University of Zurich
Department of Informatics

Burkhard Stiller
Thomas Bocek
Fabio Hecht
Cristian Morariu
Peter Racz
Gregor Schaffrath
(Eds.)

Communication Systems II

TECHNICAL REPORT – No. ifi-2008.01

January 2008

University of Zurich
Department of Informatics (IFI)
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland

ifi

B. Stiller, T. Bocek, F. Hecht, C. Morariu, P. Racz, G. Schaffrath (Eds.):
Technical Report No. ifi-2008.01, January 2008
Communication Systems Group (CSG)
Department of Informatics (IFI)
University of Zurich
Binzmühlestrasse 14, CH-8050 Zurich, Switzerland
URL: http://www.csg.uzh.ch

Introduction

The Department of Informatics (IFI) of the University of Zürich, Switzerland works on research and teaching in the area of computer networks and communication systems. Communication systems include a wide range of topics and drive many research and development activities. Therefore, during the autumn term HS 2007 a new instance of the Communication Systems seminar has been prepared and students as well as supervisors worked on this topic.

The areas of communication systems include among others wired and wireless network technologies, various network protocols, network management, Quality-of-Service (QoS) provisioning, mobility, security aspects, peer-to-peer systems, multimedia communication, and manifold applications, determining important parts of future networks. Therefore, this year's seminar addressed such areas in more depth. The understanding and clear identification of problems in technical and organizational terms have been prepared and challenges as well as weaknesses of existing approaches have been addressed. All talks in this seminar provide a systematic approach to judge dedicated pieces of systems or proposals and their suitability.

Content

This new edition of the seminar entitled "Communication Systems II" discusses a number of selected topics in the area of computer networks and communication systems. The first talk on "P2P Storage Networks" gives a short overview on peer-to-peer networks and discusses distributed storage systems based on peer-to-peer technology. Talk two on "Ethernet Passive Optical Networks (EPON)" presents a new access network technology for high bandwidth network access. Talk three on "VPNs and Their P2P Alternative P2P@i" gives an overview on virtual private networks and presents an alternative solution based on peer-to-peer technology. "Web Services – Technology and Security" as talk four presents web services and discusses their security aspects. Finally, talk five on "BioLANCC und die Datenschutzgesetze" investigates data protection laws in the context of biometric systems.

Seminar Operation

Based on well-developed experiences of former seminars, held in different academic environments, all interested students worked on an initially offered set of papers and book chapters. Those relate to the topic titles as presented in the Table of Content below. They prepared a written essay as a clearly focused presentation, an evaluation, and a summary of those topics. Each of these essays is included in this technical report as a separate section and allows for an overview on important areas of concern, technology architectures and functionality, sometimes business models in operation, and problems encountered.

In addition, every group of students prepared a slide presentation of approximately 45 minutes to present its findings and summaries to the audience of students attending the seminar and other interested students, research assistants, and professors. Following a general question and answer phase, a student-lead discussion debated open issues and critical statements with the audience.

Local IFI support for preparing talks, reports, and their preparation by students had been granted by Thomas Bocek, Fabio Hecht, Cristian Morariu, Peter Racz, Gregor Schaffrath, and Burkhard Stiller. In particular, many thanks are addressed to Peter Racz for his strong commitment on getting this technical report ready and quickly published. A larger number of pre-presentation discussions have provided valuable insights in the emerging and moving field of communication systems, both for all groups of students and supervisors. Many thanks to all people contributing to the success of this event, which has happened in a lively group of highly motivated and technically qualified students and people.

Zürich, January 2008

Contents

Kapitel 1

P2P Storage Networks

Raphael Blatter

Peer-to-Peer ist ein Netzwerk, in welchem alle partizipierenden Geräte gleichberechtigt, also sowohl Konsument wie auch Anbieter sind. P2P kann zwischen Computern allgemein oder auch zwischen Servern stattfinden. Der Schlüssel zu einem erfolgreichen P2P-Netzwerk ist die Schaffung von Redundanz gegen die Unzuverlässigkeit einzelner Mitglieder. Die P2P-Technologie kann auch zum verteilten Speichernetze benutzt werde, sowohl als File Sharing-Netze, wie auch als Permanent Storage Netzwerke. Dies sind nur zwei mögliche Anwendungen, auch private P2P-Netzwerke sind möglich, als Collaboration-Lösung. Das Ziel dieser Arbeit besteht darin, einen Überblick über bestehende Konzepte wie auch über vorhandene theoretische Ansätze zu geben. Dabei sollen vor allem Aspekte der Sicherheit wie auch der Incentives genauer angeschaut werden. Je nach Ziel des P2P Storage Networks sind zur Aufrechterhaltung der Sicherheit die Verschlüsselung oder das Signieren von Dateien, oder Reputationssysteme notwendig. Für ein sinnvolles Reputationssystem müssen immer auch Pseudonyme verwaltet werden. Auch gegen DDoS-Angriffe muss vorgesorgt werden, zum Beispiel mit Nonfungible Micropayments oder guten Algorithmen. Die Konsistenz wichtiger Daten wird vor allem durch Signaturen und die Fragmentierung der Daten mithilfe eines Secret Sharing Algorithmus sichergestellt. Mit geeigneten Incentives muss verhindert werden, dass Personen Leistungen benutzen, ohne selber solche anzubieten. Dies wird mit dem direkten Tausch von Leistungen, mit transitiv wirksamen Micropayments oder mit monatlichen Bezahlungen erreicht. Mit den repräsentativen Beispielen Freenet, Free Haven, OceanStore, Tahoe und Bittorrent wird der Einsatz der genannten Konzepte gezeigt.

Inhaltsverzeichnis

1.1 P2P – die Gedanken hinter der Technologie

In diesem Kapitel wird gezeigt, was ein Peer-to-Peer Netzwerk ausmacht. Es werden verschiedene Arten vorgestellt, wie die P2P-Technologie auch praktisch umgesetzt wird, vor allem auch welche Konzepte grundsätzlich existieren, um P2P für die verteilte Speicherung von Dateien zu verwenden. Die unterschiedlichen Ziele verschiedener Konzepte werden analysiert, was einen Einfluss auf die zu verwendenden Technologien hat. Am Schluss des Kapitels wird die Redundanz, der Schlüssel zur erfolgreichen Speicherung von Dateien, diskutiert.

1.1.1 Von Client/Server zu P2P

Die Unterschiede zwischen dem gängigen Client/Server Modell und der beschriebenen P2P-Technologie werden in diesem Kapitel genauer beschrieben. Vor allem gezeigt wird, welchen Einfluss Peer-to-Peer auf die Zukunft der aktuellen Client/Server Konzepte hat.

1.1.1.1 P2P Geschichte

Seit dem Jahr 2000 ist der Begriff Peer-to-Peer weit verbreitet [18]. Im Folgenden werden die Vor- und Nachteile von P2P gegenüber der klassichen Client/Server-Architektur gezeigt.

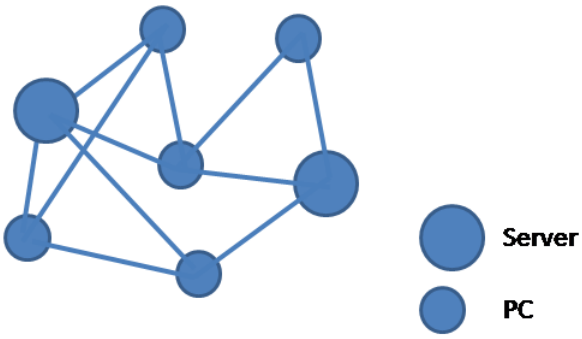


Abbildung 1.1: P2P-Architektur

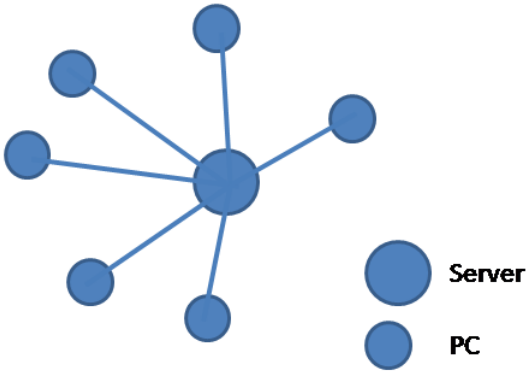


Abbildung 1.2: Client/Server-Architektur

P2P ist ein neuer Begriff, beschreibt aber genauso gut das ursprüngliche Konzept des Internets [18][15]. Das Internet wurde als dezentralisiertes Netzwerk geplant, in dem alle angeschlossenen Geräte Daten (und später auch Dienste) sowohl in Anspruch nehmen wie auch anbieten. Wie Abbildung 1.1 zeigt, sind zusammenarbeitende Geräte direkt miteinander verbunden. Alle Geräte waren gleichberechtigt, um heutige Begriffe zu verwenden, sie waren sowohl Client wie auch Server. Schon bald, besonders im Laufe der Kommerzialisierung des Internets, wurden, wie Abbildung 1.2 zeigt, die Clients als reine Nutzer von Informationen und die Server als Anbieter von Informationen getrennt.

Obwohl sich die Funktionalität von Clients im Netzwerk grösstenteils auf den Konsum beschränkte, wurden sowohl die jeweilige Hardware wie auch die Verbindung immer leistungsstärker. Die P2P-Bewegung will dieses Potential nutzen, sei es freie Rechenleistung, wie zum Beispiel SETI@home [1], oder riesige Mengen von Speicherplatz, die sonst nie benutzt würden [19]. Die optimale Nutzung vorhandener Ressourcen ist mittlerweile nur noch ein Teilaspekt von P2P. Aus der verteilten Technologie ergeben sich viele weitere Vorteile wie eine sicherere Lagerung von Daten, bessere Verfügbarkeit und kürzere Transportwege der Daten von der Quelle zum Ziel.

1.1.1.2 Die Stärken von P2P liegen in der Kombination mit der Client/Server-Architektur

Die Vorteile von P2P kommen jedoch nicht automatisch mit dem Design einer P2P-Architektur, sondern sie müssen geplant und systematisch umgesetzt werden. In dieser Arbeit geht es darum, wie man die Vorteile nutzen und die Nachteile minimieren kann. Der Blickwinkel soll aufgrund des Umfangs auf Themen der Sicherheit und der Incentives beschränkt sein. Allgemein gilt zu den Eigenschaften von P2P, wie Dingledine, Freedman und Molnar geschrieben haben:

> Being Peer-to-Peer doesn't make the problems go away. It just makes the problems different [7].

Genauso wenig wie P2P ein Heilmittel gegen alle Probleme des Internets ist, ist ein System nach reinen P2P-Richtlinien als Ziel des heutigen Internets zu sehen. P2P wird die heutige Client/Server-Architektur des Internets nie ersetzen, sondern mit seinen Vorteilen ergänzen. Für viele Problemstellungen ist Client/Server nach wie vor die bessere Lösung [17]. Vor allem intern in Unternehmen, ist meistens ein gemischter Weg zu bevorzugen [21].

Wie sich auch in den Beispielen zeigen wird, sind reine dezentralisierte P2P-Systeme äusserst rar und haben häufig mehr einen theoretischen Hintergrund als einen praktischen. Schon der Klassiker unter den Filesharing-Programmen, Napster, basierte auf zentralen Servern als Vermittler [19]. Dies nicht, weil eine komplett dezentralisierte Architektur nicht möglich gewesen wäre, sondern weil es zu den Stärken des P2P auch die Stärken von zentralisierten Servern, nämlich das Suchen und Vermitteln von Kontakten, nutzen wollte.

1.1.2 Definition eines Peers

Zuerst soll eine Definition des englischen Wortes 'peer' betrachtet werden:

> A person who has equal standing with another or others, as in rank, class, or age [31]

Wenn im Zusammenhang mit Computern aus der obigen Definition das Wort *person* weggenommen wird, bleibt eine Lücke, die beliebig gefüllt werden kann. Es gibt ganz verschiedene Stufen von P2P, je nachdem welche Entität als Peer definiert wird. Während die klassischen Filesharing-Tools wie in Abbildung 1.3 vor allem einzelne Heimcomputer als Peers nehmen, ergibt sich bei Permanent Storage Networks ein P2P-System zwischen den Servern [8], wie Abbildung 1.4 zeigt, bei denen sich immer noch sowohl konsumierende wie auch produzierende Clients einloggen um das Netzwerk zu benutzen. Das ganze verteilte P2P-Netzwerk verhält sich für den Client wie ein einziger Server und wird auch auf diese Weise benutzt.

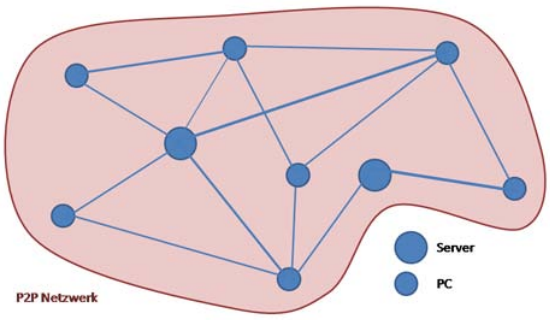


Abbildung 1.3: Heimcomputer als Peers

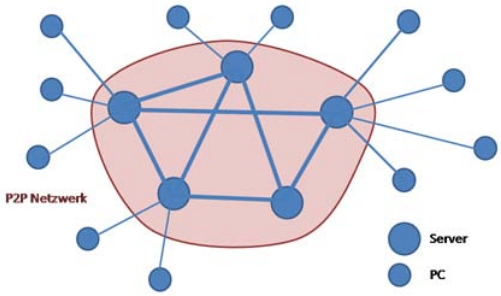


Abbildung 1.4: P2P zwischen den Servern

Je weiter die genauen Begrifflichkeiten untersucht werden, desto weniger klar werden die Grenzen zwischen unterschiedlichen Architekturen.

> P2P environment is inherently untrustworthy and unreliable [5].

Aussagen wie diese in einem Paper über Freenet sind auf der jeweiligen Stufe, in diesem Fall ein Netzwerk, in dem jeder privat kontrollierte Heimcomputer ein Peer darstellt, zu betrachten und machen in einem unternehmensinternen P2P Storage Network wenig Sinn. Dort sind die Peers keineswegs unzuverlässig, da alle Server unter der Kontrolle des Unternehmens sind.

1.1.3 Die Arten von P2P Storage Networks

Durch unterschiedliche Bedürfnisse betreffend Datenspeicherung ergeben sich auch unterschiedliche Ziele und somit unterschiedliche Lösungskonzepte. Werden verschiedene P2P-Systeme miteinander verglichen, so sind auch immer die jeweiligen Ziele des jeweiligen Netzwerkes zu betrachten. Ein Satz von Wiley zur Zusammenarbeit unterschiedlicher Systeme illustriert diesen Sachverhalt gut:

> You should not expect a free system such as Gnutella to understand a micropayment transaction or an anonymous system such as Freenet to understand user trust ratings [26].

Damit soll gezeigt werden, dass es nicht die optimale Lösung gibt, sondern die Systeme auf ganz anderen Zielsetzungen beruhen. Generell kann zwischen zwei grossen Gruppen unterschieden werden, die die Mehrzahl heutiger P2P Storage Network Lösungen ausmachen. Einerseits sind dies Konsumenten-zentrierte, andererseits Anbieter-zentrierte Systeme [26].

1.1.3.1 Konsumenten-zentrierte P2P-Netzwerke

Konsumenten-zentrierte Systeme sind vor allem die allgemein bekannten Filesharing-Applikationen, wie heute zum Beispiel Emule [29] oder BitTorrent [27]. Die Benutzer benutzen diese Netze, um einfach und schnell an Daten zu gelangen. Heute sind dies häufig Lieder, Software oder Filme, das System funktioniert aber genauso für Texte oder andere Informationen. Überlegungen zu rechtlichen oder moralischen Aspekten würden den Umfang der Arbeit sprengen. Wichtig dabei ist, dass hier die wenigsten ein Interesse daran haben, einmal publizierte Daten so lange wie möglich zur Verfügung zu stellen. Einige Firmen wie Redhat oder SUSE benutzen diese Kanäle zur Distribution ihrer Software [28], dies sind jedoch noch Ausnahmen.

In solchen Systemen bestimmt die Nachfrage alleine die Verfügbarkeit, dies wird aber mit unterschiedlichen Mechanismen geregelt. Es ergibt sich, dass die Speicherung unzuverlässig ist. Sobald ein Dokument nicht mehr nachgefragt wird, verschwindet es aus dem gemeinsamen Speicher. Wie Abbildung 1.5 zeigt, lässt sich ein klassisches Muster erkennen. Wenn die Datei neu eingestellt wird, erhöht sich die Nachfrage und somit auch das Angebot nach und nach bis zu einem Maximum, um dann wieder gegen Null zu sinken [6].

