Problemseminar im WS 2003/04 – Prof. Rahm

Peer-to-Peer (P2P) Data-Management

P2P Security, Trust and Privacy Sharing

Bearbeiter: Christian Lehmann

Betreuer: Dr. Dieter Sosna

Inhaltsverzeichnis

1. Einleitung:

1.1. Allgemeine Einführung:

Heute nutzen mehrere Millionen Nutzer das Internet und Peer-to-Peer File-Sharing Systeme ohne dabei genau zu wissen, welche Gefahren sich dahinter verbergen. Diese Ausarbeitung soll dazu dienen, die unterschiedlichen Gefahren zu erläutern und Lösungsvorschläge zu unterbreiten.

Zu Beginn werden die allgemeinen Sicherheitsmechanismen vorgestellt und kurz erläutert. Anschließend werden aktuelle Sicherheitsprobleme in Peer-to-Peer Systemen untersucht und teilweise gelöst.

Peer-to-Peer File-Sharing Programme wie Kazaa oder Emule sind die am meisten heruntergeladenen Computerprogramme der heutigen Zeit. Die Sicherheit dieser Programme wird in einem extra Kapitel untersucht.

1.2. Definitionen

Security: Praktiken, die von Individuen durchgeführt werden um all ihr physikalisches und intellektuelles Eigentum vor allen Arten von Angriffen und Plünderungen zu schützen. [SM97]

Trust: Vertrauen, dass man selbst anderen Institutionen oder Instanzen entgegenbringt.

Privacy: Privacy bedeutet die Sicherheit vor dem Eindringen von anderen Personen in das eigene Privatleben oder Angelegenheiten sowie die Geheimhaltung dieser Informationen.

2. Grundfunktionen sicherer Systeme

2.1. Grundbegriffe:

- ***Identifikation***

  Inhalt: Der Nutzer teilt dem System mit, wer er ist.

  Realisierung: Die Identifikation erfolgt durch Benutzer-IDs. Idealerweise sollte jeder Nutzer eine eindeutige systemweite Benutzer-ID besitzen, die in allen Applikationen genutzt wird.

- ***Authentifikation***

  Inhalt: Überprüfung der vom Benutzer angegebenen Identität.

  Realisierung: Üblicherweise geschieht die Authentifikation durch ein Passwort. Dabei ist ein Austausch von Informationen zwischen dem Nutzer und der Anwendung nötig, um das Passwort zu übermitteln. Moderne Verfahren der Authentifikation sind Irisscanner, Fingerabdrucksscanner oder Stimmenidentifizierung.

- ***Autorisation***

  Inhalt: Die Autorisation regelt die Vergabe von Rechten.

  Realisierung: Vergabe von Administrator- oder Gastrechten.

- ***Rechte -Prüfung***

  Inhalt: Bei jedem Zugriff auf ein Objekt wird die Berechtigung dieses Zugriffs gegen vergebene Rechte geprüft.

  Realisierung: z.B. durch Eigenschaften der Dateien (Flags)

- ***Schutz vor Verlust der Vertraulichkeit***

  Inhalt: Schutz vor unbefugter Einsichtnahme in Informationen bei der Datenhaltung und beim Datentransfer.

  Realisierung: Durch Zugriffskontrolle sowie Verschlüsselung.

- ***Schutz vor Verlust der Datenintegrität***

  Inhalt: Das System enthält Vorkehrungen, die es ermöglichen nicht-korrekte Datenveränderungen zu erkennen, zu verhindern und rückgängig zu machen.

  Realisierung: Durch Ein-Wege-Hashfunktionen angewandt auf Dateien kann eine Veränderung festgestellt werden.

- ***Funktionen in vernetzten Systemen***

1. Wechselseitige Authentifikation

   Das sichere Authentifizieren der beiden Kommunikationspartner untereinander.

2. Schutz der Kommunikation

   Schutz der Datenintegrität auf dem Weg durch ein Netz vor Verlust der Integrität oder der Vertraulichkeit bzw. Erkennen wenn ein Verlust aufgetreten ist.

3. Anonymität

   Die Anonymität steht im Widerspruch zu den obigen Funktionen, dennoch kann es Aktionen im Internet geben, bei denen Anonymität erwünscht ist. Bei der Anonymität

sollen sowohl Sender und/oder Empfänger anonym sein, und es soll verborgen werden, dass überhaupt eine Kommunikation stattgefunden hat.

3. Untersuchung spezieller P2P Programme auf ihre Sicherheit

3.1. Der Edonkeyclient Emule (Version 0.30e für Windows)

Emule ist der populärste Client für das Edonkey-Netzwerk. Mit Emule ist es möglich Proxies einzustellen. Damit können Rechner, die sich aus Sicherheitsgründen hinter einem Proxy befinden auch mit Emule arbeiten und Dateien tauschen. Der Proxy verringert die Angriffsmöglichkeiten über IP-Adressen.
Freigaben sind für einzelne Verzeichnisse möglich, aber nicht für spezielle Dateien. Weiterhin ist die Freigabe unübersichtlich, da übergeordnete Verzeichnisse nur fett gedruckt werden. Diese heben sich nur schwach von den nicht freigegebenen Verzeichnissen ab. Hier wäre eine Rotfärbung besser geeignet um anzuzeigen, dass Unterverzeichnisse freigegeben wurden.
Es ist erlaubt Netzlaufwerke freizugeben, durch die Angabe der Netzpfade wie '\\Server\Verzeichnis'. Damit können firmeninterne Daten durch einen Nutzer ohne große Anstrengung freigegeben werden. Darum sollte man als Netzwerkadministrator genau überwachen, welcher Nutzer den Emuleclient nutzt und entsprechend dagegen vorgehen.
Durch Webinterfaces kann der Nutzer seinen Emuleclient von jedem anderen Computer mit Internetzugang steuern. Ein nettes Feature, aber auch eines der größten Sicherheitsrisiken im Emule. In den Hilfedateien wird auch ausdrücklich darauf hingewiesen, dieses Feature nur zu aktivieren, wenn man es nutzt. Es gibt einen Administratoraccount, mit dem man den Emuleclient komplett steuern kann. Weiterhin gibt es die Möglichkeit von Gastaccounts. Dieser Account kann keine Einstellungen am Emule vornehmen, aber dennoch Dateien zum Download hinzufügen. Weiterhin gibt es das MobileMule, mit dem die Fernsteuerung auch über javafähige Handys möglich ist. Die Accounts werden durch ein Passwort abgesichert. Hat man aber einmal das Passwort herausgefunden, kann man dem Emuleclient jede Menge copyrightgeschützte Dateien hinzufügen und einer Behörde einen Tipp zukommen lassen. Auf diese Weise hat der Nutzer ein Strafverfahren am Hals, für dass er eigentlich nichts kann.

