens wird dieser neue String verschlüsselt und an den Server zurückgesendet. Stimmt das gesendete Passwort mit dem Passwort überein, was für den jeweiligen Benutzer auf dem Server gespeichert ist, fordert der Server den Client auf, die Verbindungsinformationen – also die IP-Adresse des Rechners, auf dem der Client installiert ist, und den dem Client zugewiesenen Port – zu übermitteln. Diese Verbindungsinformationen werden zusammen mit der Kontaktliste des Benutzers in einer temporären Datei auf dem Server gespeichert.
Ausgehend von diesen Informationen sucht der Server nun nach bereits eingeloggten Kontakten aus der Liste des Benutzers. Sollte diese Suche einen Treffer ergeben, werden die entsprechenden Verbindungsinformationen des Kontakts an den Client des Benutzers gesendet, ebenso empfängt der Client des Kontakts die Verbindungsinformationen des Benutzers. Je nach Art der empfangenen Informationen wird im Client das Statusicon für den entsprechenden Kontakt gesetzt.

4.2.2. Kommunikation (Peer-to-Peer)

Basiert das Instant Messaging-Netzwerk auf einer Peer-to-Peer-Architektur, so findet die Kommunikation zwischen den Benutzern nur zwischen den jeweiligen Clients statt, ohne den Server noch miteinzubeziehen, wie die folgende Abbildung veranschaulicht.