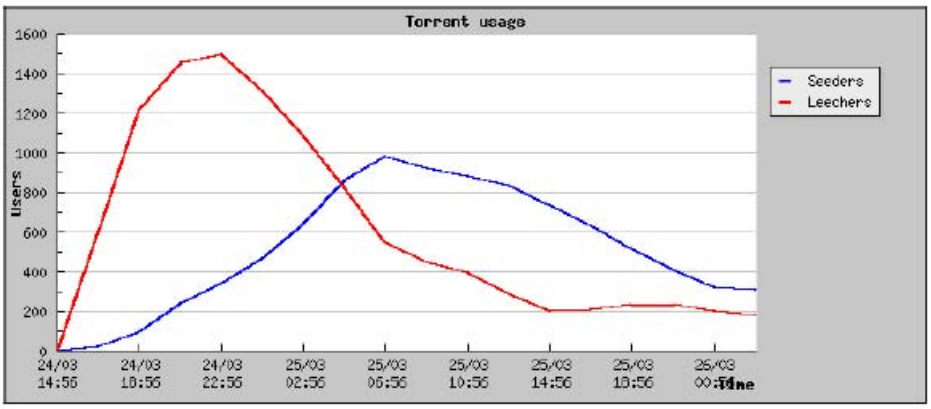


Abbildung 1.5: Leecher- (rot) und Seeder-Werte (blau) über die Zeit betreffend einer Datei [6]

1.1.3.2 Anbieter-zentrierte P2P-Netzwerke

Als Gegensatz dazu zeigen sich Anbieter-zentrierte Applikationen, wie sie im Gebiet von Permanent Storage Lösungen existieren. Hier haben die publizierenden Benutzer ein Interesse daran, ihre Daten im System zu behalten. Die Gründe dazu können sehr unter-

schiedlich sein, sei es um eine Information möglichst weit zu verbreiten, um Zensur zu umgehen oder auch einfach um persönliche Daten sicher zu speichern.

Daraus ergeben sich nicht nur vom wirtschaftlichen Standpunkt aus andere Ansätze, indem jetzt eine Bezahlung der Publikation und nicht mehr des Konsums nötig ist, sondern auch betreffend den zu verwendenden technischen Prinzipien. Die Speicherung der Daten muss zuverlässig sein und durch entsprechende Algorithmen garantiert werden. Die Kontrolle über die Verteilung der Daten muss von den Benutzern weg zur Software selbst übergeben werden.

1.1.3.3 P2P als Basistechnologie

P2P Storage Networks können zu ganz unterschiedlichen Zwecken benutzt werden. Peer-to-Peer ist nur die Technologie dahinter, dazu Bricklin:

> Peer-to-Peer is plumbing [3]

Die Technologie ist für ein breites Spektrum an Anwendungen einsetzbar, sie bietet nur die Grundlage für die Applikationen, die darauf aufbauen.

P2P kann neben den File Sharing und den Permanent Storage Tools auch zur Zusammenarbeit an Projekten benutzt werden. Da Projekte immer mehr über Unternehmensgrenzen hinweg stattfinden [21], erschwert sich das Management eines zentralen Servers zur Zusammenarbeit. Die Nutzung der P2P-Technologie erlaubt es, ohne einen externen Administrator hinzuzuziehen und Ressourcen zu organisieren [21], eine gemeinsame Datensammlung aufrechtzuerhalten. Natürlich sind in diesem System die Anforderungen anders als in den oben beschriebenen Möglichkeiten. Das P2P-Netzwerk beschränkt sich auf wenige Benutzer und der selektive Zugang zu den Daten wird zum zentralen Ziel. Beispiele dieser Gruppe sind die ursprüngliche Implementation von Groove [21] oder das weiter unten beschriebene Tahoe.

1.1.4 Redundanz als Schlüsselidee zur P2P-Technologie

In diesem Kapitel wird gezeigt, wie mithilfe von Redundanz die Zusammenarbeit von unzähligen unzuverlässig vorhandenen Computern ein Netzwerk zur zuverlässigen Speicherung von Daten benutzt werden kann. Im Gegensatz zu den File Sharing Programmen muss in Permanent Storage Networks die Redundanz aktiv gebildet werden.

1.1.4.1 Redundanz als Ersatz für Zuverlässigketi

Egal welche Ziele verfolgt werden, Redundanz ist ein Schlüsselkonzept der P2P-Technologie. Selbst wenn alle Peers unter einheitlicher Kontrolle sind (z.B. intern in einem Unternehmen), ist Redundanz absolut notwendig, um die Verfügbarkeit, wie aber auch minimale

Transportwege zu garantieren. Sind die Peers nicht unter zentraler Kontrolle, sondern in einem heterogenen Netzwerk wie dem Internet verteilt, wird Redundanz umso wichtiger, da die Computer, auf welchen die benötigten Dateien gespeichert sind, nicht nach Bedarf wieder ins Netzwerk integriert werden können. Hong bringt dies auf den Punkt:

> Peer-to Peer systems need to anticipate failures as ordinary, rather than extraordinary, occurrences [10].

Es gilt der Grundsatz, dass alle Peers prinzipiell unzuverlässig sind. Peers können häufig und ohne Vorwarnung verschwinden und später wieder auftauchen, oder auch nicht [5]. Das Schlüsselkonzept von P2P heisst:

> using redundancy to replace reliability [16]

Durch die grosse Redundanz im gesamten Netzwerk werden aus wenigen unzuverlässigen Computern ein grosses, zuverlässiges Gesamtsystem [1]. Wenn immer Computer mit gewissen Daten verschwinden, hat es sehr wahrscheinlich viele verbleibende Computer, die diese Information auch noch besitzen.

Redundanz ist jedoch nicht bloss nützlich, um die Verfügbarkeit aufgrund unzuverlässiger Systeme sicherzustellen. Redundanz in Anbieter-zentrierten Netzen, und nicht nur dort, dient auch dazu, böswilliges Löschen oder Manipulation der Informationen zu verhindern. Gelöschte Daten können durch Redundanz wiederhergestellt und manipulierte Daten erkannt werden [7].

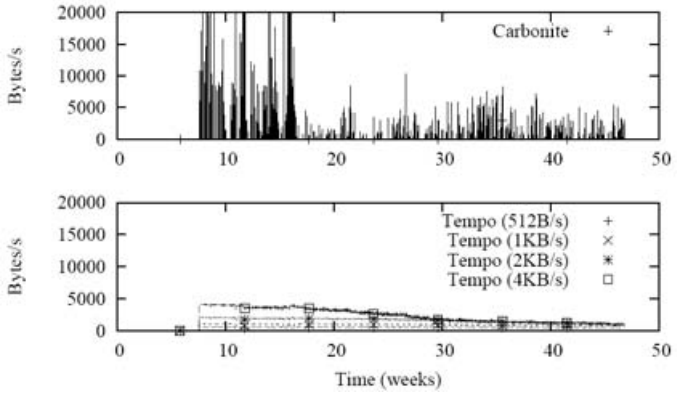
Auch erhöht eine verteilte Redundanz von Daten die Performance und senkt dabei die Transportwege und somit die Netzauslastung, indem die Redundanz ähnlich einem Cache benutzt wird [4].

1.1.4.2 Automatische Redundanzbildung

Während in Filesharing-Netzen die Redundanz automatisch mit der Nachfrage entsteht und Redundanz nicht mehr nötig ist, sobald die entsprechende Nachfrage nicht mehr vorhanden ist, muss in anderen Systemen, wo Zuverlässigkeit wichtig ist, die Redundanz aktiv erstellt, überwacht und korrigiert werden [20].

Die Generierung von optimaler Redundanz ist je nach Implementation vom Anbieter der Information bestimmt. Es gibt unterschiedliche Ansätze, reaktive Algorithmen, die nachdem ein Ausfall erkannt wurde sofort die fehlenden Daten neu verteilen, was optimal für den Speicherbedarf, jedoch schlecht für die Bandbreitebenutzung zu Spitzenzeiten ist, wie Abbildung 1.6 zeigt. Im Gegensatz dazu stehen proaktive Systeme, die permanent mit geringer Netzauslastung nötige Redundanzen erstellen, was keine temporär überlasteten Netze zur Folge hat, aber die Festplatten füllen kann [20].

Redundanzen sind für die Sicherheit eines P2P-Systems überaus wichtig. Je nach Zielen müssen speziell angepasste Lösungen konzipiert und umgesetzt werden.



[20]

Abbildung 1.6: Reaktive vs. proaktive Redundanzbildung

1.2 Beispiele

In diesem Kapitel werden fünf repräsentative Beispiele genauer analysiert. Die ausgewählten Beispiele enthalten eine Grosszahl von Konzept, die auch die unzähligen anderen P2P Storage Networks ausmachen.

1.2.1 Freenet

Freenet ist ein Dinosaurier der P2P-Technologie. Trotzdem soll diese Implementierung als erstes beschrieben werden, da sie einige sehr durchdachte Systeme aufweist und trotzdem vergleichsweise einfach ist.

Freenet ist komplett dezentralisiert [5]. Es gibt keine zentralen Server und alle Peers sind am Anfang gleichberechtigt, egal ob sie auf einem starken, permanent laufenden Server oder einem nur zeitweise verfügbaren PC sind. Die Teilnahme am Netz ist gratis [5].

Eine wichtige Eigenschaft von Freenet ist, dass es versucht, anonymen Zugang zu gewähren. Anfragen werden nach dem Prinzip einer *steepest-ascent hill-climbing search* über verschiedene Peers hinweg durchgeführt [5]. Jedes Peer auf dem Weg verschlüsselt die komplette Anfrage und schickt sie mit seinem eigenen Public Key weiter. Damit kann kein Peer auf dem Weg herausfinden, woher die Anfrage ursprünglich stammt [5]. Auf dem gleichen Weg werden die gefundenen Files mehrfach verschlüsselt wieder zurück geschickt [12].

Dateien werden nach ihrem Hash sortiert auf den unterschiedlichen Peers abgelegt und auch so wieder angefragt [5]. Auf jedem Peer wird ein Log geführt, wie oft eine Datei gelesen wurde. Häufig angefragte Dateien, die nicht auf diesem Peer gespeichert sind, werden nach einer Weile automatisch auf die eigene Harddisk kopiert, während wenig angefragte Dateien gelöscht werden [5].

Die Daten selbst werden mithilfe des Hash gesucht, was die Konsistenz garantiert. Falls die Daten geändert wurden, stimmt der Hash nicht mehr und die Datei reagiert nicht mehr auf die Anfrage [5].

Dies alles beinhaltet gemäss Kritikern einen grossen Schwachpunkt von Freenet. Die Priorisierung von Dateien erfolgt nach der Nachfrage, womit keinerlei langfristige Speichermöglichkeit garantiert wird [12]. Freenet ist für das Speichern von privaten Dateien ungeeignet, da sie bald gelöscht würden. Ein weiteres Problem von Freenet ist, dass es keinerlei Incentives bietet. Leute, die Speicherplatz zur Verfügung stellen, tun dies freiwillig und ohne Gegenleistung.

Da von den Peers dynamische Routing-Tabellen mit Peers, die erfolgreiche Antworten auf Anfragen gesendet haben, geführt werden, werden zuverlässige Peers, die lange Uptimes haben, in den Routing-Tabellen favorisiert und bilden nach einer Zeit eine Art automatisch generierter Backbone [5].

Freenet hat ein sehr gutes Konzept, ist aber mittlerweile mehr vom akademischen Standpunkt her interessant. Der Mangel an Garantien zur langfristigen Speicherung und das Fehlen der Incentives macht das System kaum einsetzbar, obwohl es immer noch einige der besten Konzepte hat, die P2P je umgesetzt hat.

1.2.2 Free Haven

Im Gegensatz zu Freenet will Free Haven die Persistenz der Daten garantieren [8]. Das System arbeitet ebenfalls anonym [8]. Während in Freenet die Peers auch von normalen PCs gebildet werden, basiert das P2P System in Free Haven auf einem Verbund von Servern, dem so genannten *servnet* [8].

Während der Signatur einer Datei wird einmalig ein Schlüsselpaar für diese spezifische Datei erstellt. Die Identifikation dieser Datei findet später über deren Public Key statt [8]. Dies garantiert die Konsistenz der Dateien. Ist eine Datei erst einmal auf dem Netz, kann sie auch vom Urheber nicht mehr gelöscht werden [8], sie wird erst nach Ablauf des vom Anbieter angegebenen Zeitraums automatisch von den Servern gelöscht.

Free Haven funktioniert mit einem direkten Tauschhandel, unterstützt durch ein verteiltes Reputationssystem. Jeder Datei wird ein Tauschwert von Dateigrösse multipliziert mit der verbleibenden Lagerzeit zugeordnet [8]. Eigene Dateien muss man mit anderen Servern gegen Dateien mit ähnlichem Tauschwert tauschen, um sie so ins Netzwerk einzufügen. Der Bestand von Dateien wird regelmässig mithilfe eines *Buddy*-Systems kontrolliert. Server, die eine Datei halten, überprüfen regelmässig eine zugeordnete Partnerdatei [8]. Falls etwas gemäss Tauschabkommen zu früh gelöscht wurde, wird dies in einer Reputationstabelle notiert und anderen Servern auf Anfrage mitgeteilt [8].

Zudem können Server Dateien nach ihrem Bedarf aufnehmen. Will ein Anbieter seinen Server aus dem Netz entfernen, so versucht er, seine Dateien mit langen Lagerfristen gegen andere auszutauschen, die zwar grösser sind, aber weniger lang gehalten werden müssen. Dies kann er machen, bis er ungestraft alle gelagerten Dateien löschen und den Server vom Netz nehmen darf [8].

Das System erfüllt ein anderes Ziel als Freenet, hat aber auch seine Schwächen. Auch ein Reputationssystem hindert Server kaum daran, vom Netzwerk mitsamt den fremden

Daten zu verschwinden, sobald die eigenen Daten auf dem Netz verteilt sind. Das *Buddy*-System bringt zusätzlich ein Problem. Wenn ein Administrator auf seinen Servern zwei zusammengehörende *Buddies* kontrolliert, kann er beide löschen, ohne an Reputation zu verlieren.

1.2.3 OceanStore

Auf dieses Konzept soll nur kurz eingegangen werden. OceanStore versucht wie Free Haven, eine langfristige Datenspeicherung zu garantieren. Das P2P-Netzwerk besteht aus zwei Klassen von Servern. Eine äussere Klasse von freiwilligen Servern ist für eine gewisse Redundanz zuständig, um auch eine grosse geographische Verteilung zu ermöglichen. Ein zentraler Kern von Servern wird von kommerziellen Anbietern geführt, die Speicherplatz gegen eine monatliche Gebühr verkaufen. Diese Daten werden jedoch von dieser Firma nicht nur selbst gelagert, sondern auch ins OceanStore Netzwerk eingefügt und verteilt, sowohl auf andere kommerzielle Server wie auch auf freiwillige. Im Gegenzug speichert die Firma auch Daten von anderen kommerziellen Firmen [11].

Die zentralen Server sind als Gegenleistung für die Gebühr dafür verantwortlich, sicher zu stellen, dass immer eine genug grosse Redundanz der Daten vorhanden ist. Dazu durchsuchen sie periodisch das Netzwerk und korrigieren mangelnde Verteilungen [11].

Alle Daten werden verschlüsselt [11], um nur jenen Zugang zu gewähren, die den nötigen Schlüssel besitzen, das heisst die Auftraggeber sowie ihre Vertrauenspartner.

1.2.4 Tahoe

Dabei handelt es sich um eine neuere Applikation, welche vor allem private P2P-Netzwerke erstellt, um einer kleinen Gruppe Zugang zu den gespeicherten Daten zu verschaffen.

Jedes Netz, sei es ein privates oder auch ein grosses öffentliches, hat zwei dedizierte Server. Einer davon ist dafür verantwortlich, Verbindungen zwischen den Peers zu vermitteln, ein anderer ordnet den Dateipfaden in den virtuellen Ordnern die entsprechenden Identifier zu [25]. Das System wird dadurch anfällig für DDoS-Angriffe.

Die Dateien werden verschlüsselt transportiert und gelagert, um Unbefugten den Zugriff zu verweigern und die Konsistenz mithilfe eines Hashes sicherzustellen [25].

Das Potential ist vorhanden, um eine erfolgreiche Groupware-Applikation oder ein verteiltes Ordnersystem für Privatpersonen zu werden. Das Bedürfnis nach Zugang zu den eigenen Dateien, egal wo man sich befindet, wird immer grösser. Tahoe erfüllt dieses Bedürfnis mit P2P-Technologien. Die Entwicklung wird zeigen, ob Tahoe sich in diesem etablierten Markt auf Client/Server-Struktur bewähren kann.

1.2.5 BitTorrent

Als letztes Beispiel sollen die Ziele und die Umsetzung des wohl momentan bekanntesten P2P-Netzwerkes aufgezeigt werden. Im Gegensatz zu den meisten vorgängig beschriebenen Applikationen, versucht BitTorrent keineswegs Dateien langfristig zu lagern. Das Ziel von BitTorrent ist, aktuelle, häufig nachgefragte Dateien schnell zu verteilen. Dabei wirkt bewusst das System, dass Dateien nur so lange schnell verfügbar sind, wie die Nachfrage gross ist [6]. Verschiedene Firmen nutzen diese Eigenschaften von BitTorrent, um ihre Software schnell und günstig zum Download anzubieten, ohne Mirrors beschaffen zu müssen [28].

Auf Anonymität wird verzichtet, indem direkte Verbindungen zwischen den Peers hergestellt werden. Es gibt zentrale Tracker, die dafür verantwortlich sind, dass sich Peers gegenseitig finden.