Da man sich über Emule auch Nachrichten schicken kann, ist man auch hier vor Spam nicht sicher. Deshalb gibt es die Möglichkeit nur Nachrichten von Freunden zuzulassen. Leider ist diese Einstellung nicht standardmäßig aktiviert. Auch das Filtern von Nachrichten ist möglich (siehe Beispiel).

Der Advanced Spamfilter ignoriert Nachrichten, wenn bereits fünf Nachrichten von dem Nutzer eingegangen sind und bisher keine Antwort erfolgte, oder wenn bei der ersten Kontaktaufnahme bereits eine Internetadresse mitgesendet wird.

Unter 'nutze sichere Identifikation' verbirgt sich ein Public-Key-Verfahren mit Signatur um eine Nutzerauthentifikation zu gewährleisten. Damit soll ein Nutzer seine Kredits, die er erworben hat, auch nach einem Neustart des Clients besitzen.

Dazu erstellt Nutzer A einen privaten 384 bit RSA Schlüssel, der auf der Festplatte gespeichert wird. Ironischer Weise steht in der Hilfe nichts davon, dass man dieses Verzeichnis dann unter keinen Umständen freigeben sollte. Dieser Schlüssel wird einmalig erzeugt und bleibt ab dann für alle Identifikationen erhalten. Sollte die Datei mit dem privaten Schlüssel verloren gehen, hat Nutzer A, damit alle seine Kreditpunkte verloren. Verbinden sich zwei Nutzer, welche beide diese Option aktiviert haben, senden sie jeweils einen öffentlichen Schlüssel zusammen mit einer Zufallszahl an ihren Partner. Dieser speichert den Schlüssel in einer Datei. Die Zufallszahl wird bei jeder Verbindung neu generiert. Diese Speicherung findet auch nur statt, wenn sich die beiden Teilnehmer noch nicht kannten.

Will sich Nutzer A zu einem späteren Zeitpunkt erneut bei Nutzer B anmelden, erzeugt er mit Hilfe seines privaten Schlüssels, dem öffentlichen Schlüssel von B und einer Zufallszahl eine digitale Signatur. Diese Signatur ist gültig, bis sich die IP von einem der beiden Teilnehmer ändert, oder einer den Emuleclient beendet.

Nachdem B die Signatur von A erhalten hat, überprüft er, ob diese aus seinem öffentlichen Schlüssel und seiner Zufallszahl erzeugt wurde, und ob sie zu dem öffentlichen Schlüssel von A passt.

Diese Option ist in Version 0.30e bereits standardmäßig aktiviert.

Bei Emule gibt es auch eine Vorschaufunktion für gewisse Dateien. So kann man sich avi, mpg, mpeg, divx, xvid, zip ,rar und ace Dateien mit der Vorschaufunktion ansehen. Allerdings nur, wenn der Anfang und das Ende der Datei bereits heruntergeladen wurde. Somit kann man sich einigermaßen vor Self-Help-Attacken (Fakes) schützen.

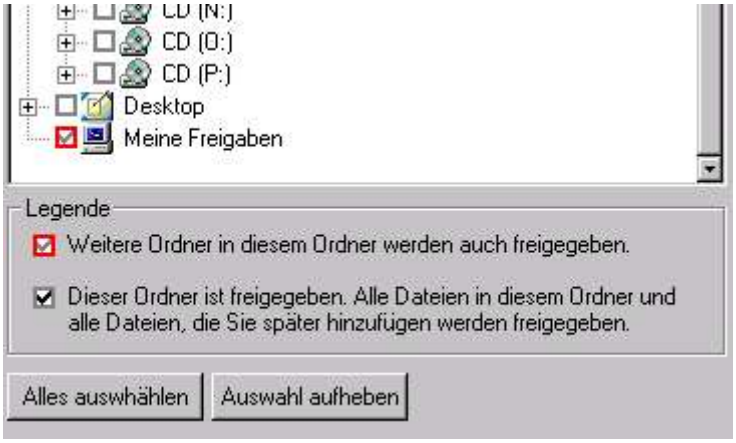
Zusammenfassung:

Emule ist ein Client, bei dem die Nutzerauthentifikation auch bei einem erneuten Verbinden möglich ist. Die Datenintegrität wird durch Hashwerte geprüft, die man sich auch im Client ansehen kann. Wurde die Datei auf dem Übertragungsweg verfälscht, wird der Teil dieser Datei erneut geladen. Somit wird exakt die Datei heruntergeladen die zu dem Hashwert gehört.