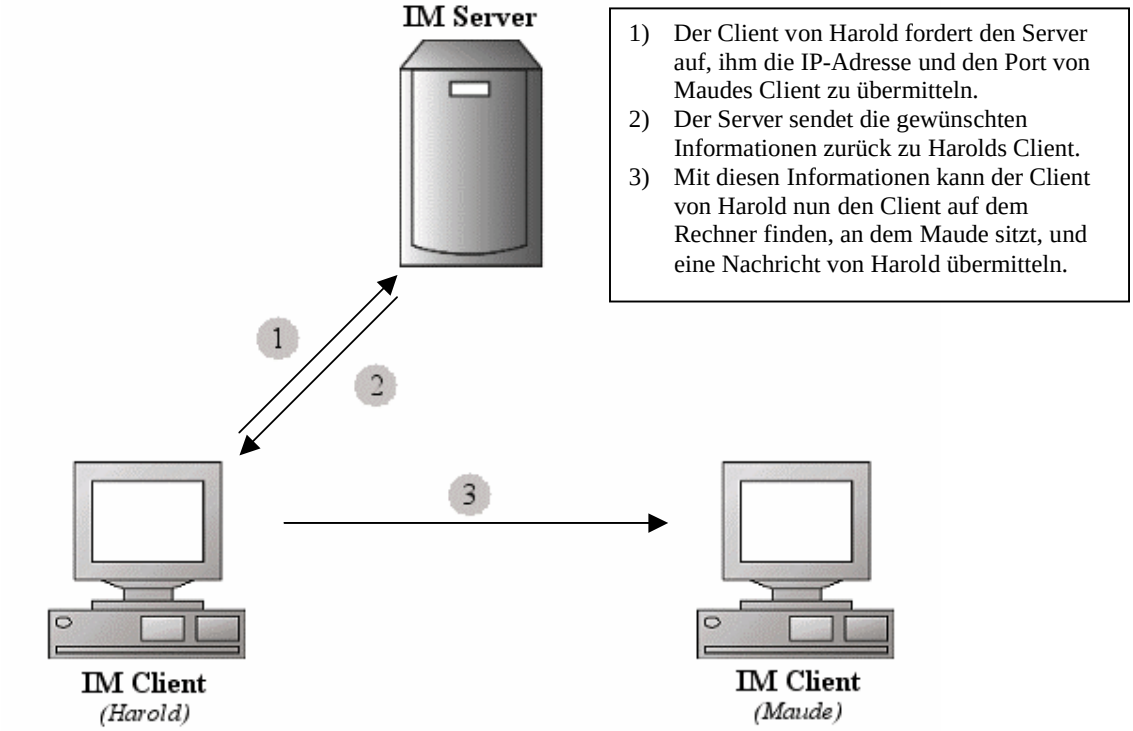

Abb. 1: Darstellung der Kommunikation in einer Peer-to-Peer-Architektur

Diese Netzwerkarchitektur ist besonders dann zu empfehlen, wenn beide Benutzer Teil desselben Netzwerkes sind, wie das z.B. in einem Unternehmen der Fall sein könnte. Zwar läuft die Anmeldung am Server über das Internet, die Kommunikation zwischen den beiden Benutzern läuft jedoch ausschließlich über das Netzwerk ab, d.h. die Unterhaltung kann nicht über das Internet belauscht werden, was eine größere Sicherheit im Umgang mit vertraulichen Daten bedeutet.

4.2.3. Kommunikation (Client-to-Server)

Die wenigsten Netzwerke verwenden heute noch eine Peer-to-Peer-Architektur. Stattdessen hat sich gewissermaßen die Verwendung einer Client-to-Server-Architektur eingebürgert. Wenn ein Benutzer sich mit einem seiner Kontakte unterhalten möchte, so wird die Nachricht für den Kontakt zuerst an den Server gesendet, der diese Nachricht dann an ihren Empfänger weiterleitet.

Diese Client-to-Server-Architektur birgt allerdings den großen Nachteil, dass eine Unterhaltung potentiell durch den Anbieter des jeweiligen Instant Messaging-Netzwerkes mitgeschnitten werden kann, was eine starke Gefährdung der Privatsphäre darstellt. In der Tat löste AOL mit einer dahingehenden Änderung seiner Allgemeinen Geschäftsbedingungen im Februar 2005 einen Aufschrei der Empörung aus. Mit dem Zustimmen zu der aktualisierten Version nahmen die Benutzer nämlich nicht nur einen Eingriff in ihre Privatsphäre in Kauf, sondern gestatteten AOL auch, sämtliche Inhalte zu eigenen Zwecken zu verwenden. Nachdem dies bekannt geworden war, zog AOL seine Allgemeinen Geschäftsbedingungen

zur Überarbeitung zurück; bei deren Neuerscheinen war der entsprechende Passus verschwunden.