Ein weiterer grosser Unterschied zu den oben erwähnten Beispielen besteht darin, dass der Benutzer die Kontrolle darüber hat, welche Dateien er auf seinen PC laden und wie lange er sie anderen anbieten will. Über alternative Kanäle, im Allgemeinen auf Websites, werden kleine Torrent-Dateien angeboten, die Tracking-Informationen zu verfügbaren Musikstücken oder anderen Dokumenten enthalten [6]. Diese Torrent-Dateien enthalten nicht die Datei selbst, sondern nur deren Hash-Wert und Verweise darauf, wo im Netzwerk diese Datei gefunden werden kann.

Als Incentive wirkt vor allem eine Art Tauschhandel. Peers laden nur solange Teile einer Datei hoch, solange man selbst auch ihnen Teile derselben Datei sendet [6]. Die Peers haben also ein Interesse daran, die bereits heruntergeladenen Dateien zu verbreiten, um auch selbst zu neuen Teilen zu kommen.

Vor allem das einfache, aber sehr effektive System der Incentives, aber auch die Möglichkeit, Teile von unfertig vorhandenen Dateien anzubieten, sind für den enormen Erfolg von BitTorrent verantwortlich. Für langfristiges Speichern von Dateien sind solche Filesharing-Netzwerke hingegen sinnlos, da nur populäre Dateien im System bleiben.

1.3 Sicherheit der Daten

Die Sicherheit der Daten in einem P2P Storage Networks muss auf verschiedene Arten sichergestellt werden. Je nach Bedarf, muss die Lesbarkeit eingeschränkt werden. Vielfach ist es auch wichtig, Informationen über den Ursprung von Daten oder anderen Leistungen zu erhalten, bevor man diese nutzt. Dies wird mit Zertifikaten oder einem Reputationssystem ermöglicht.

1.3.1 Verschlüsselung

Das Konzept der Verschlüsselung wird häufig in P2P-Netzwerken verwendet. Auch eine zentrale Rolle spielen andere kryptographische Verfahren, die im Zusammenhang mit

Signaturen, mit Hash-Erstellung oder mit unterschiedlichen Arten von Micropayments wichtig sind.

In den erwähnten privaten P2P-Netzen nimmt die Verschlüsselung eine zentrale Stelle ein. Da die Einsicht der Informationen auf die jeweilige Gruppe beschränkt bleiben muss, wird zum Beispiel bei Groove standardmässig alles verschlüsselt [21].

Die Verschlüsselung von Daten wird auch in anonymen P2P Permanent Storage Systemen eingesetzt, jedoch aus einem anderen Grund. Obwohl auch hier die Einsicht mithilfe der Verteilung eines Schlüssels eingeschränkt werden kann, so ist das primäre Ziel der Verschlüsselung ein anderes. Einerseits wird mit der Verschlüsselung jegliche Manipulation sofort erkannt und andererseits weiss ein Besitzer eines Servers so nicht, welche Dateien auf seinem System sind, da er nur einen Teil des Schlüssels besitzt und weitere Teile auf anderen Servern verteilt sind [23]. Damit kann er selbst Dateien nicht selektiv löschen, aber andererseits macht er sich auch nicht strafbar, da für ihn die Dateien nur zufällige Bit-Folgen darstellen [8].

1.3.2 Accountability

Während in der realen Welt der Hersteller oder Verkäufer eines Produktes oder einer Leistung ein starker Hinweis auf die Qualität des Produktes oder der erbrachten Leistung selber ist, so fehlt diese Möglichkeit meist im Internet. In der Client/Server-Struktur kann über die Domain des Servers schnell der Betreiber ausfindig gemacht und zur Rechenschaft gezogen werden [24][7]. Auch gibt es in dieser Architektur relativ wenige, statische Anbieter, was die Bildung einer Reputation erlaubt. Wenn man von der Webpage eines bekannten Anbieters ein Programm herunterlädt, so kann man davon ausgehen, dass es keinen Schaden anrichtet [24].

In P2P-Systemen ist jeder Benutzer zugleich auch Anbieter. Zudem wechseln die vorhandenen Anbieter ständig, was die Bildung einer Reputation stark erschwert. Dateien werden nicht von den Servern der Hersteller heruntergeladen, sondern von den Heimcomputern unbekannter Benutzer. Die Benutzer sind zudem nicht permanent online, was zur Folge hat, das die selbe Datei nacheinander von verschiedenen Anbietern heruntergeladen werden kann. Server besitzen meistens einen Namen und gehören einer Domain an. Diese Domain muss vom Unternehmen oder einer Privatperson unter ihrem richtigen Namen registiert werden. Anbieter in einem P2P-Netzwerk besitzen normalerweise keine eigene Domain und können somit mit normalen Mitteln nicht zur Rechenschaft gezogen werden [7]. Dies alles erschwert die Beurteilung der Qualität von Produkten oder Dienstleistungen aufgrund des Anbieters, sei es zum Beispiel Software oder auch Speicherplatz für meine Dateien..

1.3.2.1 Signaturen und Zertifikate

Eine Möglichkeit zur Lösung dieses Problem besteht darin, mit kryptographischen Verfahren die Zuordnung einer virtuellen Identität zu einer realen sicherzustellen [15]. Dazu

werden mit asymmetrischen Verschlüsselungen Daten signiert. Dies kann geschehen, indem die ganze Datei mit dem privaten Schlüssel verschlüsselt wird oder, wie normalerweise üblich, ein Hash der Datei [24]. Der öffentliche Schlüssel wiederum wird entweder über persönliche Kanäle verteilt, auf einer bekannten Webpage publiziert oder im besten Fall durch eine Zertifizierungsstelle signiert. Die Person oder das Unternehmen muss sich dazu bei einer vertrauenswürdigen Stelle authentifizieren und bekommt somit auf seine wahre Identität das Zertifikat ausgestellt [24]. Damit kann kryptographisch mit einer statistisch gesehen sehr hohen Wahrscheinlichkeit sichergestellt werden, dass es sich beim fraglichen Anbieter tatsächlich um die genannte Person oder das Unternehmen handelt.

Solche Zertifizierungsdienste werden bereits von einer Auswahl an Firmen wie zum Beispiel auch der Schweizer Post angeboten [30] und werden auch für Privatpersonen immer attraktiver.

Eine Alternative ist ein System namens *Web of Trust*, das zum Beispiel bei PGP in Betrieb ist. Dabei können in einer Public Key Infrastructure die öffentlichen Schlüssel von anderen Personen gegenseitig zertifiziert werden. Damit kann transitiv die Authentizität eines öffentlichen Schlüssels bestätigt werden, falls ein direkter Pfad zum Schlüssel der betreffenden Person besteht [7][21]. Erfahrungsgemäss wirkt hier der Small-World Effekt, was transitive Pfade mit einer durchschnittlichen Länge von 6 zu Folge hat [7].

Obwohl diese Möglichkeiten einige Probleme beheben können, sind sie lange nicht für alle Zwecke geeignet. So ist in anonymen Permanent Storage Systemen eine Zuordnung von Anbietern zu realen Personen genau nicht erwünscht. Das Hauptziel solcher Netze ist es, jegliche Korrelation von digitaler zu realer Identität zu unterbinden.

1.3.2.2 Reputation

Ein Reputationssystem kann die Qualität von Angeboten erhöhen, sei es in Systemen, wo eine Zuordnung von virtuellen zu realen Identitäten erwünscht ist oder sei es in Systemen, wo mit Pseudonymen gearbeitet wird. In diesem Kapitel soll beschrieben werden, was Reputation ist und wie ein Netzwerk Reputation einsetzen kann. Wie Lethin von Reputation Technologies es definiert:

> Reputation is the memory and summary of behaviour from past transactions [13].

Ein Problem ergibt sich natürlich sofort daraus, denn:

> Reputation system does not judge intent, merely actions [8].

Neue Ratings können nur reaktiv vergeben werden, erst nachdem sich Entitäten falsch verhalten haben. Im Zusammenhang mit P2P Storage Networks kann das im schlimmsten Fall heissen, dass Daten zuerst verloren gehen müssen, bevor eine Reaktion darauf geschieht. Es gibt Ansätze, bei denen neue Peers mit der minimal möglichen Reputation

anfangen, und sich erst nach Bewährung eine Reputation verdienen können [7]. Obwohl dies die Probleme von Pseudospoofing minimiert, so erschwert es den Eintritt neuer Peers beträchtlich.

Es werden unterschiedliche Arten von Reputationssystemen verwendet. Am bekanntesten, da auch auf vielen populären Webpages verwendet, sind zentralisierte Reputationssysteme. Dies widerspricht den Prinzipien von reinem P2P, bringt aber Vorteile wie besserer Schutz vor Fälschungen und einfachere Umsetzung mit sich [13]. Es gibt jedoch verschiedene Varianten von dezentralisierten Reputationssystemen, welche leichter zu manipulieren, dafür aber flexibler einsetzbar sind.

Zentralisierte Reputationssysteme sind weit verbreitet und in vielen Formen im Einsatz. Eines der Probleme, mit dem immer mehr Applikationen und Webpages mit zentralisierten Reputationssystemen zu kämpfen haben ist die Frage, wem die Reputationsdaten eigentlich gehören [13].

Als Alternativen gibt es verschiedene Ansätze, Reputationssysteme verteilt aufzubauen. Ein einfacher Ansatz ist, dass bei Fehlverhalten eines Peers (vorzeitiges Löschen von Daten, Nutzen von Ressourcen ohne selbst Ressourcen anzubieten usw.) jenes Peer, das das Fehlverhalten feststellt, dies an möglichst viele andere Peers per Broadcast weitergibt. Alle Peers tragen diese Daten nun in Ihre Sammlung von Reputationsdaten ein, um weitere Entscheidungen auf diesen Daten zu basieren. Nach dem gleichen System, aber in umgekehrter Weise, können auch die Erfahrungen lokal gespeichert werden [8]. Wenn ein Peer eine Leistung eines anderen Peers in Anspruch nehmen will, kann es per Broadcast zuerst alle Reputationsdaten in Reichweite bezüglich dieses spezifischen Peers abfragen. Um das System trotzdem skalierfähig zu halten, muss die Reichweite von Anfragen stark eingeschränkt werden.

Sofort ergeben sich dadurch weitere Probleme. Reputationen können einfach gefälscht werden, indem zusammenarbeitende, böswillig eingestellte Peers sich gegenseitig ausgezeichnete Reputationen geben oder andere fälschlicherweise als unzuverlässig darstellen. Als mögliche Lösungen können pro Peer separate Zahlen für die Performance und für die Zuverlässigkeit, mit welcher der Server andere beurteilt, gespeichert werden [7]. Diese Zuverlässigkeiten wirken transitiv über Vertrauensketten. Falls sich über eine Kette unterschiedliche Peers jeweils hohe Zuverlässigkeiten in der Bewertung gegeben haben, kann der Ursprung der Kette transitiv davon ausgehen, dass die Bewertungen des Peers am Ende der Kette auch zuverlässig sind.

Als besonderen Vorteil eines dezentralisierten Systems gilt, dass jedes Peer seine eigenen Algorithmen verwenden kann, um die verteilten Informationen zu deuten [7]. Während für sicherheitskritische Peers eine hohe transitive Zuverlässigkeit gewährleistet sein muss, kann für andere ein einfacher Durchschnitt der erhaltenen Reputationen auf Anfragen genügen. Das Problem der Erschwerung von Neueinsteigern kann damit reduziert werden, dass bereits vorhandene Peers, die sich eine Reputation als zuverlässige Bewerter verdient haben, neuen Peers eine gute Reputation geben können [8]. Dies ist zum Beispiel sinnvoll, wenn ein Besitzer eines Peers einem Bekannten, von dem er weiss, dass er keine böswilligen Aktionen durchführen will, den Einstieg erleichtern will.

Weiterführende Modelle können auch die Art der abgewickelten Transaktionen einbeziehen. Ähnliche Transaktionen zur bevorstehenden werden stärker bewertet, wie grössere Transaktionen auch [7]. In Storage Systems kann dies die Grösse der zu verschiebenden Dateien sein, aber auch bei unverschlüsselten Daten Ähnlichkeit der Inhalte. Falls sich P2P Netzwerke nicht bloss auf Speicherung beschränken, kann auch nach Art der getauschten Ressource, sei es CPU-Zyklen (z.B. zu Suchfunktionen), benutzter Speicherplatz oder Bandbreite eingeteilt und bewertet werden.

Als Zwischenweg gibt es auch die Möglichkeit, vertrauenswürdige Moderatoren einzusetzen [7]. Diese können abgeschlossene Transaktionen kontrollieren und objektive Bewertungen abgeben. In einem System, wie oben beschrieben, muss dies nicht explizit implementiert werden. Peers, die viele Reputationen generieren und allgemein als zuverlässig gelten, können im lokalen Algorithmus stark gewertet werden. Diese würden inoffiziell die Funktion der Moderatoren übernehmen.

1.3.3 Pseudonyme

In diesem Kapitel wird gezeigt, dass ein System, welches mit Pseudonymen arbeitet, nicht gleich Anonymität garantiert. Zudem wird analysiert, wie Pseudonyme mit einem Reputationssystem zusammenhängen, da Entitäten ohne Pseudonyme nicht über eine Session hinweg identifiziert werden können. Eine Möglichkeit, das Reputationssystem zu umgehen, besteht darin, sich wiederholt neue Pseudonyme zuzulegen. Ein P2P Storage Network muss dem entgegenwirken.

1.3.3.1 Pseudonyme als Mittelweg zwischen Anonymität und Signaturen

Ein Bereich, der sehr nahe beim Thema Accountability anzusiedeln ist, sind Pseudonyme. Häufig ist es wegen unzureichend vorhandener Infrastruktur, zu hohen Preisen oder weil es für den Benutzer zu umständlich ist, sich ein persönliches Zertifikat ausstellen zu lassen, nicht möglich, digitale Entitäten zu realen in Zusammenhang zu bringen. Vielfach ist dies von den Benutzern auch gar nicht erwünscht, sie wollen anonym bleiben. Obwohl manche Sicherheitskonzepte darauf aus sind, alle Benutzer so anonym wie irgendwie möglich zu halten, so ist das eine andere Art von Sicherheit als der Schutz vor böswillig geschriebenem Code oder vor Angriffen auf die Verfügbarkeit von Daten und Services. Bei der Anonymität als Sicherheitskonzept geht es darum, die Benutzer sicher vor Verfolgung oder Diskriminierung oder auch schlicht *sicher* vor den Gesetzen zu halten.

Der Gebrauch von Pseudonymen kann keineswegs mit Anonymität gleichgesetzt werden. Auch mit dem Gebrauch von Pseudonymen kann mit genug starken finanziellen oder rechtlichen Mitteln die reale Person ausfindig gemacht und zur Rechenschaft gezogen werden. Trotzdem erhalten Personen durch den Gebrauch von Pseudonymen einen gewissen Schutz der Privatsphäre gegenüber der grossen Allgemeinheit, es ermöglicht aber immer noch in einem gewissen Ausmass die Nutzung der Vorteile der digitalen Identifikation.

1.3.3.2 Pseudonyme als Basis eines Reputationssystems

Um ein Reputationssystem umzusetzen, braucht man mindestens Pseudonyme, um Reputationen länger als eine Session aufrechtzuerhalten. Es muss möglich sein, Nutzungen über grössere Zeiträume Entitäten zuzuordnen, um ein sinnvolles Reputationsprofil erstellen zu können. Als Entität kann je nach System eine Person, ein PC, ein Server oder gar eine Ressource, das heisst Daten selbst, gemeint sein.

In der aktuellen Implementierung des Internets mit IPv4 ist es nicht möglich, allen Teilnehmern fixe IP-Adressen zuzuteilen. In der Praxis werden über DHCP aus einem Bereich IP-Adressen nach Bedarf verteilt. Für den einzelnen Computer heisst das, dass er häufig seine Kennung auf dem Netz ändert [15]. Pseudonyme übernehmen die Aufgabe, Computer auch mit neuen IP-Adressen identifizieren zu können.

Bei Permanent Storage Netzwerken ist es wichtig, die Zuverlässigkeiten der Server zu kennen, bei File Sharing Netzwerken mehr die Bandbreite einzelner Computer und wieder bei anderen Systemen sind die Nutzer zu bewerten, egal von wo sie den Service nutzen [19]. Auch Daten können über Pseudonyme oder über einen Hash eine Reputation zugeordnet bekommen, was heute oft benutzt wird [14]. Immer wenn Reputation wichtig ist, müssen dazu die nötigen Pseudonyme vorhanden sein.

1.3.3.3 Pseudospoofing

Pseudonyme sind nicht direkt mit der zugehörigen realen Entität verknüpft. Daraus ergibt sich das Problem des Pseudospoofings, das heisst, man versetzt in Verruf geratene Entitäten mit einem neuen Pseudonym und setzt dieselben Entitäten so wieder ins System. Dies kann das Erstellen eines neuen Accounts für einen User [7], das Umbenennen eines Pseudonyms eines Computers oder eine Umbenennung der Daten sein. Selbst wenn das Pseudonym von Daten aus einem Hash besteht, kann nur wenig an den Daten geändert werden, um einen komplett neuen Hash zu erhalten.

Als eine mögliche Lösung dazu müssen neue Entitäten schlechter bewertet sein als bereits vorhandene, egal wie sie sich verhalten haben [7]. In einem solchen System müssen aber Algorithmen wirken, die es ermöglichen, wie oben beschrieben, neuen, über andere Wege bekannten Entitäten eine gute Startreputation zu geben [8].