Nähere Informationen zu der Arbeitsweise von Emule findet sich unter [EM03]

3.2. Kazaa Lite 2.4.3 (Windows)

Kazaa Lite ist die von Ad- und Spyware befreite Version der normalen Kazaa Version.



In Kazaa gibt es einen Ordner 'My Shared Folder' in dem alle Dateien gelagert werden, die man herunterlädt. Dieser Ordner ist auch standardmäßig freigegeben für das Tauschen von Dateien im Kazaa Netzwerk. Wem dieser Ordner nicht genügt, der kann auch eigene Ordner zu den Freigaben hinzufügen. Bei dieser Methode werden die Ordner rot markiert, die freigegebene Unterordner enthalten. So kann man sehr einfach seine Freigaben im Auge behalten.

Weiterhin kann man einen Suchassistenten nutzen, der einem die Festplatte nach Dateien durchsucht, die man freigeben könnte.

Davon ist aber abzuraten, da man schnell persönliche Daten freigeben könnte, wenn man die Liste der gefundenen Daten nicht genau untersucht.

Eine besonders gelungene Methode die freigegebenen Dateien aufzulisten, ist es diese nach ihrer Art zu unterscheiden. So kann man schnell sehen welche Musik-, Video- oder Bilddaten freigegeben sind.

Ein integrierter Virenscanner bietet einen gewissen Schutz vor Viren, die man sich über das Netzwerk herunterladen könnte.

Kazaa Lite wird es vorerst nicht weiterentwickelt, da Sharman Networks, Hersteller von Kazaa, die Betreiber der Kazaa Lite Webseite verklagt hat. Sie verletzten

Urheberrechte und behindern den Verkauf der werbefreien Version Kazaa Plus für ca. 30 Dollar.

Zusammenfassung:

Kazaa bietet keine Möglichkeit der Nutzerauthentifikation, nutzt aber auch kein Feature wie Kreditpunkte. Es ist nicht ersichtlich, dass eine Prüfung der Datenintegrität stattfindet, so dass Dateien verfälscht beim Nutzer eintreffen können.

Der Virenschutz sowie die Übersichtlichkeit der Freigaben erleichtern unerfahrenen Benutzern die Bedienung des Clients. Negativ sind vor allem die Ad- und Spyware in der kostenlosen Kazaa-Version.

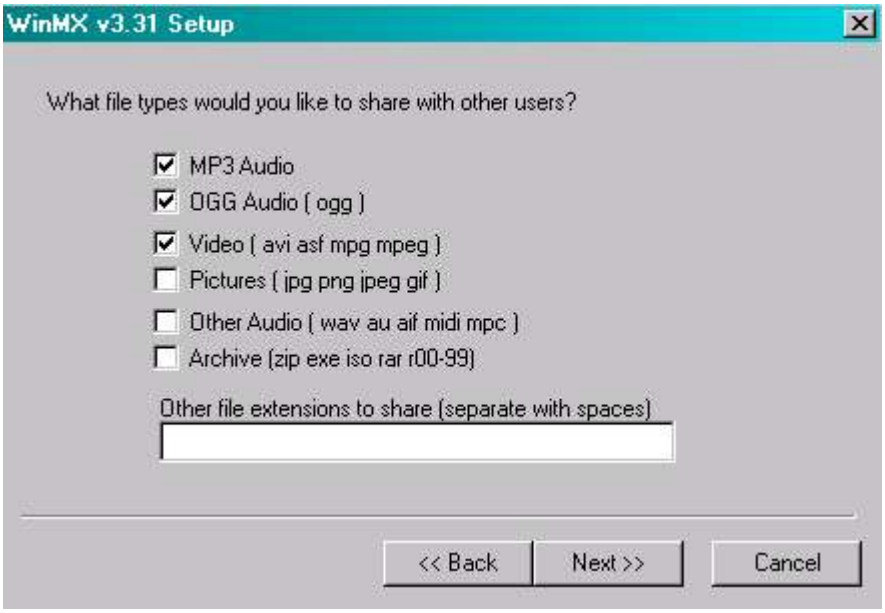
Weitere Informationen zu Kazaa findet man unter [KA03]

3.3. WinMX 3.31

WinMX ist ein weiteres bekanntes File-Sharing-Programm mit eigenem dezentralen Netzwerk. WinMX ist frei von Ad- und Spyware.

Während der Installation wird das Freigabeverzeichnis abgefragt. Dabei wird standardmäßig 'Eigene Dateien\My Music\' vorgeschlagen, wovon abzuraten ist. Wünschenswert wäre ein eigenes leeres Verzeichnis, dass bei der Installation als Unterverzeichnis angelegt wird.

Weiterhin muss man die Dateitypen angeben, die man freigeben möchte. So sind MP3, *.ogg sowie avi, mpg und mpeg vorgegeben. Weiter Formate kann man wählen oder direkt angeben. Dieses Feature wäre auch für andere File-Sharing-Systeme wünschenswert, da so wenigstens eine gewisse Kontrolle auf Dateibasis möglich ist.



WinMX hat auch ein Chatsystem, dass standardmäßig gut gegen Spam geschützt ist. So werden Nachrichten nur von Freunden und Nutzern,

bei denen man hoch- oder herunterlädt zugelassen.
Freigegebene Dateien werden zu ihrem Verzeichnis gehörend angezeigt. Es gibt keinen internen Virenscanner oder ein Kreditpunktesystem in WinMX.

Zusammenfassung:
WinMX kommt ohne Authentifizierungsmechanismen aus und testet keine Datenintegrität nach dem herunterladen. Es ist also nicht sichergestellt, dass die Daten unverändert angekommen sind. Nachteilig ist, dass man die definierbaren Dateifilter nur sehr schwer im Menü wiederfinden kann, so dass eine schärfere Einschränkung schwerfällt.