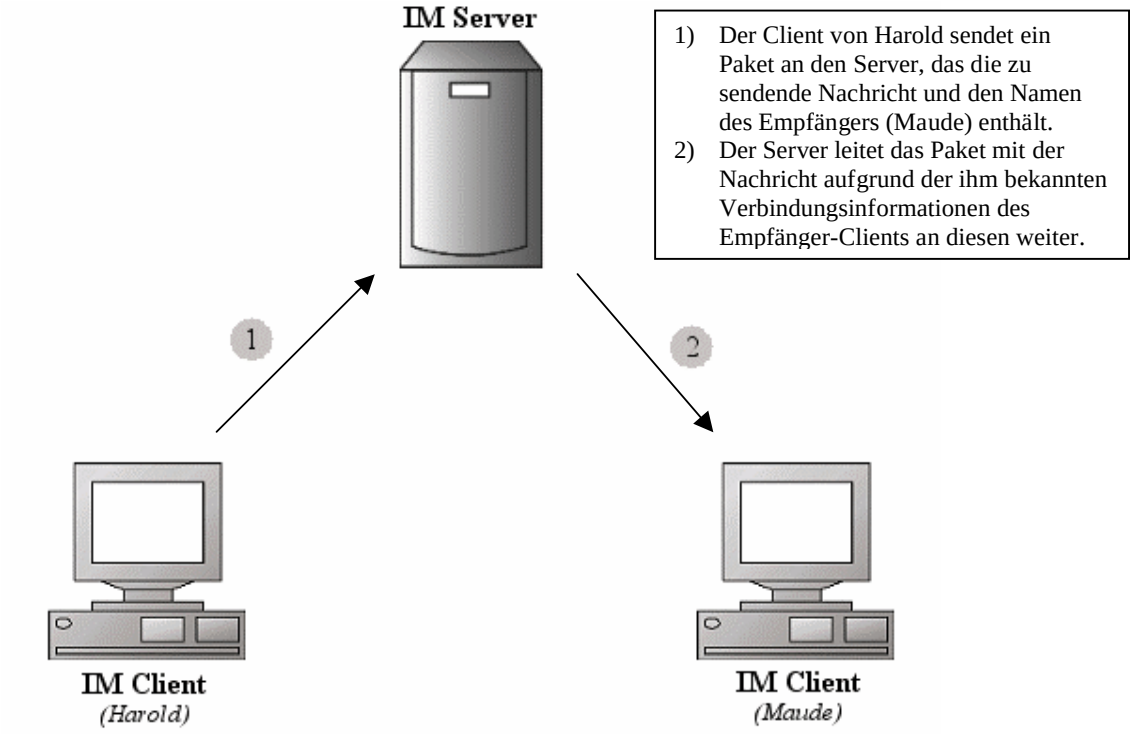

Abb. 2: Darstellung der Kommunikation in einer Client-to-Server-Architektur

Generell begünstigt diese Netzwerkarchitektur das Mitschneiden einer Unterhaltung durch Dritte. Selbst wenn das nicht serverseitig durch den Betreiber erfolgt, besteht immer noch die Gefahr, dass die Unterhaltung – die unverschlüsselt über das Internet übertragen wird – durch fremde Personen mitgeschnitten wird. Dies ist nicht nur dann ein Problem, wenn ein Unternehmen Instant Messaging zur internen Kommunikation einsetzt und es um vertrauliche Unternehmensdaten geht, sondern auch in privaten Unterhaltungen, in denen womöglich Telefonnummern, Adressen oder Bankverbindungen ausgetauscht werden.
Wie eingangs erwähnt ist es jedoch die Client-to-Server-Architektur, die sich im Lauf der Jahre durchgesetzt ist und so findet sie heute zumindest in den Netzwerken der großen Anbieter ihre Verwendung, z.B. im AIM-, MSN-, ICQ- und Yahoo!-Netzwerk.

4.2.3. Abmelden

Wenn der Benutzer die Nachrichtensitzung beenden möchte, wählt er in seinem Client den Status „offline“, woraufhin der Client eine Nachricht an den Server sendet, dass die Sitzung beendet werden soll. Die Clients der Kontakte erhalten eine Nachricht vom Server, dass der entsprechende Benutzer sich abgemeldet hat. Schlussendlich wird die temporäre Datei mit den Verbindungsinformationen, welche zu Beginn der Nachrichtensitzung auf dem Server angelegt wurde, gelöscht, so dass innerhalb des jeweiligen Instant Messaging-Netzwerkes keine Informationen mehr darüber verfügbar sind, wie der jeweilige Kontakt zu erreichen ist. Ab diesem Zeitpunkt erscheint man auch in den Kontaktlisten seiner Kontakte als offline.