1.3.3.4 Weiterführende Aspekte

Es gibt Konzepte, bei denen Entitäten sich über einen zentralen Server einloggen müssen, um ihre Identität zu authentifizieren. Damit geht man jedoch wieder einen Schritt weiter weg vom Konzept von P2P und reduziert die Vorteile wie Ausfallsicherheit drastisch, da es einen zentralen Angriffspunkt gibt. Dezentralisierte Systeme haben das Problem, dass in Verruf geratene Entitäten sich als bewährte Entitäten mit einem guten Ruf ausgeben, indem sie zum Beispiel das Pseudonym von bekannten Servern als ihr eigenes ausgeben. Als simple, aber sehr effektive Lösung muss somit jedes Pseudonym, egal für welche Entität

es steht, im Hintergrund aus einem asymmetrischen Schlüsselpaar bestehen [21]. Durch kryptographische Verfahren kann so jederzeit auch in einem dezentralisierten System ein Pseudonym eindeutig einem Benutzer oder einer Ressource zugeordnet werden.

Es gibt in der Praxis viele Applikationen, die bewusst auf Pseudonyme verzichten oder diese bloss zur Identifikation von Daten anwenden. Bei den anderen gibt es eine grosse Auswahl an unterschiedlichen Methoden und Kombinationen. Dieses Kapitel soll die grundlegenden Prinzipien erklären, die hinter den Systemen stehen, auch wenn sie häufig implizit verwendet werden.

1.3.4 DDoS-Resistenz

Distributed Denial of Service-Angriffe können Server, aber auch Services eines P2P-Systems temporär ausser Betrieb nehmen. In diesem Kapitel werden die konkreten Probleme erläutert, welche speziell in P2P Storage Networks von Interesse sind. Es gibt verschiedene Ansätze, DDoS-Angriffen entgegenzuwirken, diese werden in diesem Kapitel ebenfalls beschrieben.

1.3.4.1 DDoS als Problem

Auch wenn es als ein Vorteil von P2P-Systemen gilt, dass sie gegen Denial of Service Attacken resistent sind, so sind sie doch keineswegs immun. Wer Daten in einem P2P Storage Network speichert, ist daran interessiert, dass diese Daten nicht nur lange gespeichert bleiben, sondern dass sie auch jederzeit abrufbar sind, wenn jemand sie braucht. Dies ganz egal, aus welchem Grund man die Daten einem P2P-Netzwerk anvertraut. Im Gegensatz dazu können Personen oder Organisationen ein grosses Interesse daran haben, die Verfügbarkeit solcher Daten, wenn auch nur kurzfristig, zu unterbinden [22].

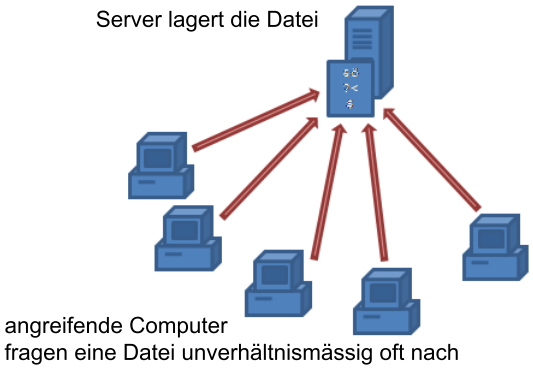


Abbildung 1.7: DDoS-Angriff durch unzählige Anfragen

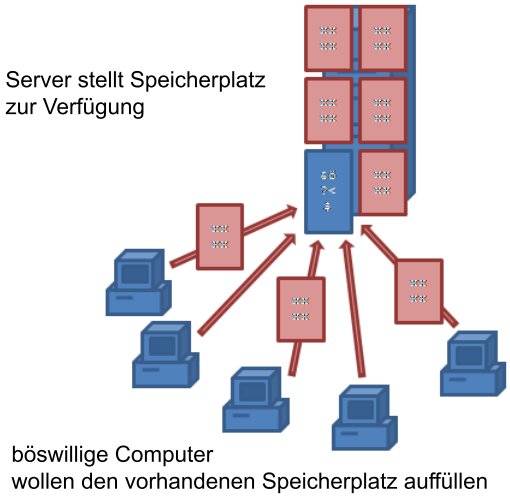


Abbildung 1.8: DDoS-Angriff durch Auffüllen des Speichers

Abgesehen von Angriffen auf zentrale Verwaltungsserver mit Such- oder Vermittlungsfunktionen sind im Storage Bereich vor allem zwei Arten von DDoS möglich. Einerseits kann, was Abbildung 1.7 darstellt, durch übermässiges Abfragen einer Datei die Netzauslastung so gross werden, dass weitere Anfragen nicht bedient werden können, andererseits können, wie Abbildung 1.8 zeigt, so viele sinnlose Dateien auf ein P2P Speichersystem hochgeladen werden, dass der Speicher für weitere Daten nicht mehr zur Verfügung steht, da der ganze Platz aufgebraucht ist.

1.3.4.2 IP-Filter

Als Gegenmittel sind gängige IP-Filter naheliegend. Falls dieselbe IP innerhalb eines bestimmten Zeitraums zu viele Male denselben Service verlangt, sei es das Hinzufügen oder die Abfrage einer Datei, so wird sie für eine Weile gesperrt [23]. Das Hauptproblem ist, dass mit heutigen Distributed Denial of Service Attacken ganze Heerscharen von Bots auf fremden Computern eingesetzt werden können. Bots sind böswillige Computerprogramme, die ohne das Wissen des Besitzers des Computers auf Befehl eines Hackers oder gemäss eines vorprogrammierten Auslösers Aktionen durchführen. Auch können Ursprungsadressen einfach gefälscht werden, was zumindest auch die Bandbreite stark reduzieren könnte.

Ein weiteres Problem ist das DHCP-System. Wenn jemand böswillig von einer IP aus einen Angriff durchgeführt hat und gesperrt wurde, so haben während einer gewissen Zeit alle, die diese IP vom Provider bekommen, ebenfalls keinen Zugang mehr [24].

1.3.4.3 Micropayments

Ein anderer Ansatz sind sogenannte Nonfungible Micropayments, auch bekannt unter dem Namen *proof of work* [7]. Dabei geht es darum, dass Benutzer vor einer Aktion eine speziell vom Anbieter gestellte rechenintensive Aufgabe lösen müssen. Es sind Aufgaben zu wählen, die schwer zu berechnen, aber einfach zu überprüfen sind, wie zum Beispiel partielle Hash-Kollisionen [7] oder auch Primfaktorzerlegungen von grossen Zahlen. Der Anbieter kann mit dem Resultat nichts anfangen, aber es zeigt ihm, dass der Benutzer etwas geleistet hat. Diese Berechnungen können auf einem Computer je nach Bedarf wenige Sekunden in Anspruch nehmen. Einzelne, legitime Anforderungen werden somit kaum merklich gestört, Massenanfragen aber stark erschwert.

Details zu solchen Konzepten werden immer ausgereifter und das Potential auch für andere Anwendungen (zum Beispiel Spam-Schutz im Email-Verkehr) ist sehr gross [7]. Trotzdem ist diese Lösung mit den jetzigen technologischen Möglichkeiten kaum sinnvoll einsetzbar. Mit Bots auf Massen von Computern, sind solche Barrieren für professionelle Hacker nur kleine Hindernisse. Auch verfügen Unternehmen über sehr viel Rechenpower, die sie auch für solche Zwecke einsetzen können, um kompromittierende Dokumente in P2P Storage Networks unzugänglich zu machen.

Ein ähnliches Konzept benutzt Fungible Micropayments, das heisst Zahlungen, die zuerst verdient und dann vom empfangenden Server wieder benutzt werden können.

1.3.4.4 Algorithmen zur impliziten DDoS-Resistenz

Ein einfaches, aber trotzdem sehr effektives Lösungskonzept beinhaltet Algorithmen, welche die Datenbenutzung dezentralisiert wahrnehmen und darauf reagieren. Freenet hat simple Algorithmen, die aber sehr effektiv gegen DDoS Attacken sind. Häufig nachgefragte Dateien werden vervielfacht und an verschiedenen Orten gespeichert, während wenig gefragte Dateien gelöscht werden [5]. Will nun jemand böswillig den Zugang zu einer Datei mit einer Übermenge an Anfragen blockieren, so hat dies bloss eine starke Reproduktion der Datei auf andere Server zur Folge, um der Nachfrage gerecht zu werden. Der Angreifer würde genau das Gegenteil seiner Absicht als Resultat erzielen. Will der Angreifer den zur Verfügung stehenden Speicher mit sinnlosen Daten füllen, um den Service zu blockieren, so werden jeweils seine sinnlosen Daten zuerst wieder von den Servern gelöscht, sobald kein Platz mehr vorhanden ist, da sie wohl am wenigsten nachgefragt werden.

Mit wenigen, durchdachten Algorithmen kann der Bedarf nach hoch komplizierten und womöglich auch teuren Mechanismen verhindert werden. Es gibt unzählige Studien zu gezielten und ungezielten Angriffen auf verschiedene P2P Storage Networks [10]. Generell lässt sich sagen, dass P2P-Systeme gegen DDoS Attacken resistenter sind als zentralisierte Systeme. Da eine Datei oder ein Service in einem P2P-Netzwerk über viele Computer verteilt ist, müssen alle Peers, auf denen sich Replikate befinden, ausser Kraft gesetzt werden und nicht bloss ein einziger oder wenige Server, wie in einer Client/Server-Architektur.

1.3.5 Konsistenz

In einem verteilten Speicher sind eine Grosszahl der Computer, auf welchem Dateien gelagert sind, nicht unter einheitlicher Kontrolle. Veränderte Dateien müssen somit klar als solche erkannt werden können, damit ein Benutzer auch die Datei erhält, die er haben will. Eine weitere Schwierigkeit ist es in einem solchen System, dem Ersteller die Möglichkeit zu geben, Änderungen anzubringen, diese Möglichkeit aber für alle anderen zu unterbinden.

1.3.5.1 Datenänderung als Angriffsmethode

Ebenso wichtig, wie den zuverlässigen Zugang zu Daten sicherzustellen, ist es, die Konsistenz der Daten zu garantieren. Vom Standpunkt eines Angreifers ist es einiges effektiver, Daten nach eigenem Gutdünken zu verändern als sie zu löschen oder einfach nicht mehr verfügbar zu machen. Durch das Verändern der Daten können diese an die Bedürfnisse des Angreifers angepasst werden, was eine Aussage im Sinne des Angreifers verbreiten würde. Das Problem wird umso schwieriger, wenn es sich um ein anonymes System handelt, wo kein öffentlicher Schlüssel des Urhebers besteht.

1.3.5.2 Hash als Suchschlüssel

Es gibt eine Reihe von Konzepten, Konsistenzprobleme zu lösen. Häufig wird mit einem kryptographischen Hash gearbeitet. So wird zum Beispiel in einigen Implementierungen

der Hashwert in die Suchfunktion eingebaut und jedesmal überprüft. Der Link, der auf eine Datei im Netzwerk zugreift, enthält den Hashwert. Der Hashwert ist eine folge von Bits, welche mit kryptographischen Verfahren aus der Bitfolge der ursprünglichen Datei ausgerechnet wird. Statistisch gesehen ist es sehr unwahrscheinlich, dass zwei unterschiedliche Dateien den selben Hash generieren, auch wenn sie nur leicht unterschiedlich sind. Wurde die Datei verändert, so zeigt der Link nicht mehr darauf, da die abgeänderte Datei einen neuen Hash besitzt. Solange man also Zugang zu einem korrekten Link hat, sei es über Email oder andere Wege, wird man auch das dazugehörige korrekte Dokument erhalten, oder aber keines, falls alle Versionen der ursprünglichen Datei innerhalb der definierten Anzahl von Suchschritten verändert wurden [23].

1.3.5.3 Konsistenz durch Redundanz

Ein weit verbreitetes Konzept, die Konsistenz möglichst zu erhalten, ist der Einsatz von Redundanzen. Um sowohl die Konsistenz wie auch die Verfügbarkeit sicherzustellen, gibt es Methoden, welche die Datei symmetrisch verschlüsselt auf einer Vielzahl von Servern platzieren. Der symmetrische Schlüssel wiederum wird mithilfe eines Secret Sharing Algorithmus wie Abbildung 1.9 zeigt in eine Anzahl Teile aufgeteilt, wovon eine frei wählbare Untergruppe mit mindestens einer bestimmten Zahl von Teilschlüsseln genügt, um den ursprünglichen Schlüssel wiederherzustellen [22]. Auf jedem Server, der die verschlüsselte Datei lagert, wird auch ein Teil des Schlüssels platziert. Dies hat auch zur Folge, dass selbst der Besitzer des Servers keine Ahnung hat, welche Daten er lagert, da sein Teil des Schlüssels nicht dazu reicht, die Datei zu entschlüsseln [23].

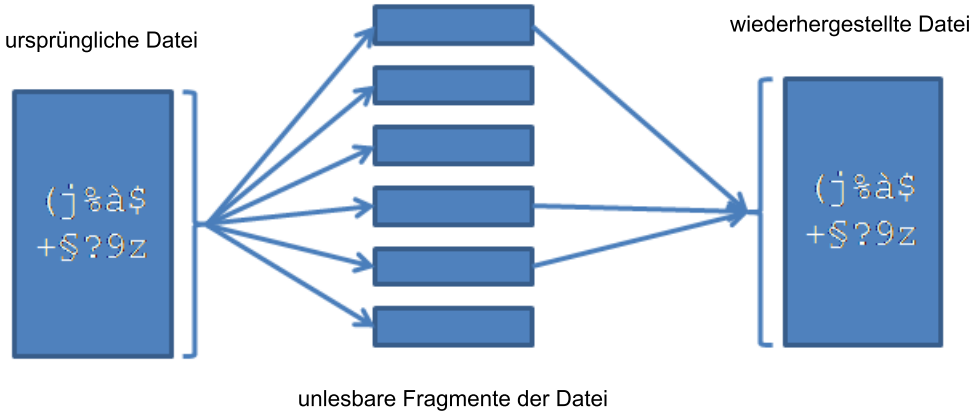


Abbildung 1.9: Aufteilung in Fragmente mit Secret Sharing

Ein Benutzer, der die Datei lesen will, braucht die Datei von einem beliebigen Server sowie die vorher vom Ersteller festgelegte Anzahl an Schlüsselteilen. Klappt die Entschlüsselung nicht, so stimmt die Konsistenz von entweder einem Schlüsselteil oder der Datei nicht [23].

Die Konsistenz ist nur dann gefährdet, wenn zufälligerweise alle Server, von denen ein Schlüsselteil geholt werden, korrupt sind und zusammen eine geänderte Datei mit einem neuen Schlüssel unter altem Namen erstellt haben.

1.3.5.4 Berechtigte nachträgliche Änderungen

Dem Ersteller eines Dokuments die Möglichkeit zu geben, dieses später noch zu verändern, ermöglicht alternative Angriffswege wie Gewalt, Drohungen oder Erpressung, um Personen zum Löschen oder Verändern eines Dokuments zu veranlassen [2] und es bringt verbunden mit Redundanz wiederum ein Konsistenzproblem, da womöglich parallel mehrere neue und alte Versionen existieren. Deshalb haben die meisten Implementationen auf dieses Feature verzichtet [2]. Dateien werden nach einer gewissen Zeit [8] oder mangels Nachfrage [5] irgendwann gelöscht und veränderte Daten werden als komplett neue Datei ins System eingefügt.

Es gibt einzelne Konzepte, um mit einer Datei jeweils auch den Hash eines Passwortes zu speichern. Dies gibt jedem, der das Passwort besitzt, die Möglichkeit, ein Updatefile auf den Server zu legen. Je nach Ansatz kann dies ein Link zur neuen Datei oder aber anzubringende Änderungen an der bereits vorhandenen Datei beinhalten [11]. Zu beachten dabei ist, dass die Dateien auf den Servern normalerweise verschlüsselt sind [11]. Die Änderungsdatei muss entweder Instruktionen zur Änderung der verschlüsselten Datei enthalten, oder aber Instruktionen zur Veränderung der unverschlüsselten Datei und muss selbst verschlüsselt sein.

Datenkonsistenz ist wichtig in jeder Implementierung von P2P Storage Networks. Mit Redundanz und kryptographischen Mitteln wie Hash, Verschlüsselung oder Shared Secret Algorithmen ist dieses Ziel umsetzbar. Gekoppelt mit Spiders, die Dateien zwischen Redundanzen vergleichen und fehlerhafte entfernen, kann Konsistenz erreicht werden.

1.4 Incentives

Ohne Incentives würde ein Grossteil der Benutzer in P2P Storage Networks Leistungen nur konsumieren, ohne selber welche anzubieten. In diesem Kapitel wird beschrieben, mit welchen Mitteln einem solch egoistischen Verhalten entgegengewirkt werden kann.