3.4. Freenet-Projekt

Das Freenet-Projekt hat es sich zum Ziel gemacht Dateien anonym tauschen zu können. Es ist ein dezentrales System, dass niemand kontrolliert – auch nicht die Programmierer.
Um die Authentizität von Dateien sicherzustellen, werden kryptographische Methoden zur Schlüsselerstellung angewandt. Die Dateien werden selbständig im Netz verbreitet, ohne dass andere User diese herunterladen. Das oberste Ziel vom Freenet-Projekt ist die Anonymität. Freenet ist ein Javaplugin für den Browser, über den dann die Kommunikation läuft. Zu Beginn ist das System sehr langsam, was sich aber durch einen langen Betrieb bessern soll.
Die Anonymität in Freenet wird gewährleistet, indem jeder Client als Proxy für andere Knoten dient. Selbst wenn man herausfindet, dass ein Nutzer Daten zu einer bestimmten Datei angefordert hat, weiß man noch nicht, ob er nicht als Proxy für einen anderen Nutzer gedient hat.
Es gibt keinen Suchalgorithmus, der das Suchen nach Dateien ermöglicht. Es soll unmöglich sein, herauszufinden, wo Dateien gespeichert sind. Eine Dateiauswahl erfolgt nur über Keys, womit eine Suchefunktion sehr schwer fällt.
Ein Beispiel für eine Datei die auf Webseiten im Freenet zu finden ist:

Diese Datei wurde von einem Author per Webinterface eingetragen und steht zum herunterladen bereit. Fügt man diesen Schlüssel jetzt hinzu, wird die Datei von anderen Knoten angefordert. Über einen „Hops to Live“ Faktor wird bestimmt wie tief die Anfrage gehen soll. Im Obigen Beispiel wurde mit 15 Hops kein Ergebnis erzielt.
Die Schlüssel dienen dazu, dass ein Nutzer nicht weiß, welche Daten er gerade hostet. Er könnte zwar bekannte Schlüssel mit denen auf seinem PC abgleichen, aber es kann von keinem Nutzer verlangt werden, dass er ständig die Schlüssel abgleicht. So wird versucht die Legalität des Nutzers zu sichern, da dieser nicht für den Inhalt verantwortlich gemacht werden kann. Schließlich weiß er nicht, welche Daten er auf der Festplatte hat. Er weiß es nur von den Daten, die er selbst mit bekanntem Schlüssel heruntergeladen hat.
Wenn man eine Datei anbieten möchte, muss man den Publisher-Key bekannt machen. Dazu gibt es mehrere Möglichkeiten. So kann man über Web Interfaces den Key mit einer Beschreibung dazu hinterlegen. Durch die Web Interfaces ist die Anonymität weiter gewährleistet. Man kann sie auch im IRC-Netzwerk verteilen, wobei man dabei wieder die IP des Nutzers herausfinden kann.

Zusammenfassung:

Das Freenet-Projekt ist ein Peer-to-Peer Netzwerk, dass besonderen Wert auf Anonymität legt. Die Performance des Systems ist zweitrangig – so die Ersteller. Leider ist es gerade für Neueinsteiger in diesem Netz frustrierend, wenn man umständlich nach Dateien

suchen muss und der Seitenaufbau sehr schleppend vorangeht. Für den Nutzer ist es kaum möglich herauszufinden, welche Dateien er gerade weiterleitet oder hostet. Weiterhin kann man dem Nutzer nicht nachweisen, dass er bestimmte Dateien heruntergeladen hat, da er Dateien auch weiterleitet.
Es gibt keinen Virenscanner bei diesem Projekt um Daten auf Viren zu überprüfen.
Somit ist es den Erstellern gelungen ein anonymes, aber langsames und umständliches Peer-to-Peer Netzwerk zu erschaffen.
Bei Fragen zu diesem Projekt sei auf [FN03] verwiesen.

4. Aktuelle Sicherheitsprobleme in P2P-File-Sharing Systemen

Die Nutzung von P2P File-Sharing Systemen bringt verschiedene Sicherheitsprobleme auf, die es so auch im 'normalen' Internet gibt.

4.1. Hauptprobleme

- ***Unbeabsichtigtes Sharen von persönlichen Informationen:***

Peer-to-Peer Systeme ermöglichen, oftmals viel zu einfach, das Tauschen von persönlichen Daten. So haben Studien von Good und Krekelberg [GK02] mehrere Beispiele bei Kazaa-Nutzern festgestellt, die persönliche Daten wie Steuererklärungen, Emailpostfächer oder Abrechnungen freigegeben hatten. Dadurch geben diese Nutzer Informationen an Millionen Nutzer weiter, die sie sonst niemandem freiwillig erzählen würden.
Häufig gibt man persönliche Informationen aufgrund einer falschen Konfiguration der Software frei. So wird bei den meisten File-Sharing Programmen ein Ordner freigegeben, womit dann alle Dateien in diesem Ordner freigegeben sind! Unerfahrene Nutzer haben nur einen Download-Ordner für alle Daten aus dem Internet. So teilen sie alle Daten, die sie herunterladen, gleich mit Millionen von anderen Nutzern, solange keine Schritte unternommen werden, um das Tauschen zu unterbinden.
Manche Systeme sind auf "maximales Tauschen" ausgelegt und raten dem Nutzer mehrere Ordner freizugeben um bei eigenen Downloads eine höhere Priorität zu

bekommen.
Viele Systeme erfahren regelmäßige Updates, die eine falsche Konfiguration erschweren. So war es in den ersten Versionen von Kazaa mit einem Klick möglich die gesamte Festplatte freizugeben. Heute wird erst noch ein Popupfenster erzeugt, in dem darauf hingewiesen wird, dass alle Dateien auf dieser Festplatte freigegeben werden. Die Software schlägt dann vor die Festplatte nicht freizugeben, hat aber dennoch den "Freigeben" Button als Default.
Tagebücher, persönliche Briefe oder finanzielle Unterlagen werden gelegentlich in Peer-to-Peer Netzwerken gefunden. Einmal veröffentlicht, können diese Dokumente für Betrug, eindringen in die Privatsspähre oder gar Idenditätsdiebstahl genutzt werden.