5. Sicherheitsaspekte

Wenn man sich einmal vor Augen führt, dass die gesamte Kommunikation innerhalb von Instant Messaging-Netzwerken bis heute unverschlüsselt erfolgt[4] und dass Instant Messenger eine Vielzahl von Angriffsflächen bieten, so ist eigentlich erstaunlich, dass die Netzwerke bisher von großen Angriffen verschont geblieben sind.
Denn der Instant Messenger an sich ist eine ideale Plattform für die Verbreitung von Würmern und anderen Schädlingen. Das hat vier Gründe:
Erstens sind Instant Messenger mittlerweile quasi allgegenwärtig. Wie bereits in den vorherigen Kapiteln erwähnt, erfreuen sie sich großen Zulaufs und noch größerer Beliebtheit. Auch wenn die Prognose des Unternehmens Jupiter Media Metrix, die den Anteil der Instant Messaging-Nutzer an der gesamten Onlinebevölkerung für das Jahr 2003 auf 90% schätzte, letztendlich doch nicht eingetreten ist, ist davon auszugehen, dass diese Marke eines Tages erreicht wird.
Zweitens bieten sie dadurch, dass sie als große Netzwerke mit einem zentralen Server organisiert sind, eine gewisse Kommunikationsinfrastruktur. Diese Infrastruktur wird unterstützt durch die Kontaktlisten, von denen jeder Benutzer über jeweils eine verfügt. Stellt man sich nun vor, dass ein Benutzer von einem Wurm befallen ist, so stellt diese Kontaktliste eigentlich nichts anderes dar als ein integriertes Verzeichnis zum Auffinden neuer Opfer – ähnlich dem Adressbuch eines E-Mail-Programmes.
Drittens ist es äußerst schwierig, einen Instant Messenger durch einen Virenscanner zu überwachen. Zwar bieten mittlerweile einige Clients an, die heruntergeladenen Dateien durch den lokal installierten Virenscanner auf Würmer, Viren und andere Schädlinge zu überprüfen, doch dieses Feature ist nicht so weit verbreitet wie man meinen könnte. Gerade auch deshalb bieten einige Hersteller von Virenscannern Plugins für alle gängigen Instant Messenger an. Doch die Entwicklung dieser Plugins ist schwierig, da sie auf den jeweiligen Clients der Anbieter basieren, die sich genau wie die Protokolle von Zeit zu Zeit ändern – weswegen auch die Plugins immer wieder geändert werden müssen. Und selbst wenn die Entwicklung dieser Plugins vereinfacht würde, so bestünde weiterhin das Problem, dass nicht der Instant Messaging-Verkehr selbst überwacht wird sondern lediglich die Dateien, die über das jeweilige Netzwerk übertragen werden – und auch das findet erst statt, nachdem die Datei den Rechner des jeweiligen Benutzers bereits erreicht hat.
Viertens sind die meisten Instant Messenger durch einfach zu schreibende Skripte leicht zu kontrollieren, auch wenn es nicht jeder Anbieter den Programmierern dieser Skripte so leicht macht und seine Benutzer ausdrücklich dazu auffordert, den Instant Messenger mit Hilfe von selbst geschriebenen Programmen in Visual Basic oder JavaScript ihren individuellen Vorstellungen anzupassen.

Die eigentlichen Gefahren für die Benutzer eines Instant Messengers sind vielfältig. Sie reichen von scheinbar profanen Gefährdungen wie den Abhören einer Unterhaltung über Trojaner bis hin zu Würmern. Sofern es dabei allerdings um so genannte Exploits geht, also das Ausnutzen von Fehlern im Quelltext des jeweiligen Instant Messengers, so reagieren die meisten Anbieter zum Glück schnell und umsichtig durch Patches oder – wenn möglich – Ausmerzen des jeweiligen Problems auf Seiten des Servers.
Bei Trojanern stellt sich das als schwieriger dar. Theoretisch gesehen begünstigt die Infrastruktur in Instant Messaging-Netzwerken die Entwickler von Trojanern allein schon durch den dem modernen Instant Messaging zugrunde liegenden Gedanken der Präsenz.

[4] Lediglich der Anbieter des in Polen weit verbreiteten Instant Messengers Gadu Gadu bietet seinen Benutzern ab der aktuellen Version 6.0 optional eine SSL-Verschlüsselung an.

Selbst wenn das Opfer des Trojaners eine dynamische IP-Adresse besitzt, die sich bei jeder Einwahl ändert, so bleibt doch der Screenname des Opfers immer gleich. Wenn der Entwickler des Trojaners das Opfer auf seiner Kontaktliste stehen hat, so wird er auch jederzeit über den Status des Opfers informiert.