1.4.1 Incentives als Gegenmittel zum Egoismus

Wie viele Gebiete der Wirtschaft, leidet die P2P-Strategie unter der von Garett Hardin beschriebenen *tragedy of the commons*. Darunter versteht man, dass bei einem unregulierten Zugang zu beschränkten Ressourcen jedes Individuum darauf aus ist, seinen eigenen Nutzen zu maximieren. Damit wird die Ressource jedoch selbst zerstört, was der Gesamtheit der Individuen schadet [7][4]. Jedes erfolgreiche P2P-System muss deshalb etwas gegen diese Bewegung unternehmen, indem es Anreize liefern muss, dass die Benutzer Ressourcen liefern und nicht nur konsumieren [10]. Es liegt in der Natur der Sache, dass ebensoviel Daten hinauf- wie hinuntergeladen werden müssen [6].

Unterschiedliche Systeme verfolgen unterschiedliche Ziele und so müssen ganz unterschiedliche Anreize generiert werden. Während in Konsumenten-zentrierten Systemen die Leute

möglichst viele Daten herunterladen wollen, ohne selbst welche anbieten zu müssen, so liegt in Anbieter-zentrierten Systemen das Interesse der Benutzer vor allem darin, ihre Daten auf möglichst viele Server hochladen zu dürfen, ohne selbst viele fremde Daten speichern zu müssen.

1.4.2 Direkter Tausch

Eine einfache Möglichkeit ist es, eine Art direkter Tauschhandel zu implementieren, nach dem Prinzip tit-for-tat. Hat ein Benutzer erst einmal ein erstes Segment einer Datei auf seinen Computer heruntergeladen, so wird er mit anderen Computern in Kontakt treten, die ebenfalls diese Datei wollen. Falls sie, wie in Abbildung 1.10 gezeigt, gegenseitig Teile haben, die der jeweils andere nicht hat, so tauschen sie diese [6]. Die Suche nach Tauschpartnern geht so lange weiter, bis die Datei komplett heruntergeladen ist.

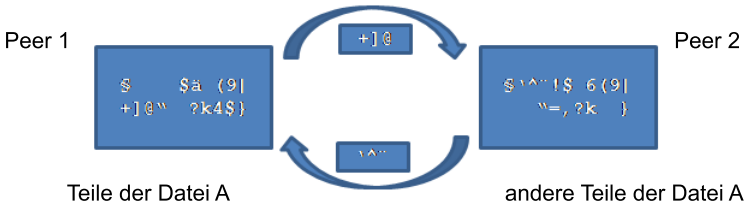


Abbildung 1.10: Tausch von Dateifragmenten

Sobald der Download komplett ist, kann man die Datei für andere User sperren, oder aber man bietet sie weiter als Seeder an. Ein Seeder ist ein Peer, welches eine Datei anderen anbietet, obwohl er sie bereits komplett heruntergeladen hat. Während dieser Zeit bietet man vor allem Benutzern, die mit dem Download der Datei beginnen wollen und selbst bloss andere Dateien zum Tauschen haben, diese an. Falls ein Peer länger als eine Minute keine Daten mehr hochlädt, hören auch die anderen Peers auf, ihm Daten zu senden [6].

Dieser Algorithmus ist noch mit vielen kleinen Optimierungen verbunden, trotzdem hat dieses einfache Tauschprinzip dazu beigetragen, BitTorrent heute zum weitverbreitetsten Filesharing-Netzwerk zu machen.

1.4.2.1 Datentausch in Permanent Storage Netzwerken

Algorithmen zum direkten Tausch von Daten gibt es auch in Permanent Storage Netzwerken. Da die knappe Ressource dort vor allem der Speicherplatz und die Speicherzeit ist, muss sich ein Algorithmus anders verhalten. Jeder Datei wird ein Tauschwert zugeordnet. Server können nun frei untereinander Dateien mit ähnlichen Tauschwerten handeln.

Durch die dynamische Durchmischung der Dateien durch das ganze Netzwerk erhöht sich die Verteilung und damit die Sicherheit des Systems. Damit ergibt sich auch ein Anreiz, Speicherplatz anzubieten. Jemand der selbst Dateien in einem solchen Permanent Storage Netzwerk speichern will oder diesen Service für andere anbietet, muss also im Gegenzug

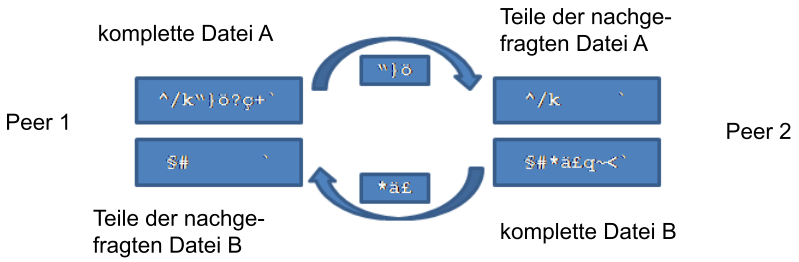


Abbildung 1.11: Tausch von ganzen Dateien

soviel Speicherplatz und Lagerzeit anbieten, wie er selbst beansprucht. Wichtig dabei ist, auch die Redundanzen zu beachten [23]. Um eine Datei zwanzig mal im Netzwerk zu speichern, muss er folglich zwanzig Dateien mit ähnlichem Tauschwert auf seinem Server speichern.

Im Gegensatz zu Filesharing Netzwerken werden hier, wie Abbildung 1.11 zeigt, ganze Dateien getauscht. Zudem spielt hier die Zeit eine Rolle, das heisst mit jedem Tausch verpflichtet sich der Server, die aufgenommene Datei bis zu ihrem angegebenen Ablaufdatum zu behalten oder nach Protokoll weiter zu tauschen. Ein *Server oeconomicus* würde seine Dateien gegen fremde eintauschen, die fremden jedoch sogleich trotz Abmachung wieder löschen, um selbst Speicherplatz zu sparen, was das ganze System auflösen würde. Deshalb muss hier zusätzlich zum Tausch jeweils eine Kontrolle stattfinden, ob die Abmachungen eingehalten wurden. Diese Kontrolle kann zum Beispiel von freien Spidern durchgeführt werden [11]. Eine weitere Möglichkeit ist es, dem Server, der die Datei zuerst ins Netzwerk gestellt hat, die Verantwortung der Überwachung zu übergeben. Andere Ansätze übergeben einem zufällig gewählten *Root-Server* diese Verantwortung [11]. Es gibt auch Implementationen, die auf einem *Buddy*-Prinzip beruhen. Dabei wird jeder Datei eine entfernte Kopie zugeordnet. Der Server, auf dem eine Datei gespeichert ist, überprüft dann regelmässig, ob der *Buddy* noch vorhanden ist [8]. Der Server muss somit für jede seiner Dateien ebenfalls die Information gespeichert haben, wo sich die zugehörige Partnerdatei befindet.

Um Fehlverhalten zu bestrafen, muss jeweils ein Reputationssystem vorhanden sein. Server, die ein Fehlverhalten feststellen, notieren dies, melden dies zum Beispiel per Broadcast [8] oder starten eine Wiederherstellung der Daten um die Redundanz aufrechtzuerhalten.

1.4.3 Bezahlung

Wie man in der Wirtschaft schon vor einigen Tausend Jahren entdeckt hat, kann der Tauschhandel mit hohem Aufwand verbunden sein. Durch ein transitiv wirksames Zwischenstück wie Geld können zeitliche und geographische Unterschiede wie auch verschiedene Bedürfnisse zusammengebracht werden. Genauso verhält es sich mit P2P Storage Networks.

Chun et al. haben in ihrer Arbeit *Selfish Caching in Distributed Systems: A Game-Theoretic Analysis* festgestellt, dass mithilfe Bezahlung immer ein Optimum für die Gesellschaft gefunden werden kann [4]. In ihren spiel-theoretischen Experimenten simulierten sie einen Markt, in dem Preise dynamisch nach Angebot und Nachfrage verhandelt werden [9][4].

Mit Bezahlung ist nicht sofort reales Geld gemeint. Es ist natürlich möglich, digitale Münzen, die zu realen umgetauscht werden können, zu benutzen. So kann auch mit anderen Währungen, wie zum Beispiel das *Mojo* im ehemaligen Mojo Nation, gehandelt werden [16].

1.4.3.1 Fungible Micropayments

Mojo war ein sogenanntes Fungible Micropayment. Im Gegensatz zu den Nonfungible Micropayments, die bloss zum Schutz vor Überflutung dienen, können erhaltene fungible Micropayments vom Empfänger weiterbenutzt werden. Jemand der einen Dienst anbietet, sei es nun langfristig Speicherplatz, dass er eine Datei uploadet oder auch dass er Rechenleistung zur Verfügung stellt, bekommt dafür virtuelle Münzen wie Mojo bezahlt. Diese wiederum können für eigene Bedürfnisse verwendet werden [24]. Somit kann jeder das verkaufen, was sein Computer am besten kann, sei es Bandbreite, Speicherplatz oder Rechenleistung und mit den erhaltenen Münzen das einkaufen, was er braucht, sei es Permanent Storage, Musikdateien oder sonstige Computerressourcen.

Ein grosser Vorteil zum direkten Tausch besteht auch darin, dass Micropayments in kurzen Abständen bezahlt werden. Ein Server, der Permanent Storage anbietet hat somit Interesse daran, die Datei auf seinem Server zu belassen, da dies sonst erkannt und die Bezahlung eingestellt wird. Um beidseitige Fairness zu garantieren, müssen die Micropayments genug klein sein und in genug kleinen Abständen bezahlt werden [7]. Wie oben erwähnt, können Preise immer wieder neu verhandelt werden.

Fungible Micropayments haben ein enormes Potential im Bereich von P2P-Netzwerken allgemein. Obwohl schon seit Jahren intensiv in diese Richtung geforscht wird, gilt auch jetzt noch die Aussage von Geels und Kubitron, dass noch kein genug sicheres, leistungsstarkes und günstiges System vorhanden ist, um digitale Münzen unfehlbar mit realen konvertierbar zu machen [9]. Besonders kompliziert wird es, wenn die einzelnen Parteien sowohl gegenüber dem Tauschpartner wie auch gegenüber der Bank anonym bleiben wollen [2].

Seit einigen Jahren gibt es kryptographische Ansätze wie DigiCash zur Lösung dieser Problematik, aber nur im Macropayment Bereich [7]. Weiter erschwert wird ein solches System dadurch, dass eine Transaktion meistens nicht direkt, sondern je nach Anspruch nach Anonymität über mehrere Zwischenstationen geroutet wird, welche alle ihren Teil beitragen, indem sie jeweils entschlüsseln oder neu verschlüsseln. Alle diese Zwischenstellen müssen ebenfalls mit Münzen bezahlt werden [7]. Dies kann momentan nur auf Kosten der Anonymität durchgeführt werden, da die Identität jedes Hops für die Zahlung von Micropayments bekannt sein muss.

Wie im Kapitel zu DDoS erwähnt, schützen fungible Micropayments auch vor Denial of Service Attacken. Nicht, dass sie ganz verhindert werden können, aber:

> With micropayments, you are, in effect, being paid to be attacked [26].

Ein weiteres Problem mit realen Micropayments ist psychologisch. Wer gibt schon gerne einem Server sein Portemonnaie zum verwalten, auch wenn natürlich Grenzen zur möglich sind, wie viel Geld ein Server pro Zeiteinheit maximal benutzen kann. Momentan ist es aber vor allem noch ein Problem der Mathematik wie auch des Bankensystems, bis Micropayments eingesetzt werden können, da die aktuellen Systeme zu einfach fälschbar oder zu teuer in der Umsetzung sind, verglichen mit dem Wert eines einzelnen Micropayments.

1.4.3.2 Macropayments

Das Konzept der Macropayments ist älter als die Micropayments. Im Gegensatz zu den Micropayments werden, wie der Name schon sagt, grössere Beträge verschoben, dafür weniger häufig. Die Algorithmen sind aufwändiger, dafür um einiges sicherer als Micropayments [7]. Die grösseren Beträge und längeren Zwischenräume setzen aber auch Vertrauen voraus, dass eine bezahlte Leistung auch erfüllt wird.

Umsetzbar und ökonomisch wären Konzepte wie in Anderson's Eternity Service oder in OceanStore, wo monatlich ein gewisser Betrag an ein Unternehmen gezahlt wird [2][11], sei es nun durch die oben beschriebenen anonymen Verfahren oder auf herkömmlichem Weg. Das Unternehmen verpflichtet sich als Gegenleistung dazu, die Daten sicher aufzubewahren.

Im Gegensatz zu herkömmlichen Servern, die Speicherplatz gegen Bezahlung anbieten, sind diese Firmen Teil eines grösseren, potentiell weltweiten P2P Storage Networks. Die verwalteten Dateien werden zusätzlich zur Aufbewahrung auf den eigenen Servern mehrfach auf dem ganzen Netzwerk verteilt. Im Gegenzug lagert die Firma Dateien von ähnlichen Firmen oder Privatpersonen auf ihren kontrollierten Servern [11].

Ein solches Angebot kann auch teilweise oder ganz werbefinanziert durchgeführt werden. In diesem Bereich ruht ein grosses Potential von sicheren P2P Storage Networks als Alternative zu teuren, und trotzdem bei weitem nicht so redundanten zentralisierten Angeboten.

1.5 Schlussfolgerung und Zukunftsaussichten

P2P Storage Networks haben viele, unterschiedliche Ziele. Damit wird klar, dass es nie die Killerapplikation schlechthin geben kann [26]. Die jeweiligen Implementationen müssen eine Kombination von sehr unterschiedlichen Technologien auswählen.

Eine totale Sicherheit ist nie möglich [21], aber durch eine geschickte Wahl von Systemen, sei es über zertifizierte Signaturen oder über Pseudonyme gekoppelt mit einem guten Reputationssystem, das eine Art soziales Netz ersetzt [13], ist eine Annäherung durchaus möglich. Wichtig ist, dass im Gegensatz zur aktuellen allgemeinen Praxis Sicherheit allgegenwärtig sein muss [21][11], ausser es wird vom System ausdrücklich anders verlangt. Daten sind immer verschlüsselt, die Konsistenz wie auch der Ursprung werden immer überprüft und Verbindungen finden über verschlüsselte Protokolle statt. Sicherheit darf nicht zu komplex für den User sein, da er sonst den Service nicht nutzen wird [21], deshalb muss Sicherheit wo immer möglich im Hintergrund und automatisch geschehen.

Natürlich ist dies keineswegs in allen Systemen verlangt. In Filesharing-Netzwerken soll der Zugang zu Dateien allen offen stehen. Eine Verschlüsselung ist somit nicht nötig. Aber auch hier wird ein Hash benutzt, um die Konsistenz zu überprüfen.

Um die Vorteile der P2P Technologie nutzen zu können, muss möglich sein, dass Peers frei das Netzwerk verlassen und wieder betreten, ohne die Funktionalität des Systems zu beeinträchtigen [7]. Dies wird vor allem durch Replikation erreicht. Je wichtiger eine Information, desto grösser muss die Redundanz und die Verteilung über das gesamte Netzwerk sein

Für Benutzer müssen und können Anreize geschaffen werden, damit nicht nur konsumiert, sondern auch Ressourcen angeboten werden [4]. Es gibt unterschiedliche Ansätze, dies zu erreichen. Ressourcen können direkt zwischen Computer getauscht werden, oder mithilfe von Micropayments kann ein transitiv wirksames System zum Kauf und Verkauf von Ressourcen aufgebaut werden. Es ist ein aktuelles Problem, Micropayments effizient und sicher an reales Geld zu koppeln. Aber auch die kommerzielle Nutzung von P2P Storage Networks gegen eine monatliche Gebühr ist eine Möglichkeit, die bestehende Konzepte von Datenspeicherung ersetzen oder ergänzen kann.

Das Internet hat mit der Kommerzialisierung eine andere Benutzergruppe und somit ganz andere Anforderungen erhalten. Ursprünglich war es sinnvoll, dass alle Benutzer sowohl Ressourcen anbieten wie auch konsumieren, weil die Wissenschaftler selbst Daten gesammelt und Arbeiten verfasst haben. Sie konnten im Internet nach heutiger P2P Philosophie ihre eigenen Ressourcen anbieten und gleichzeitig andere konsumieren.

Heute hingegen benutzt ein Grossteil der Benutzer das Internet privat nur als Konsument, das heisst, ein Grossteil hat meist selbst nichts zu veröffentlichen, das er anderen zugänglich machen will. Selbst für die Ausnahmen gibt es gut funktionierende zentralisierte Community-Systeme und Webhoster, die alle solche Bedürfnisse besser erfüllen, als P2P-Netze würden [16].

Die P2P Technologie hat heute mit vielen Problemen zu kämpfen. So erschweren Firewalls den Zugang zu vielen Servern und PCs [15], private Internetverbindungen sind heute meistens asymmetrisch eingerichtet, da private Anwender nicht als Anbieter von Ressourcen, sondern nur als Konsumenten gesehen werden, und DHCP und NAT geben Computern langfristig keine eindeutige Identität im Netzwerk [15].

Den Problemen muss mit Systemen wie dem Gebrauch von Pseudonymen und asymmetrischen Verschlüsselungsverfahren entgegengewirkt werden, damit Identitäten auch über

wechselnde IPs und gar über verschiedene Computer hinweg erkannt werden können, was bei rein konsumorientierten Systemen nicht nötig ist. Ein Computer, der einen Dienst auf einem zentralen Server benutzt, muss vom Server nicht über einen grossen Zeitraum aus identifiziert werden können, da jegliche Anfragen vom Computer ausgehen und nicht vom Server.