- ***Spyware und Adware***

Spyware ist eine Software, die ohne das Wissen des Nutzers Informationen über den Nutzer sammelt, und diese an dritte versendet. Manche File-Sharing Systeme wie Kazaa installieren Spyware auf dem Rechner des Nutzers ohne diesen darüber zu informieren. Diese übermitteln unter Umständen private Daten an dritte ohne das Wissen des Nutzers. Ein Hauptproblem von Spyware ist, dass sie nur schwer erkannt und entfernt werden kann.

Beispiele für Spyware:

"W32.Dlder.Trojan"

Ein Trojaner, der besuchte Webseiten speichert und diese an dritte weitersendet. "W32.Dlder.Trojan" wurde in früheren Versionen von File-Sharing Systemen wie Kazaa oder LimeWire gefunden. [DM]

"vx2.dll"

Dieses Spywareprogramm kam mit verschiedenen Versionen von Audiogalaxy und sammelte ebenfalls Informationen über besuchte Webseiten, erstellte Werbepopups und sammelte sogar die Informationen, die Nutzer in Webformulare eingegeben hatten. [BJ]

"Gator"

Das dominierende Programm des Werbevermarkters Gator beruht auf dem Anzeigenverbreitungssystem GAIN (Gator Advertising and Information Network). Dessen

Türöffner schleicht sich mehr oder weniger heimlich im Gefolge zahlreicher Gratis-Downloads aus dem Web auf PC-Festplatten, um anschließend tröpfchenweise die Bausteine eines Reklameroboters von den Gator-Servern nachzuladen. Hat der Hintergrundprozess "Trickler" seine Aufgabe erfüllt, sammelt der Gator-Roboter Informationen über die Surf-Gewohnheiten des PC-Benutzers und bombardiert diesen mit Popup- und Werbebannern. [GT03].
Gator hebt sich von anderer Spyware dadurch ab, dass es bei Besuchen von Webseiten Banner von konkurrierenden Webseiten platziert. So kann es vorkommen, dass man auf der Seite von Ford surft und Werbebanner von Toyota bekommt. Aufgrund dieser Technik wurde Gator auch schon mehrere male verklagt. Bisher konnten sich die Gator-Betreiber aber immer außergerichtlich einigen.

Da sich Spyware immer heimlich installiert und agiert, hat der Nutzer kaum die Möglichkeit festzustellen, ob er von Spyware "befallen" ist, oder ob die Webseite selbst diesen Pop-up-Banner geöffnet hat.
Man kann Spyware nur entgegenwirken, wenn der Nutzer über jede Software, die installiert wird, informiert ist. Auch darf kein Zwang bestehen Spyware zu installieren, um Peer-to-Peer Systeme zu nutzen.

- ***Sicherheitsprobleme:***

Nutzer von Peer-to-Peer Netzwerken sehen sich mit den gleichen Sicherheitsproblemen wie 'normale' Internetnutzer konfrontiert. Wie bei anderen Anwendungen müssen Peer-to-Peer Nutzer darauf achten nur Programme zu starten, deren Ursprung sie kennen und dem sie vertrauen. Derzeit sind Peer-to-Peer Systeme genauso (un)sicher wie andere Internetanwendungen auf dem Markt.

Viren und Würmer:

Da Peer-to-Peer File-Sharing Systeme es erlauben Daten an Millionen andere Nutzer zu verteilen - von denen die meisten Nutzer blutige Anfänger sind - gibt es ständig die Gefahr, dass Dateien aus den Peer-to-Peer Netzen Viren oder Würmer enthalten.
Natürlich ist es auch möglich gefährliche Dateien per Email zu erhalten. Den besten

Schutz gegen Viren bietet nach wie vor Antivirensoftware mit aktuellen Virendefinitionen. Aber auch eine Antivirensoftware kann nie 100%-igen Schutz bieten.

Onlineattacken:

Sobald man sich in ein Peer-to-Peer Netzwerk einklinkt, können andere Nutzer die IP Adresse (Internet Protokoll) des Nutzers herausfinden. Dann können Hacker mit Portscans, unter Ausnutzung von Windowsfehlern, die Kontrolle über den PC erlangen.
Diese Gefahr besteht aber nicht nur bei Peer-to-Peer Systemen, sondern bei allen Onlineaktivitäten, die auf IP basieren. Ein wirksamer Schutz hiergegen ist ein Proxy, der als Firewall fungiert.