Auch wenn es sehr paradox klingen mag, in diesem speziellen Fall hat die fehlende Interoperabilität auch ihr Gutes. Denn dadurch, dass man aus einem Netzwerk heraus nicht in ein anderes Netzwerk kommunizieren kann, ist es einem Wurm oder Trojaner auch nicht möglich, sich ohne weiteres von einem Netzwerk auf das andere zu übertragen. Setzt man voraus, dass ein Wurm für ein spezielles Instant Messaging-Netzwerk programmiert und in dieses Netzwerk eingeschleust wurde, so ist letztlich nur dieses Netzwerk von dem Wurm betroffen – für die Benutzer in anderen Netzwerken besteht keine Gefahr.

6. Zusammenfassung

Zusammenfassend kann man sicherlich sagen, dass Instant Messaging enorm von der hohen Verbreitung des Internets profitiert hat. Wäre es heutzutage nicht möglich, zu einem vergleichsweise geringen Festpreis unbegrenzt Zeit online zu verbringen, hätte Instant Messaging als Form der unkomplizierten und schnellen Kommunikation niemals solche Beliebtheit erlangt, da es schlicht und ergreifend unerschwinglich wäre. Die Nutzerzahlen werden weiter steigen, wenn auch die Wachstumsraten der letzten Jahre wahrscheinlich nicht mehr erreicht werden können, da sich aufgrund der bereits jetzt recht hohen Nutzerzahlen eine gewisse Sättigung einstellen wird.
Doch das entscheidende Feature, welches das moderne Instant Messaging überhaupt erst zu dem gemacht hat, was es ist, ist mit Sicherheit die Präsenz. Durch Kontaktlisten und Statusicons ist es so einfach wie nie, den Aufenthaltsort von Freunden, Bekannten oder Geschäftskollegen zu bestimmen und Aussagen darüber zu treffen, ob eine Unterhaltung zum entsprechenden Zeitpunkt möglich ist oder nicht.
Das einzige Hindernis auf dem Weg zu einem weltumspannenden Kommunikationsnetz ist wahrscheinlich die fehlende Interoperabilität, welche die Benutzer zur Installation mehrerer Instant Messenger zwingt, wenn sie keinen der Multiprotokoll-Clients verwenden möchten.
Doch all diese Punkte beinhalten ein größeres Sicherheitsrisiko als den meisten Benutzern heute bewusst sein dürfte. Dass eine höhere Verbreitung z.B. auch bedeutet, dass die Wahrscheinlichkeit, den eigenen PC durch einen Instant Messaging-Wurm zu infizieren, signifikant steigt, ist eine Tatsache, die in der Euphorie über die Einfachheit dieser Kommunikationsform leicht übersehen wird. Nur wenn vor diesen Gefahren genauso konsequent gewarnt wird wie dies z.B. im Fall der E-Mail-Würmer geschehen ist, kann vermieden werden, dass diese schmerzhafte Lektion zweimal gelernt werden muss.

Quellenangabe

- „Instant Messaging“
  http://de.wikipedia.org/wiki/Instant_Messaging

- „TERM-talk: PLATO’s Instant Messaging“
  http://www.platopeople.com/termtalk.html

- „The ICQ Story“
  http://www.icq.com/info/icqstory.html

- „Patent creates IM wrinkle“
  http://news.com.com/2100-1023-978234.html

- Jeff Tyson, „How Instant Messaging Works“
  http://computer.howstuffworks.com/instant-messaging.htm

- „AOL Instant Messenger: Verwirrung um Nutzungsbedingungen“
  http://www.golem.de/0503/36954.html

- „Threats to Instant Messaging“
  http://securityresponse.symantec.com/avcenter/reference/threats.to.instant.messaging.pdf