P2P muss man den jeweiligen Bedürfnissen anpassen. P2P kann als Basistechnologie im immer aktuelleren Zusammenhang der Virtualisierung verwendet werden. Das geht über das Auseinanderhalten der Informationen von ihren physischen Datenträgern [18][11] hinaus. CPU-Leistung, Netzwerkbandbreite usw. können in virtuellen Maschinen, die verteilt im virtuellen Netzwerk gespeichert sind, dynamisch nach Bedarf benutzt und per Micropayments bezahlt werden.

Als Grundlage zu so einem System könnte dezentralisiertes P2P dienen, gekoppelt mit den nötigen Pseudonym- oder Zertifikate- und einem Micropayment-System. Das P2P-System selbst besteht zwischen tausenden bis hunderttausenden von Servern auf der ganzen Welt. Ressourcen, aber auch Dienste werden dynamisch zu Tagespreisen automatisiert nach Bedarf bei den Anbietern eingekauft, während die Zuverlässigkeit der Server neben Zertifikaten auch mit verteilten Reputationssystemen sichergestellt wird.

P2P Storage Networks bieten für kleinere Datenmengen mit ihrer grossen geographischen Verteilung [11] günstige und mindestens so sichere Alternativen zu Hochsicherheitszentren, solange der Schlüssel zur Entschlüsselung sicher gehalten werden kann.

Auch unternehmensintern können virtuelle Datenserver erstellt werden. Virtuell, da sie intern aus einem P2P-System bestehen, das die Daten autonom und ohne externe Steuerung repliziert und damit die Verfügbarkeit auch bei einem Ausfall einzelner physischen Server sicherstellt. Die virtuelle IP auf dieses System kontaktiert einfach den nächsten verfügbaren Server, der Anfragen intern im Netzwerk weiter gibt.

P2P Storage Networks ist eine starke Idee, die Zukunft wird zeigen, ob solche Netzwerke auch längerfristig überleben können.

Literaturverzeichnis

[1] D. Anderson: *SETI@home*; In A. Oram (Editor): Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology, O'Reilly and Associates, Inc, Sebastopol, 1. Auflage, März 2001, S. 67-76.

[2] R.J. Anderson: *The Eternity Service*; In Proc. of Pragocrypt'96, 1996, S. 242-252. `http://www.cl.cam.ac.uk/~rja14/Papers/eternity.pdf`

[3] D. Bricklin: *The Cornucopia of the Commons*; In A. Oram (Editor): Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology, O'Reilly and Associates, Inc, Sebastopol, 1. Auflage, März 2001, S. 59-63.

[4] B.G. Chun, K. Chaudhuri, H. Wee, M, Barreno, Ch.H. Papadimitriou und J. Kubiatowicz: *Selfish Caching in Distributed Systems: A Game-Theoretic Analysis*; In Proc. of ACM Principles of Distributed Computing (PODC)'2004, Juli 2004, S. 21-30. `http://www.project-iris.net/irisbib/papers/selfish:pods2004/paper.pdf`

[5] I. Clarke, S.G. Miller, T.W. Hong, O. Sandberg und B. Wiley: *Protecting Free Expression Online with Freenet*; In IEE Educational Activities Department: IEEE Internet Computing, Piscataway, Volume 6, Issue 1, Januar 2002, S. 40-49. `http://freenetproject.org/papers/freenet-ieee.pdf`

[6] B. Cohen: *Incentives Build Robustness in BitTorrent*; In Proc. of the International Workshop on Peer-to-Peer Systems (IPTPS)'2003, Mai 2003. `http://www.bittorrent.org/bittorrentecon.pdf`

[7] R. Dingledine, M.J. Freedman und D. Molnar: *Accountability*; In A. Oram (Editor): Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology, O'Reilly and Associates, Inc, Sebastopol, 1. Auflage, März 2001, S. 271-340.

[8] R. Dingledine, M.J. Freedman und D. Molnar: *Free Haven*; In A. Oram (Editor): Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology, O'Reilly and Associates, Inc, Sebastopol, 1. Auflage, März 2001, S. 159-187.

[9] D. Geels und J. Kubiatowicz: *Replica Management Should Be A Game*; In Proc. of the 10th workshop on ACM SIGOPS European workshop: beyond the PC, 2002, S. 235-238. `http://oceanstore.cs.berkeley.edu/publications/papers/pdf/sigops-economy.pdf`

[10] T.W. Hong: *Performance*; In A. Oram (Editor): Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology, O'Reilly and Associates, Inc, Sebastopol, 1. Auflage, März 2001, S. 203-241.

[11] J. Kubiatowicz, D. Bindel, Y. Chen, S. Czerwinski, P. Eaton, D. Geels, R. Gummadi, S. Rhea, H. Weatherspoon, W. Weimer, Ch. Wells und B Zhao: *OceanStore: An Architecture for Global-Scale Persistent Storage*; In Proc. of ASPLOS'2000, November 2000. `http://oceanstore.cs.berkeley.edu/publications/papers/pdf/asplos00.pdf`

[12] A. Langley: *Freenet*; In A. Oram (Editor): Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology, O'Reilly and Associates, Inc, Sebastopol, 1. Auflage, März 2001, S. 123-132.

[13] R. Lethin: *Reputation*; In A. Oram (Editor): Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology, O'Reilly and Associates, Inc, Sebastopol, 1. Auflage, März 2001, S. 341-353.

[14] J. Miller: *Jabber*; In A. Oram (Editor): Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology, O'Reilly and Associates, Inc, Sebastopol, 1. Auflage, März 2001, S. 77-88.

[15] N. Milnar und M. Hedlund: *A Network of Peers: Peer-to-Peer Models Through the History of the Internet*; In A. Oram (Editor): Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology, O'Reilly and Associates, Inc, Sebastopol, 1. Auflage, März 2001, S. 3-20.

[16] T. O'Reilly: *Remaking the Peer-to-Peer Meme*; In A. Oram (Editor): Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology, O'Reilly and Associates, Inc, Sebastopol, 1. Auflage, März 2001, S. 38-58.

[17] A. Oram: *Afterword*; In A. Oram (Editor): Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology, O'Reilly and Associates, Inc, Sebastopol, 1. Auflage, März 2001, S. 393-397.

[18] A. Oram: *Preface*; In A. Oram (Editor): Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology, O'Reilly and Associates, Inc, Sebastopol, 1. Auflage, März 2001, S. vii-xv.

[19] C. Shirky: *Listening to Napster*; In A. Oram (Editor): Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology, O'Reilly and Associates, Inc, Sebastopol, 1. Auflage, März 2001, S. 21-37.

[20] E. Sit, A. Haeberlen, F. Dabek, B.G. Chun, H. Weatherspoon, R. Morris, M.F. Kaashoek und J. Kubiatowicz: *Proactive replication for data durability*; In Proc. of the International Workshop on Peer-to-Peer Systems (IPTPS)'2006, Februar 2006. `http://iptps06.cs.ucsb.edu/papers/Sit-tempo.pdf`

[21] J. Udell, N. Asthagiri und W. Tuvell: *Security*; In A. Oram (Editor): Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology, O'Reilly and Associates, Inc, Sebastopol, 1. Auflage, März 2001, S. 354-380.

[22] M. Waldman, L.F. Cranor und A.D. Rubin: *Publius*; In A. Oram (Editor): Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology, O'Reilly and Associates, Inc, Sebastopol, 1. Auflage, März 2001, S. 145-158.

[23] M. Waldman, L.F. Cranor und A.D. Rubin: *Publius: A robust, tamper-evident, censorship-resistant web publishing system*; In Proc. of 9th USENIX Security Symposium, August 2000, S. 59-72. `http://www.cs.nyu.edu/~waldman/publius/publius.pdf`

[24] M. Waldman, L.F. Cranor und A.D. Rubin: *Trust*; In A. Oram (Editor): Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology, O'Reilly and Associates, Inc, Sebastopol, 1. Auflage, März 2001, S. 242-270.

[25] Z. O'Whielacronx und B. Warner: *Tahoe Releasenotes version 0.6*; `http://allmydata.org/trac/tahoe/browser/relnotes.txt?rev=1346`, zuletzt besucht: September 2007.

[26] B. Wiley: *Interoperability Through Gateways*; In A. Oram (Editor): Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology, O'Reilly and Associates, Inc, Sebastopol, 1. Auflage, März 2001, S. 381-392.

[27] *BitTorrent*; `http://www.bittorrent.com`, zuletzt besucht: Oktober 2007.

[28] *BitTorrent and openSUSE*; `http://en.opensuse.org/BitTorrent`, zuletzt besucht: September 2007.

[29] *Emule*; `http://www.emule-project.net`, zuletzt besucht: Oktober 2007.

[30] *PostZertifikat - Die elektronische Unterschrift*; `http://www.post.ch/de/index_pm/pm_privatkunden/pm-postzertifikat.htm`, zuletzt besucht: September 2007.

[31] *www.dictionary.com: peer*; `http://dictionary.reference.com/browse/peer`, zuletzt besucht: September 2007.

Chapter 2

Ethernet Passive Optical Networks (EPON)

Lukas Fries

This seminar work gives an overview over Ethernet Passive Optical Networks (EPON). The EPON technology is seen as a revolution for access networks which have become more and more the bottleneck between the powerful backbone networks of service providers on one side and home or office-LANs on the other side. Existing technology in access networks such as Digital Subscriber Line (DSL) or Cable Modem (CM) cannot satisfy emerging demands for high bandwidth anymore. With passive optical networks (PON) there seems to be a solution for this problem. EPONs are passive optical networks that build up on the Ethernet protocol which is currently very widespread in local networks. They combine low-cost fiber infrastructure with low-cost Ethernet equipment and offer high bandwidth at the same time.

Contents

2.1 Introduction

Over the last years the demand for high bandwidth in networks has continuously increased. Data traffic has been growing by more than 100 percent per year [1]. Furthermore there are many emerging services that require high bandwidth availability in order to operate at a proper service level, such as Voice over IP (VoIP), video conferencing, video on demand or online computer games such as massively multiplayer online role-playing games (MMORPG). The past years, to cover the increased bandwidth need, service providers have invested a lot of money in their backbone networks to upgrade their available bandwidth. New services were offered for customers, such as DSL or CM. These services were successors of the analog modem which was operating at a line speed of 56 kb/s. With the new services, customers had an increased bandwidth available of 128 kb/s up to 1.5 Mb/s (DSL). Cable television providers used their existing cable television networks to offer data services too. Their networks were often hybrid fiber coax (HFC) networks where fiber lines reach from the distribution office (head-end) to a curbside optical node. From there on the signal is distributed using coaxial cable infrastructure. Such a curve node offers bandwidths around 36 Mb/s. But this bandwidth might then be shared between up to 2000 households. In peek times this leads to an incredible slow network speed from a single users perspective.

In the office or at home, customers use LAN infrastructure which operate at bandwidth rates off 100 Mb/s (Ethernet infrastructure most common). Newest WLAN standard drafts where devices are already available on the market offer up to 300 Mb/s transmission rate [12]. Service provider backbones operate at speed rates of 10 Gb/s. The access networks, also called the last mile or the first mile networks, which connect the above networks operate at a speed of 1 Mb/s per node and below. It is therefore obviously that the access networks function as bottlenecks between the two high bandwidth networks. How can the infrastructure in access networks be upgraded to comply with bandwidth demands from customer networks (subscriber terminals) in direction of service provider networks (central office) and vice versa? Upstream and downstream bandwidth has to be strongly improved.

For common Internet use and applications like messaging or online games the existing infrastructure might be sufficient (at least on average). But in times of emerging VoIP and video conferencing applications there is a crucial need for more bandwidth, because these applications are sensitive to packet-delay, jitter or even worse, packet-loss. To guarantee the best transmission rate for these time-sensitive applications, quality of service (QoS) can be used. With this technology data packets are priorised within the network thus offering the higher classified packets a better transmission rate. But QoS only makes sense if the transport medium has enough bandwidth. In congested networks even QoS might not help anymore to prevent from packet-loss or similar problems. Another issue is the fact that market research has shown, that users spend 35 percent more time online after they received a bandwidth upgrade on their subscription [1]. Because of these new emerging, heavy-bandwidth consuming services, the gap in the access networks has to be eliminated.

Why can't the existing infrastructures be upgraded to higher bandwidth? Cable television networks might actually offer a higher bandwidth by using more channels for their data

traffic. But these channels are currently occupied by analog video services. For both technologies, DSL and CM, there are quite strict distance limitations. DSL for example has a distance limitation of less than 5.5 km. This distance-radius only contributes about 60 percent of subscribers (end-users) [1]. Current technologies are implemented using copper cable infrastructure which has relatively high signal loss over distance and through connectors as well. In addition these networks contain a lot of electronics between the central office and the subscriber terminals (active networks). Live electronics need to be maintained and devices operating in active networks may also need backup power devices in case of a power failure, to deal with potential power losses. Though it is still possible to upgrade existing infrastructure by expanding the current equipment with new devices and new cabling infrastructure that runs parallel to the current network infrastructure. But it is expensive, requires high maintenance and doesn't even offer very high bandwidth availability.

First this paper will give an introduction into passive optical networks in general and talk about such network architectures. Then the main content focuses on EPONs, Ethernet Passive Optical Networks. The structure is built up as follows. After the introduction to PONs,, the paper will discuss why Ethernet became the favoured protocol for a PON and therefore lead to the EPON technology. The following section relates to the history of passive optical networks and standards that have been developed. After finishing with the latest EPON technology the next chapter explains EPON architectures in general and gives examples. The architecture section then leads to the multiplexing mechanisms and dynamic bandwidth allocation algorithms. The end of this document discusses security and hardware issues that EPONs have to deal with.

2.2 Passive Optical Networks

If the expansion of copper access network infrastructure is not the solution, there has to be another option. Prices of optical network components such as fiber cables, connectors and network devices are dropping continuously. As of today it seems that optical components are becoming more cost-effective than electrical copper-based components in the long run [2]. This opens the door for a new kind of networks, passive networks that are built upon optical components. Passive networks are networks that make not use any power supply to transmitt signals, except at the line terminating devices. The term passive stands for components without any power-consuming (e.g. fiber cable). Active on the other hand means power-consuming parts such as a common STP copper cable. This section will explain in three steps how passive optical networks can be used to overcome the limitations of the current access networks.

Step 1: Overcome the costs of active network parts. Current infrastructures consist of active copper networks. These installations contain a lot of electronical parts and require a power connection to be operated. A signal can only be transmitted through a copper network by means of an electronical signal. Electronical devices are power consuming, maintenance-intensive and might even require a backup power solution like uninterruptible power supplies (UPS). This maintenance and the necessary backup installations to operate an active network lead to high costs. Additionally it is hard to search for errors in active

networks, because signal loss cannot be located easily. Optical components are - contrary to copper components - pure passive parts. They are just the carrier for a signal (laser transmission). A fiber cable does nothing at all, it just conducts through the laser signal. Only the two line-ends are active (for example two laser transmission nodes). Optical devices offer minimal maintenance and servicing costs when operating a fiber plant.

Step 2: Overcome distance limitations. As mentioned before, current access network installations like DSL have a distance limitation of 5.5 kilometers. Signal loss is much stronger in copper networks than in optical networks. Fiber installations have distance limitations of 20 kilometers or even more. Within this distance radius a service provider can cover many more of his potential customers.

Step 3: Overcome shared bandwidth limitations. Cable modem networks use a shared node at the curve switch installation. Therefore subscribers are sharing their bandwidth with many other users. To overcome these limitations optical networks offer a sophisticated solution using multiplexing techniques. They allow to divide a single physical channel into several virtual channels, offering a dedicated channel for each user and full bandwidth at the same time.

For above reasons, optical components offer low-cost hardware for high bandwidth-availability and therefore fit perfectly to build optical fiber networks closer to the subscribers [3]. Another benefit of fiber infrastructure is that fiber cables have a very low signal loss compared to copper components. Fiber offers high bandwidth availability over long distances. Due to the above facts, the last mile network infrastructure is changing from copper-based components towards optical components. This new emerging technology is also known as FTTx (fiber to the home, curb or building) [1]. Additionally fiber networks are future-safe. Passive fiber network infrastructure does not offer any services itself, the infrastructure is independent of the services running on it. Therefore bandwidth is also not depending from infrastructure. Bandwidth upgrades can be done by expanding the end terminating hardware.

Because of their passive nature these networks are called passive optical networks (PON). The first PONs have been introduced in the late 1980s for telephony [4]. Since then several improvements have been made. As of today several different types of PONs exist. Examples are the ATM Passive Optical Network, Gibabit Passive Optical Network and the most widespread, the Ethernet Passive Optical Network (EPON). In general PONs function as a point-to-multipoint network consisting of one Optical Line Terminator (OLT) and several Optical Network Units (ONU). The OLT is located in the central office and transmits traffic towards the ONUs which work as customer terminals. Traffic from the central office to the subscriber terminals is referred to as downstream traffic. On the other hand an ONU receives the downstream traffic from the OLT and forwards it to the attached devices. They send back their responses to the ONU which then sends its data towards the OLT. This type of traffic is called upstream traffic. In most of the common network topologies a remote node (RN) or access node (AN) is used between the OLT (central office) and the ONUs (subscribers). A trunk leads from the OLT over a long distance closer to the customers where the Remote Node is located. There the signal from the central office is split and sent to every customer's ONU. This process is done by the splitter/combiner devices.