"Self-Help" Attacken:

Eine neue Form der Sicherheitsverletzung für Peer-to-Peer Nutzer sind "Self-Help" Techniken. Dabei wird eine gefälschte Originaldatei freigegeben, die sich andere Nutzer, in dem Irrglauben das Original herunterzuladen, auf ihren PC laden. Diese Art ist nicht illegal, da sie keinen Schaden am PC oder Netzwerk des Nutzers anrichtet. Allerdings verschwendet der Nutzer viel Zeit und Geld, um diese Fakes herunterzuladen. Diese Form wird mehr und mehr von Musiklabels eingesetzt, die Lieder in Peer-to-Peer Systemen zur Verfügung stellen, die genauso lang sind wie das Original, nur dass innerhalb dieses Songs eine bestimmte Stelle im Lied mehrfach abgespielt wird. So hält es auch einem kurzen Check in einem Musikprogramm stand. Erst wenn man das Lied komplett abspielt, kann man die Schleife oder andere Störungen mitbekommen.
Es gibt aber auch schon aggressivere Methoden dieser Art, die Dateien löschen oder den Netzverkehr verlangsamen. Diese Praktiken sind derzeit noch illegal, aber es wird darüber nachgedacht solche Attacken zuzulassen. [SAR03]
Bei dieser brutalen Methode können PCs die Arbeit verweigern und unerfahrene PC-Nutzer irritieren.

- ***Juristische Probleme:***

Viele Dateien, die im Internet getauscht werden, fallen unter ein Copyright. Damit machen sich Nutzer strafbar, wenn sie die Dateien herunterladen oder zur Verfügung stellen. Durch das neue "Gesetz zur Regelung des Urheberrechts in der

Informationsgesellschaft" wurde selbst die Privatkopie stark eingeschränkt.
Nutzer die dagegen verstoßen, riskieren Anklagen, die bis zur Freiheitsstrafe reichen. Die Identität des Nutzers ist derzeit relativ leicht herauszufinden. Man benötigt lediglich die IP-Adresse des Nutzers, um dann vom ISP die Adresse des Nutzers zu bekommen - der Nutzer selbst bekommt von dieser Anfrage nichts mit. Erst wenn die Beamten vor der Tür stehen, wird er mit seiner Straftat konfrontiert.
Darum sollten Nutzer nur legale Dateien tauschen und verantwortungsvoll handeln.
Die Filmindustrie hat mit (umstrittener) öffentlicher Aufklärungsarbeit zum Thema Copyright begonnen. Darin werden Copyrightverletzer angeprangert, und es wird mit Freiheitsstrafen von bis zu drei Jahren gedroht. Diese Strafen erwarten aber nur Nutzer, die copyrightgeschütztes Material weiterverkaufen. Diese Feinheiten werden in den Spots absichtlich verschwiegen.
Mit diesen Risiken kommen aber auch Vorteile. So kann man freie Dateien problemlos tauschen. Die Technologie des P2P wird in immer mehr Bereichen verwendet. (z.B. das verteilte Rechnen von wissenschaftlichen Aufgaben - wie Primzahltests). Diese Software durch das Gesetz einzuschränken, ohne genau über die Konsequenzen nachzudenken, wäre nicht verantwortbar.

4.2. Vorschläge für sichere File-Sharing Systeme

1. ***Man sollte andere Nutzer über die Gefahren des File-Sharing informieren.***
   Viele Nutzer verstehen nicht genug von PCs um die Gefahren selbst zu erkennen, die sich durch die Nutzung von P2P Software ergeben kann. Solchen Menschen muss man Tipps geben wie sie diese Software sicher einsetzen können. Auch müssen die Nutzer verstehen lernen, dass Autorenrechte ein schützenswertes Gut sind.
2. ***Mehr Informationen über die File-Sharing Software.***
   Es sollte mehr Transparenz herrschen bei der Kontrolle über die freigegebenen Dateien. Spyware sollte komplett aus File-Sharing Systemen verschwinden, und man sollte informiert werden, wann Daten an dritte übermittelt werden. Dazu wäre zertifizierte Software nützlich, da PC-Nutzer im Allgemeinen die Korrektheit von Programmen nicht prüfen können.
   Unter keinen Umständen sollte es möglich sein mit Programmen aus den File-Sharing Systemen Schaden am eigenen PC anzurichten, inklusive Copyrightverletzungen.

4.3. Tipps für sicheres File-Sharing

1. Kenne die Dateien, die du freigegeben hast.
   Millionen von Nutzer können auf diese Daten zugreifen, also entscheide genau, welche Dateien freigegeben werden sollen. Beobachte also regelmäßig welche Daten freigegeben sind - vor allem wenn mehrere Leute den PC nutzen.
2. Sei vorsichtig mit Dateien, die du heruntergeladen hast.
   Heruntergeladene Dateien können Viren, Würmern oder Trojaner beinhalten. Überprüfe heruntergeladene Dateien immer mit einer aktuellen Antivirensoftware .
3. Nutze Sicherheitstools.
   Es gibt bereits eine Menge von Sicherheitstools, die die Sicherheit in Peer-to-Peer Netzen steigern und weitere werden entwickelt. Diese Tools beinhalten Firewalls, Spyware-Removal-Tools oder neuere File-Sharing Versionen mit **weniger** Sicherheitslücken.
4. Nur legale Dateien freigeben.
   Das Freigeben von copyrightgeschützten Dateien kann schnell zu juristischen Problemen führen. Darum sollten Peer-to-Peer Nutzer ständig darauf achten nur legale Dateien zu tauschen.
5. Achte auf Spyware
   Manche File-Sharingprogramme installieren heimlich Spyware, die den Nutzer auspioniert und Werbepopups öffnet. Wenn man den Verdacht hat Spyware auf dem Rechner installiert zu haben, so nutzt man eines der vielen Anti-Spyware-Tools aus dem Internet.
6. Sprich mit anderen Nutzern
   Alle Nutzer, die mit Peer-to-Peer Systemen in Kontakt treten, müssen über diese Sicherheitstips Bescheid wissen, damit sein PC dauerhaft sicher und legal bleibt.