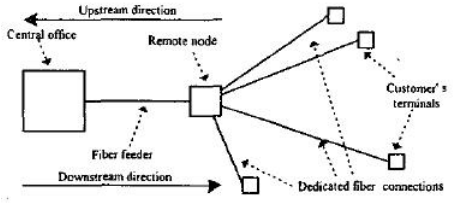


Figure 2.1: Generic point-to-multipoint architecture of a passive optical network. The shown connections represent either a single fiber or two fibers carrying resp. up- and downstream traffic [4]

There are many reasons for using a PON as an access network which has many subscribers. Despite of the dropping prices for fiber components, optical parts are still quite expensive, especially with regard to the components that have to be used at the central office. These components require state-of-the art fiber technology and large computational power to deal with network traffic management. With a PON the fiber feeder (trunk from OLT to RN) and equipment in the central office can be shared among the customers. In a conventional point-to-point network, there would be a need of having the same fiber equipment once per customer. Because PONs are point-to-multipoint networks, equipment in the central office is only needed once (disregarding the fact of a possible redundancy). Besides the reasons of high costs there is also a lot of rack space savings in the central office. There is only one line per PON that leaves the central office. This reduces space used for fiber connectors. This sharing principle creates a cost-assymetry. Professional and highly reliable network equipment can be used in the central office without heavy connection cost per individual subscriber (shared costs) [4].

Network equipment at customer sites has to be as simple and cheap as possible. The OLT at the central office deals with all tasks that require more computational power such as network management for example. Additionally the OLT has to be a stable, reliable device that supports fail-over mechanisms and load-balancing. It is not the responsibility of the individual subscribers to deal with network management operations. The ONUs can be held as simple as possible because they only need to receive downstream packets and send upstream packets. They do not care about network topology, reliability or network load. Further details about the features of OLTs and ONUs are discussed later in Section 2.5.

2.3 Ethernet

The most common PON installations today are typical passive optical networks that rely on the Ethernet 802.3 protocol as data link protocol. These networks are called Ethernet Passive Optical Networks (EPON). As of today EPONs are widespread in commercial use. The deployed volume is about 3 million lines and the installed central office capacity reaches 10 million ports [16]. The following section should give an understanding about the role that Ethernet plays in the PON world and why Ethernet PONs have achieved such a high attendance.

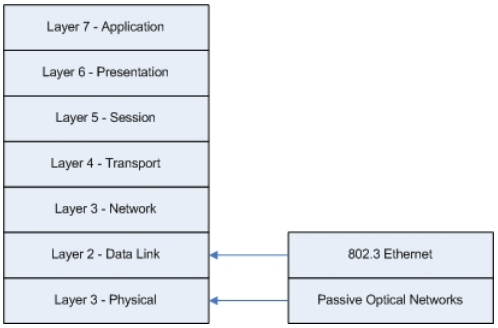


Figure 2.2: OSI Layer Model

Basically PONs work with any layer 2 protocol (data link layer). In the beginning of PON history the asynchronous transfer mode protocol (ATM) was favoured for PONs. But by the time several shortcomings when using ATM in PONs came out [1].

2.3.1 Disadvantages of Other Techniques Given the Example of ATM

ATM caused a problem with high waste of bandwidth. Since ATM uses quite small cells to transfer data over the network, data of an upper-layer protocol such as IP is fragmented into many ATM cells and transmitted over the media. If a single ATM cell gets corrupted or dropped the whole stream becomes worthless and has to be retransmitted. A dropped or corrupted ATM cell invalidates the entire IP datagram. Nevertheless, the cells with the remaining parts of this IP datagram will propagate further and therefore consume network bandwidth to send an already corrupted transmission. The Ethernet protocol aborts a transmission if it detects a collision or similar events.

Additionally ATM causes a lot of overhead traffic because it uses so small cells compared to an Ethernet frame. The relation of header size to payload size is not optimal in an ATM cell. Every cell has a 5 byte header and 48 bytes of payload while the Ethernet frame comes with 14 bytes header plus 4 bytes of checksum and a payload of up to 1500 bytes. When sending large data streams the ATM cells generate a huge overhead because of their 10 percent header data compared to 1 percent header data in an Ethernet frame. The smaller cells lead to a much higher fragmented data stream with more header information that would be better consolidated in the larger Ethernet frame. The small ATM cells were originally designed to deal with jitter problems and packet delays in networks caused by multiplexing of data traffic. Ethernet frames were situated worse concerning packet transmission reliability. Because of their header the ATM cells could be reassembled to their original data packets even if some of them arrived in wrong order. But since the introduction of Quality of Service for the Ethernet standard, it makes the Ethernet even more suitable for time-sensitive applications than ATM. QoS eliminates the drawbacks of Ethernet regarding reliability of packet transmission in time-sensitive applications [23].

Another disadvantage of ATM is its costs. Ethernet technology has become widespread available and cheap while ATM technology is still very expensive. Ethernet components

are about eight times less expensive than ATM components [1]. All these facts offer a serious advantage when building a PON by using Ethernet instead of ATM.

2.3.2 Advantages of Ethernet in PONs

First of all, Ethernet fits perfectly with the architecture of passive optical networks since it is broadcasting by nature. In a PON the OLT broadcasts packets in downstream direction towards all ONUs. The ONUs then extract the packets with destination MAC addresses that match their own address. Second, the upstream traffic is sent by the ONUs on a shared channel and therefore has the need of a collision avoidance or multiplexing mechanism. Ethernet offers built-in mechanisms like the CSMA/CD protocol for example. Basic functionality is already existing but as will be shown later the collision avoidance in EPONs is slightly different. Third, the use of Ethernet in PONs instead of other protocols means that existing Ethernet plants don't have to be replaced by other proprietary installations. They just can be reused.

Concluding the above sections, the Ethernet protocol can be used without further modifications. Existing Ethernet plants can be interlinked with EPONs and none of the existing technologies has to be changed. Another positive fact is that Ethernet is very widespread as of today, offers high bandwidth and is available at comparable low-cost. Existing plants don't have to be modified to be capable of supporting an EPON connection. However, besides all advantages that an EPON offers it also seems to be much of a political discussion between different communities. The IEEE society seems to be quite strongly established in the area of passive optical networks.

2.4 Historical Evolution of PONs - Workgroups and Standards

To get an understanding why EPONs have become so important in the development of passive optical networks, it makes sense to throw a glance at the evolution of PONs. The following section is divided into five parts. The first four subsections discuss the very general PON standards that have been developed while the last one focuses on the proprietary standards where the PONs were designed exclusively for the Ethernet protocol standard IEEE Std 802.3 [7].

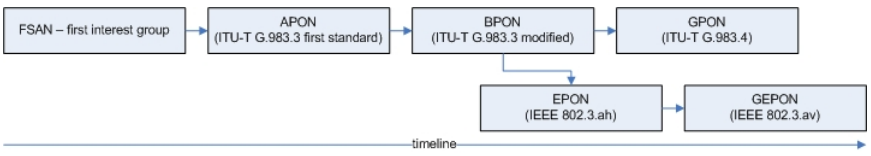


Figure 2.3: History of PON

2.4.1 FSAN

As already mentioned above, the first PON ideas were introduced in the late 80s. The Full Service Access Network group (FSAN) has been founded as an interest group for the world's leading telecommunications service providers. The FSAN was working on the fiber to the home (FTTH) architectures [6]. The idea was to overcome the bottleneck in the access networks by providing fiber technique as close to the home as possible.

2.4.2 APON

The first official standard was then released by the International Telecommunication Union (ITU). The ITU did further work on the FSAN's studies and released the first PON standard, the ITU-T G.983.3 standard [13]. The first version of a PON was based upon the asynchronous transfer mode protocol (ATM). Because of the ATM protocol used on the data-link layer, the first PON standard is known as ATM PON (APON). In 2001 the ITU-T G.983.3 standard has been approved the first time, but considerable further work has been done later in this area, continuing into 2005 [13].

2.4.3 BPON

Due to several drawbacks of the ATM protocol it fell out of favour as the standard protocol used for data transmission in a PON. With further improvements and the omission of the ATM protocol the former APON standard was now more referred to as Broadband Passive Optical Networks (BPON) rather than APON. The BPON standard does not rely on a specific protocol for data transmissions.

2.4.4 GPON

Shortly after work on the BPON standard was done, the ITU released the next standard for Gigabit Passive Optical Networks (GPON), ITU-T G.983.4 [14]. The standard was backwards compatible to the old BPON standard but allowed for higher data transmission rates by the use of sophisticated bandwidth allocation algorithms. The newer standard is still not protocol-specific. It discusses new methods of bandwidth allocation in a PON to achieve higher data transmission rates. Further information about this topic can be found in Section 2.7.

2.4.5 EPON / GEPON

Another society which took part in the race for newer PON standards was the IEEE computer society. The Ethernet in the First Mile Taskforce (EFM) was a dedicated group, which has been established within the IEEE to deal with the same problem that

the ITU-T already dealt with - migrating the first mile towards optical installations to overcome the bandwidth bottleneck caused by the access networks. Other than the ITU, the EFM worked on a PON standard that used a dedicated data-link layer protocol. The idea was to build a standard for PONs using the Ethernet protocol. Building up on the BPON standard the EFM's work lead to the IEEE Std 802.3.ah standard [10]. This standard is known as the Ethernet Passive Optical Network standard (EPON). The EFM consortium is no longer active since its work has been completed and integrated to the IEEE standard IEEE Std 802.3.ah by June of 2004. The EFM's work has lead to the publication of several advantages that the Ethernet protocol offers compared to other protocols in a PON architecture. Further work on developing better EPONs is now done by the IEEE under the name of 10G EPON system standardization - the IEEE Std 802.3.av [11].

2.5 EPON Architectures

The basic idea beyond EPON or PON in general is to deploy optical networks everywhere. There are several terms that have been created for this idea. FTTx, fiber to the x where x stands for home, business or curve is the common expression. Fiber installations should reach as close to the subscriber as possible. To implement this idea there are several topologies that have been proposed. They are not new but inherited from already existing topologies that have been in use in the Ethernet landscape before.

The challenge that comes with an EPON is mostly its high costs. Although prices are continuously dropping, optical network components are still very expensive. Because of that, fiber cabling installations have to be as economical as possible regarding the length of fiber distribution. Even more expensive than fiber cabling are the optical network devices, especially the OLTs. Therefore it is the intention to share the costs for such devices among the customers.

The solution of the above challenges is simple from a theoretical approach, but cannot always be implemented one-to-one in practice. Optical Line Terminals should be installed in the central office and offer its services to many customers at the same time. The devices at the subscriber terminals should be as simple as possible from a technical perspective. With this approach, costs for the devices can be divided up among the customers and the equipment at customer nodes is kept simple and cheap. Additionally service providers have to use cabling architectures that avoid unnecessary waste of fiber. Good topologies should therefore provide most efficient cabling and shortest possible round-trip-times (distance). To give a better understanding about such topologies, the next sections explain different topologies, their benefits and drawbacks.

2.5.1 General EPON Architecture

The EPON architecture in general can be seen from two perspectives, the downstream channel and the upstream channel. Downstream traffic is broadcasted from the central

office towards all subscriber terminals. In downstream direction data are sent from the Optical Line Terminal (OLT) which is located in the central office, towards the Optical Network Units (ONU) located at client sites. The OLT broadcasts its data towards all ONUs. The ONUs read incoming traffic and analyse the header information. If an ONU finds its own MAC address in the packet's header information about the destination MAC address, it accepts the incoming traffic and forwards it to the attached devices, otherwise it drops the data packets.

Upstream traffic on the other hand can be seen as point-to-point traffic. Each ONU sends its own data explicitly towards the OLT. Data sent from an ONU cannot be seen by other ONUs. Because all attached ONU devices send their traffic to the same OLT it is obviously that this causes problems because of a shared upstream media channel. To avoid collisions and congestion, special multiplexing and collision avoidance mechanisms are deployed. These techniques will be explained in further details in Section 2.6.

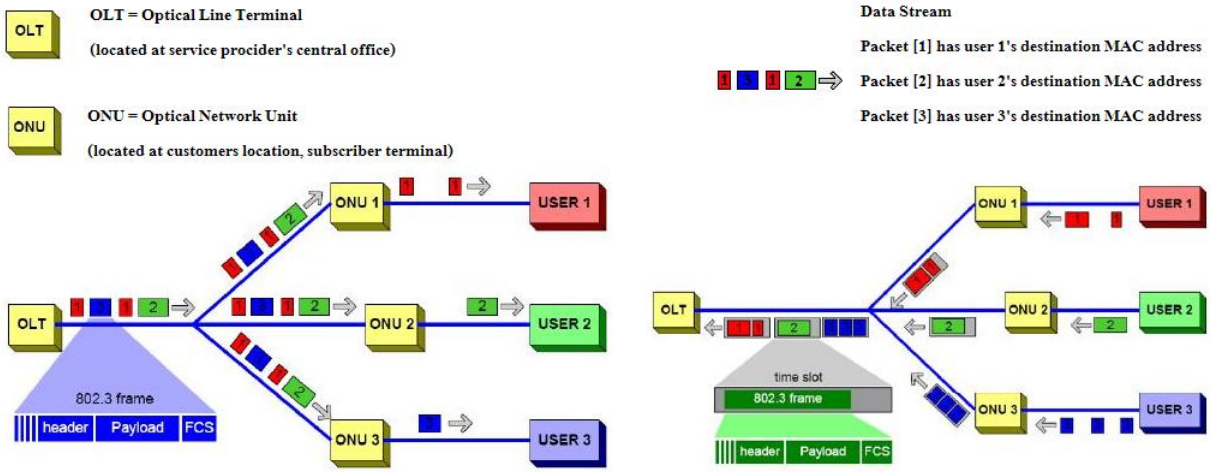


Figure 2.4: EPON Architecture Overview [24]

2.5.2 Bus Architecture

The most simple architecture goes back to the beginning of the Ethernet age and the first network installations. They used a bus topology where all devices shared a single transmission media. The same principle can be used for PON topologies. A bus leads away from the OLT. Each ONU connects to this bus by the use of a splitter/combiner device. This device splits the signal transmitted on the main bus and branches a small portion off for the connected ONU, while the main part of the signal continues on the bus. Each ONU connected leads to a small signal loss on the main bus caused by the branching of the signal. The advantage of the bus topology is its simplicity and the ease of its implementation. On the other hand, a bus topology creates a single, huge collision domain for the whole bus. This forces the application of multiplexing techniques which then could lead to a more complex installation.

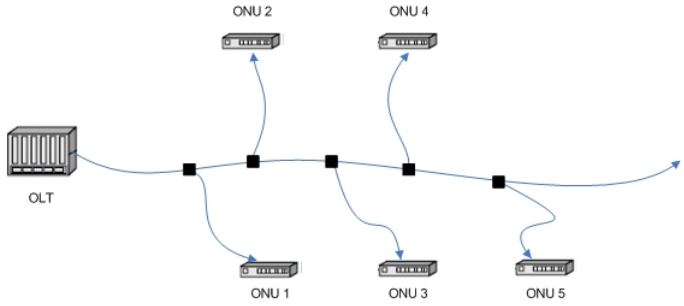


Figure 2.5: Bus Topology

2.5.3 Tree Architecture

An improvement of the bus topology is the tree architecture. Basically, a bus still leads away from the OLT. But instead of the single shared bus mentioned above, a so called trunk leads from the OLT towards the subscriber terminals. The trunk connects the OLT with a splitter/combiner device near customer locations. From there on all customers are connected to the splitter/combiner. This device receives the downstream signal from the OLT, replicates the signal and then sends it to each ONU. In the upward direction the ONUs send their traffic towards the OLT and all signals are combined at the splitter/combiner. The ONUs are connected to the splitter/combiner device each with their own lines. This technique reduces the shared media to only the trunk that carries all signals together. The most powerful cable installation will be the trunk, while branch lines to the subscriber terminals can be more simple. This leads to lower installation costs. Nevertheless, the tree architecture is more complex to implement than the bus architecture.

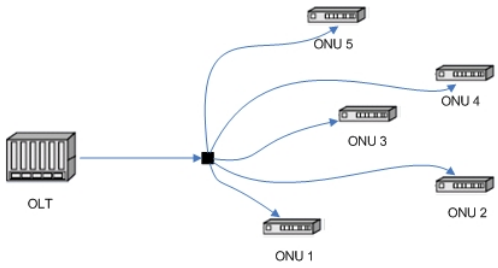


Figure 2.6: Tree Topology

2.5.4 Ring Architecture

Another alternative topology is the ring architecture. Basically a ring is quite similar to the bus architecture, but the trunk goes back to the OLT again. All ONUs are directly connected to the trunk and like in the bus topology they are connected by splitter/combiner devices which branch off part of the signal. There are two important features that a ring topology offers in contrary to other technologies. First, in a ring topology all ONUs are theoretically interconnected and would therefore be able to exchange traffic directly

between ONUs. The ONUs can see each other's upstream traffic (if configured properly) which is not the case in all other topologies. Second, the ring is a closed instance which enables the OLT to measure exactly what happened to the signal that has been transmitted through the trunk (e.g. signal strength at transmission start and signal strength at signal return). This special ability can be seen as huge advantage over other topologies because it is very important for security aspects and will be discussed again in Section 2.8. A drawback of the ring topology is its high cost of cabling infrastructure and not like the tree the ring consists of a single collision domain again. Because of its ring-form there is more fiber needed than in a tree infrastructure. Also the fact that upstream traffic can be seen by all ONUs, leads to complicated security measures when protecting each ONU's private traffic.