5. Weiterentwicklungen

5.1. Vorschläge zur Annäherung von Peer-to-Peer Systemen an Security und Privacy

Peer-to-Peer File-Sharing Systeme mit Gesetzen zu regulieren, ist schwierig und kaum sinnvoll. Peer-to-Peer Systeme entwickeln sich immer weiter hin zu Systemen mit verschlüsselten Daten, anonymen Clients, rotierenden Ports und gesplitteten Dateien, was es sehr schwer macht Peer-to-Peer Traffic zu isolieren.

In den meisten File-Sharing Systemen hat der Nutzer die Kontrolle über die Software. Er entscheidet, welche Daten freigegeben werden und welche nicht. Damit ist der wichtigste Punkt die Aufklärungsarbeit bei den Nutzern über die möglichen Sicherheitsrisiken. Sie müssen erfahren wie sie sich selbst schützen, und welche Software ihren Sicherheitsansprüchen genügt.

Diese Anforderungen genügen nicht für kommerzielle Anwendungen. Hier spielen Authentifizierung und Rechteverwaltung eine wichtige Rolle.

5.2. Digital Rights Management (DRM)

Sobald Unternehmen digitale Werke bereitstellen, bedeutet dies für sie den vollständigen Kontrollverlust über diese Werke. Das heißt, Art- und Umfang der Nutzung sowie das „Ob“- und „Wie“ der Vervielfältigung ihrer digitalen Werke.

Ein Grund dafür sind die File-Sharing-Systeme.

Das Ziel der Unternehmen ist es, dass unerlaubte Vervielfältigen, Verbreiten oder Nutzen ihrer Werke zu unterbinden. Das heißt die (Rück-) Erlangung der vollständigen Kontrolle über ihre digitalen Inhalte.

DRM ist das Instrument mit dem die Unternehmen der Theorie nach bis ins letzte Detail festlegen können:

- ob ein Nutzer das digitale Werk nutzen darf
- in welchem Umfang er das Werk nutzen kann (wie viel er sehen oder hören darf)
- wie weit das Werk verbreitet werden und weitergegeben werden kann

und das DRM soll dem Unternehmen auch nach der Veröffentlichung die Möglichkeit geben diese Verarbeitungsbeschränkungen zu verändern.

Dabei wird sich dann zeigen, wie die Konsumenten auf diese nachträgliche Änderung an ihrem erworbenen Werk reagieren werden. So wird es sicher Proteste geben, wenn beim

Kauf einer DVD die einmalige Sicherheitskopie erlaubt ist, und zwei Monate nach dem Kauf diese revidiert wird.
DRM wird sowohl in Hardware, als auch in Software umgesetzt. So gibt es bereits heute Hardwarekomponenten, die für DRM ausgelegt sind. Weiterhin wird in on- und offline Methoden unterschieden. Ein Beispiel für Online Verfahren wäre der Windows Mediaplayer, der es ermöglichen wird eine Lizenz für Titel zu erwerben, damit man diese abspielen kann. So dürften Videos und Musikdaten gefahrlos getauscht werden, da sie sich nur abspielen lassen, wenn man die Lizenz dazu besitzt.
Eine Offlinemethode wäre Adobe Acrobat zum Bearbeiten von PDF-Dokumenten. Hier kann man bereits steuern, ob der Nutzer das Dokument bearbeiten, drucken oder teilweise kopieren darf.
Ein globales Verfahren für DRM ist Palladium.
Palladium wird voraussichtlich auf der Hardwarelösung aufbauen und als systemweite sichere Schnittstelle dienen, auf die individuelle Software zugreifen kann.
Wird z.B. versucht ein Kopierschutz einer Datei zu umgehen, wird diese Datei gesperrt und die ID des Nutzers wird an den Lizenzserver geschickt. Dort wird der Nutzer auf eine Blacklist gesetzt, was ihm zukünftige Zugriffe auf die Datei verwehrt.
Letztenendes wird der Nutzer nicht die Wahre sondern die Lizenz zum Nutzen erwerben. Das heißt, dass ein Musiktitel kopiert werden kann und soll, da die Verteilung an die Endkunden so viel schneller erfolgen kann, als mit den heutigen Vertriebswegen. Wenn sich ein anderer Nutzer diese Musikdatei heruntergeladen hat, muss er sich erst die Lizenz kaufen, damit er diese Datei nutzen kann. Theoretisch könnten die Titel so billiger werden, da es für die Firmen billiger wird die Titel zu verteilen. Auch ein Bonussystem ist denkbar, dass Nutzern Kredits gibt, wenn sie zur Verteilung der Werke beitragen.
Sobald jemand eine Datei modifiziert, stimmt die Signatur nicht mehr mit der Datei überein und die Datei wird ungültig. So lädt man sich nur Dateien herunter, die eine gültige Signatur haben und sicher vor Viren und Trojanern sind.
Juristisch gesehen wird es keine Probleme geben, da man die Lizenz vor dem Abspielen kaufen muss. Bereits heute wird vom Windows Media Center eine ID an eigene Aufnahmen angehängt, so dass eine Nutzung nur auf dem PC möglich ist, der diese Aufnahme erstellt hat.
DRM versucht also nicht die Vervielfältigung zu verhindern, sondern die Nutzung ohne Lizenz. Die Unternehmen wollen sich den Effekt der schnellen globalen Verbreitung, den

die File-Sharing-Systeme bieten, zunutze machen.
Palladium wird das erste DRM-System sein, dass weltweit installiert werden wird, da es mit der nächsten Windowsdistribution ausgeliefert werden wird. Zwar soll es freiwillig sein, dieses zu nutzen, aber da die meisten Unternehmen davon Gebrauch machen werden, ist es nur eine Frage der Zeit, bis auch die Nutzer dieses System aktivieren um bestimmte Produkte nutzen zu können.
Mircosoft wird damit das Monopol für die Lizenzserver besitzen.
Da Microsoft kaum an Open-Source interessiert ist, wird es wahrscheinlich kein kompatibles DRM-System für Linux geben, so dass sich Linuxnutzer Microsoftprodukte kaufen müssen, um bestimmte Musiktitel anhören zu können.
Mit der Nutzung von DRM-Systemen in Peer-to-Peer Netzwerken werden einige der bekannten Sicherheitsprobleme verschwinden.

5.3. Zertifizierte Software

In Zukunft wird jede Software mit einem Zertifikat des Herstellers ausgestattet sein, so dass der Nutzer anhand des Zertifikates entscheiden kann, ob er diese installieren möchte. Wenn also Kazaa mit Spyware zusammen installiert werden will, müsste man zwei Zertifikate akzeptieren. So wird der Nutzer eine bessere Kontrolle über die auf dem PC installierte Software bekommen. Es könnte sogar sinnvoll sein, dass man nur zertifizierte Software installieren darf. Das bringt allerdings Nachteile mit sich. So können keine selbst geschriebene Programme ausgeführt werden oder alte nicht zertifizierte Software ist nicht mehr lauffähig.

5.4. Sonstige Entwicklungen

Unter Peer-to-Peer Systemen wird man in Zukunft nicht nur File-Sharing-Systeme verstehen, denn es wird ganz neue Arten von Peer-to-Peer-Systemen geben, sobald die Wirtschaft herausgefunden hat, wie sie diese gewinnbringend nutzen kann.
So sind Systeme denkbar, die einem Rechenkapazitäten zur Verfügung stellen.
Auch Systeme zur verteilten Datenspeicherung mit Redundanz sind denkbar, dazu Anfragen an solche Datenbanken mit Schemaintegration in Echtzeit. Das heißt Überwindung der strukturellen Heterogenität und Integration verschiedener lokaler

Schemata in ein gemeinsames globales Datenschema.
Die Authentifikation und Nichtabstreitbarkeit spielen eine wichtige Rolle. Nur wenn beide Partner sicher sein können, dass sie mit dem richtigen Kommunikationspartner verbunden sind, kann der Service starten.
Ein Nachweis der Leistungserbringung muss auch im Nachhinein problemlos möglich sein, damit die Kunden die Rechnungen weiterleiten können. Es muss also über Peer-to-Peer Netze mit Zertifikaten geregelt werden, dass jeder Nutzer, oder auch eine Nutzergruppe (Firma) durch ein eindeutiges Zertifikat erkennbar ist.
Das Angebot der copyrightgeschützen Dateien in File-Sharing-Systemen wird immer geringer werden, da es nur noch möglich sein wird, Werke mit gültiger Lizenz zu nutzen.
Das Problem der Viren und Trojaner lässt sich durch DRM verringern, wenn nicht sogar vollständig aus den Peer-to-Peer Netzwerken bannen.
.

5.5. Zertifikate und Signaturen

Ein Zertifikat ist eine Sammlung von Information zur Identifikation des Clients bzw. Servers. Ein Zertifikat enthält unter anderem den Domainnamen für den das Zertifikat ausgestellt wurde, eine Beschreibung des Ortes an dem sich der Client/Server befindet und Informationen zur verwendeten Kryptographie und deren Schlüssel und Signaturen.
Die Signaturen selbst beruhen auf den asymmetrischen Verschlüsslungsverfahren. So wird von der Nachricht beim Sender ein Hashwert gebildet, welcher dann mit dem privaten Schlüssel des Senders verschlüsselt und an den Empfänger gesendet wird. Die Nachricht selbst wird unverschlüsselt verschickt.
Mit dem öffentlichen Schlüssel kann der Empfänger den Hashwert verifizieren. Die Zertifizierungsstellen sind dabei für die Schlüsselweitergabe zuständig. Dabei besteht noch immer das Problem, dass man den Schlüssel auf einem sicheren Weg zu der Zertifizierungsstelle bringen muss, da diese nicht sicher sein kann, dass der Schlüssel zu mir gehört und nicht zu einem Angreifer.
Die Verbreitung von Zertifikaten muss nicht unbedingt an eine Zertifizierungsauthorität gekoppelt sein (was dem dezentralisierten Peer-to-Peer Gedanken widersprechen würde). Die Zertifizierung von öffentlichen Schlüsseln bei Pretty Good Privacy (PGP) könnte mit dem Peer-to-Peer Konzept gekoppelt werden.

6. Literaturverzeichnis

[BJ]: Benner, Jeffrey. "Spyware, In A Galaxy Near You." Wired News. January 24, 2002. Available at http://www.wired.com/news/technology/0,1282,49960,00.html.

[DM]: Delio, Michelle. "What They Know Could Hurt You." Wired News. January 3, 2002. Available at http://www.wired.com/news/privacy/0,1848,49430,00.html

[EM03]: http://www.emule-project.net/files/eMule.1031.chm

[FN03]: http://www.freenetproject.org/index.php?page=faq

[GK02]: Good, Nathaniel S., and Aaron Krekelberg. "Usability and privacy: A study of Kazaa P2P file-sharing." June 2002. http://www.hpl.hp.com/shl/papers/kazaa/index.html

[GT03]: http://www.heise.de/newsticker/data/hps-23.10.03-000/

[KA03]: http://www.kazaa.com/us/index.htm

[SAR03]: Sorkin, Andrew Ross. "Software Bullet is Sought to Kill Music Piracy." The New York Times. May 4, 2003. Available at http://www.nytimes.com/2003/05/04/business/04musi.html?ex=1053001791&ei=1&en=8d9f2b1d372d373

[SM97]: Secure Computing with Java - Now and the Future. A White Paper, Sun Microsystems, October 1997