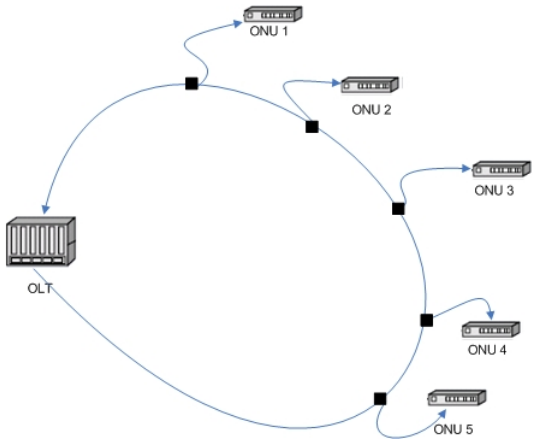


Figure 2.7: Ring Topology

2.5.4.1 A Novel Ring Architecture

The drawback of potential long round trip times and heavy cabling infrastructure due to large circle diameters can be overcome using a special kind of the ring architecture - a hybrid ring architecture [19]. This architecture combines the advantages of the tree and the ring architecture while trying to eliminate the drawbacks of both architectures. The idea is to extend the ring topology closer to the end users by having a trunk again from the OLT to the splitter/combiner device that is located close to the subscriber terminals. From there on all ONUs are integrated into the circuit again. The splitter/combiner works a bit different than in the tree architecture. It does not replicate the signal but just forwards it onto the ring. At each connected ONU there is another splitter that branches off a bit of the signal while passing through the rest of the signal. At the end of the ring when the signal comes back to the splitter/combiner the downstream traffic is filtered out (otherwise it would circulate twice on the ring) while the upstream signal is passed onto the trunk towards the central office's OLT.

2.5.5 P2MP

As can be shown by the architectures mentioned above, EPON systems are a mixture of different media types. In downstream direction packets are broadcasted by the OLT towards all ONUs. Extraction at the ONUs is done if the packet's destination MAC address matches the ONU's MAC address. This broadcasting nature is an unique indicator for a shared medium. On the other hand, the upstream traffic works completely different. Each ONU sends its traffic towards the OLT, but not to the other ONUs. The OLT processes frames from any ONU. This indicates a point-to-point medium. EPONs are therefore a mixture of both architectures, which is called a Point-to-Multipoint architecture (P2MP). Because EPONs use a shared upstream channel they also have to deal with several security issues. All connected ONUs on a network might break into the traffic of other units and use eavesdropping mechanisms to read foreign information. Section 2.8 will discuss this in further details.

2.6 Multiplexing in EPONs

EPONs do not call for complete new designs in network architecture. Basically existing architecture principles can simply be adopted to EPON designs. Nevertheless, passive optical networks have a different network structure than most of the formerly used networks. As explained above they consist of a point-to-multipoint (P2MP) architecture, which leads to several problems with the upstream channel. Devices at subscriber terminals (ONUs) share a common upstream channel. To avoid collisions during transmissions there need to be either collision avoidance and prevention mechanisms or a single physical channel needs to be divided into multiple virtual channels. Ethernet already provides a solution with the Carrier Sense Multiple Access / Collision Detection mechanism (CSMA/CD). But because EPONs are of a P2MP architecture such mechanisms are hard to implement. EPONs are non-deterministic networks. The OLT does not know what happens with the broadcasted downstream traffic and the ONUs don't know what happens with their upstream traffic. Therefore it is difficult to recognise collisions in such a network. Nevertheless the OLT could possibly detect a collision in the upstream channel and then send a jam signal to all ONUs. But because of the nature of EPONs, which may consist of links with a distance of more than 20 kilometers, it is difficult to realise this mechanism. ONUs have strongly differing round-trip times and therefore react too late or to early by resending their transmission. With the original purpose of Ethernet this would not have been an issue because the targeted networks were local area networks (LANs).

A better way to deal with the problem of a shared upstream channel are multiplexing mechanisms. Different techniques can be used to manipulate the upstream signal of each connected ONU in a way that no more signal collisions can occur. The single physical upstream channel is divided into several virtual (or even new physical) channels, each ONU gets a dedicated upstream channel.

2.6.1 Time Division Multiplexing

Very widespread is the use of the Time Division Multiplexing (TDM) procedures to guarantee a frictionless upstream transmission of all ONUs. To avoid collisions in the upstream channel, each ONU is allocated a given time slot to send its data. The OLT maintains these time slots and decides which ONU is allowed to send data at what time. While waiting for permission to send, an ONU stores incoming data from its clients in the built-in buffer. At the time when the sending permission from the OLT arrives, it bursts its stored data out at full channel speed, until the sending permission expires. If the OLT maintains the allocation of time slots, this is called a centralised approach. If an EPON consists of a ring architecture there is also the possibility of using a decentralised time allocation approach. There ONUs themselves decide when to send data and for how long [1]. Before an ONU sends its data it will send a special message to announce how many data bits it will send afterwards. The succeeding ONU therefore knows when the predecessor finishes data transmission and it will start the own data transfer right afterwards. Time frame allocation can be done either static (fixed time slot) or dynamic (variable time slot). Dynamic bandwidth allocation will be described in a separate section.

Time division multiplexing offers a cheap way of implementing a multiplexing technique. No additional or special hardware is required. The OLT gets by with just a single transceiver for all upstream traffic. On the other hand TDM does not truly create more channels, it just splits one physical channel into several virtual channels. Therefore the bandwidth offered in a TDM EPON is the full channel speed divided by the number of ONUs (variations depending on the bandwidth allocation mechanisms). Another drawback of static TDM mechanisms is a waste of bandwidth. Each ONU always receives the same transmission window. But if an ONU has nothing to transmit it just sends idle signals, while at the same time, other busy ONUs might require more sending time.

2.6.2 Wave Division Multiplexing

Whilst TDM uses a single physical channel and shares it by using different time slot allocations for the attached ONUs wave division multiplexing (WDM) works different. It creates truly new physical channels upon a single channel. Optical components are used to split the transmission signal into several wavelengths. Each ONU gets assigned a dedicated wavelength. Down- and upstream traffic are always in the wavelength according to the involved ONU. From a theoretical view WDM is very simple, there are no complex algorithms needed to share a channel. However WDM is very cost-intensive solution and therefore not the best way of implementing multiplexing in an access network. WDM requires either a tunable laser which can be adjusted for each ONUs wavelength or a receiver array at the OLT to receive multiple channels. In addition the ONUs require a specific wavelength configuration which is either hardware based or requires a tunable laser too. Regarding the current state of the art, tunable lasers are very expensive devices and therefore prohibitive for a cheap access network [1]. Hardware specific ONUs would mean that different types of ONUs have to be installed which makes the installation complex and expensive. In addition to the problems with tunable lasers or laser arrays, it is also very important that the wavelength of the lasers in the central office precisely matches the

wavelength of the laser at the remote node [3]. The ring architecture offers a good approach for a closed feedback loop, so that wavelengths of both channels (upstream/downstream) can be locked. Contrary to access networks, provider backbone networks often adopt WDM techniques because it offers highest bandwidth availability (each channel operates at full speed). Recapitulatory WDM offers a true separation of transmission channels and good protection against security break-ins because ONUs can only see their own traffic. Against these advantages stands the cost argument which theoretically prohibits the use WDM mechanisms in access networks because tunable optical lasers are still very expensive.

2.6.3 Subcarrier Multiplexing

A good alternative to wave division techniques is offered by the subcarrier multiplexing (SCM) technique. SCM works similar to WDM because it also modifies the wavelength of the different up- and downstream signals. But in contrary to WDM where optical components are used, SCM relies on electrical signal modification in the radio frequency domain. This signal is then transmitted by a single wavelength (from an optical perspective). Each subscriber gets a unique frequency assigned, the so-called subcarrier frequency, by which the original signal is modified [3]. The advantage of microwave devices is their maturity when compared to optical devices. Electrical components offer a much better frequency selectivity than their optical counterparts. At the same time these devices are cheaper than the complex optical devices. Signal modulation in the radio frequency causes very narrow bandwidth channels. Engineering and installation of such networks has to be done very carefully, to avoid frequency distortions which could cause misinterpreted signals. For example, two frequencies that lie close to each other could also be seen as a single signal with distortions.

Subcarrier Multiplexing can also be combined with Wave Division Multiplexing. With the combination of both techniques a network can use its full bandwidth with the most available channels while still separating different channels physically. [20] discusses a SCM test where a 10 Gb/s network has been set up. Four 2.5 Gb/s data streams have been combined into a single optical channel that occupies 20-GHz bandwidth. On such a network there could be several optical channels with 20-GHz bandwidth of which each is divided into four data streams using SCM technique.

2.7 Dynamic Bandwidth Allocation

EPONs that use time division multiplexing need mechanisms to allocate time frames to its connected ONUs. Static configurations always allocate the same frame size to each ONU with no respect to their effective load. This can cause heavy waste of bandwidth because idle ONUs will transmit idle signals when its their turn to send. Idle ONUs waste bandwidth while busy ONUs have to drop packets because their transmission buffers overflow. Another problem with static procedures is given by the fact that all ONUs need to be synchronised according their system time. Otherwise it could happen that unsynchronised

ONUs send their data at the same even by using different time slots, because their system time is different. To avoid such waste of bandwidth and the complexity of synchronisation, statistical (dynamic) mechanisms can be implemented. Such mechanisms contain complex algorithms that (re-)calculate time frames allocated to an ONU depending on priority or traffic load of the respective ONU. With dynamic bandwidth allocation (DBA) the available bandwidth per channel can be increased significantly.

When implementing a DBA approach a new challenge arises. EPONs are non-deterministic networks. ONUs don't know each other and the OLT does not know how much traffic ONUs have stored in their buffers. To deal with this problem, DBA protocols make use of special messages to exchange information about the network. The IEEE 802.3ah Task Force developed the Multi-Point Control Protocol (MPCP) to resolve problems related with the conventional P2P operations in P2MP networks [17].

2.7.1 Multipoint-to-Point Control Protocol

The MPCP offers mechanisms to dynamically allocate access to the optical transmission medium (single channel). The protocol divides the available channel bandwidth into timed slots (transmission units). These slots are then assigned to the attached ONUs by the OLT, based on the deployed DBA algorithm. MPCP communication uses two type of messages, the REPORT and the GATE MPCP DU [17]. The ONUs use the REPORT MPCP DU to inform the OLT about their current bandwidth demand. The OLT then calculates the available bandwidth and time, regarding possible service policies and bandwidth demand of all other ONUs. Then, the OLT sends a GATE MPCP DU to the ONU containing size and start time of the transmission. Synchronisation of all ONUs is done by the GATE MPCP messages, there is no need for additional synchronisation. Each time an ONU receives a GATE message it updates its internal clock with the information contained in the GATE message.

The build up process where the information which is necessary to operate the MPCP is collected is called discovery process (or ranging). In this quite complex process, the OLT collects information about the round-trip time (distance) to its connected ONUs and synchronises the ONU's clocks by sending system messages which contain OLT's central system time. While discovery is ongoing all standard data transmission has to be stopped and only protocol messages are transmitted through the network. This causes a network interrupt each time an ONU (or at least a new logical link) is connected to the network. Mechanisms like the IPACT protocol have been designed to overcome such problems.

2.7.2 IPACT Algorithm

To give a further understanding of the DBA methodology, a special DBA protocol is explained in this section - the Interleaved Polling with Adaptive Cycle Time (IPACT). It uses very sophisticated mechanisms to avoid the waste of bandwidth as good as possible while offering optimal load balancing between the ONUs as well [18]. IPACT aims to avoid accumulation of switchover times caused by polling for information. With IPACT, polling

requests are overlapped in time. Like the MPCP, IPACT uses control messages to collect information about the network. The messages used are GRANT (OLT grants sending time to an ONU) and REQUEST (an ONU requests sending time from the OLT). The OLT keeps a polling table where it stores round-trip time (RTT) to each ONU (distance) and the next transmission size of each ONU. The OLT processes through its polling table and grants every ONU its accurate sending time. This process is called a cycle.

This paragraph gives an example of the IPACT algorithm by assuming an EPON with one OLT and two ONUs (ONU1, ONU2). In the first step the OLT sends a GRANT message to OLT1. The GRANT message contains exactly as much bandwidth for ONU1 as it requested with its previous REQUEST message. When ONU1 receives the message, it immediately starts bursting out data stored in its buffer until send permission expires (Figure: IPACT Step 1). While ONU1 is still sending its transmission, the OLT already starts informing ONU2 about upcoming transmission slots. Because the OLT knows about the round-trip times of its ONUs it knows exactly when the last bit of the transmission from ONU1 will arrive (Figure: IPACT Step 2). After the last transmission bit, ONU1 will additionally send its new REQUEST message containing the next request for bandwidth (Figure: IPACT Step 3). After this, IPACT waits a very short time (guard time) before it wants the next data transmission to arrive. Therefore the OLT informs ONU2 about its available bandwidth and sends the GRANT message towards ONU2 even before the last bit of ONU1 arrived. This happens two times the RTT to ONU2 before it wants the first transmission byte to arrive at the OLT. By using this overlapping mechanisms, the unused sending time between two transmission is minimised to the absolute minimum, the guard time. When the OLT reaches the end of its polling table, the process starts again with ONU1. ONU1 will receive its GRANT message again even before ONU2's last transmission bits arrived at the OLT.

The following three figures describe the steps of the IPACT polling algorithm:

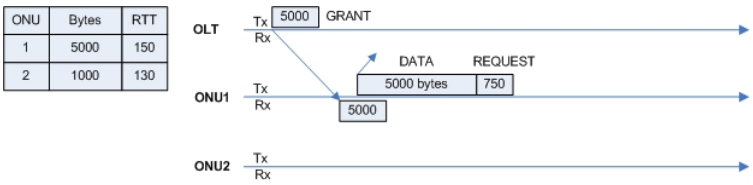


Figure 2.8: IPACT Step 1 (following [18])

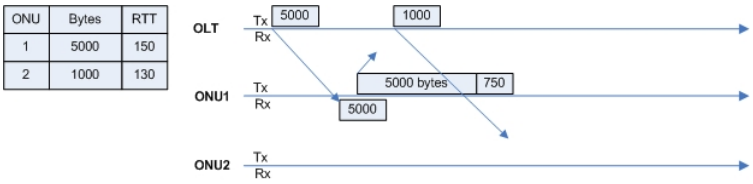


Figure 2.9: IPACT Step 2 (following [18])

With the IPACT algorithm there is no more need for clock synchronisation of the ONUs. Also the ranging process can be omitted because a new attached ONU would automatically tell the OLT about its RTT and bandwidth demand when sending its first REQUEST

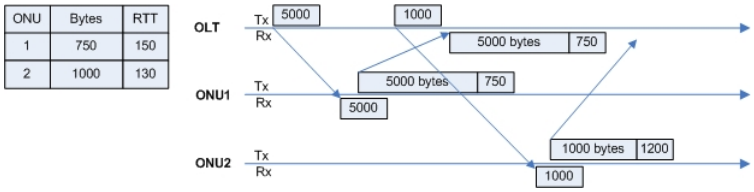


Figure 2.10: IPACT Step 3 (following [18])

message. The IPACT mechanism is managed completely centralised at the OLT which thus can deal with network changes in runtime. Each ONU that has changing values operates at a separate instance, the ONUs don't need to share their values.

2.8 Security

When talking about EPONs it has to be considered that these networks are often implemented in access networks. The access networks close the gap between the providers' backbone networks and the subscriber/customer's local network infrastructures. Access networks serve many different customers at the same time and over the same media. Customers might transmit confidential data through their network connections. Because of the broadcasting nature of the downstream channel in an EPON several security aspects have to be watched carefully. The most dangerous threat is the potential for eavesdropping in an EPON. By committing eavesdropping an attacker can later conduct theft of service (ToS) or denial of service (DoS) attacks [17].

Eavesdropping is always possible in an EPON by simply disabling all filter rules on a connected ONU. The ONU then operates in promiscuous mode and listens to all data traffic sent by the OLT. The broadcast nature of Ethernet guarantees that the ONU receives every single packet transmitted on the downstream channel. The worst issue with this method is the fact that it is nearly impossible to detect an attacker committing eavesdropping. Because EPONs are non-deterministic networks and the eavesdropping-attack is completely passive, the OLT has no way of detecting an intruder. This is only the beginning of a disaster. Eavesdropping could eventually be used for data mining. It is not always necessary to decode collected data in real-time (which is nearly impossible when having some security encryptions enabled). But nevertheless, an attacker could also be interested in just collecting data and decode this data later when off-line. By using off-line decryption the attacker might gain access to confidential data. Otherwise the collected data could be used to commit masquerading attacks. With the information collected the attacker could pretend to be another ONU and send data in its name. Not only customer data could be abused. Also system messages which are used in DBA algorithms could be manipulated. An attacker collects information till he is able to fake REQUEST messages and therefore gains the ability to steal another ONU's network resources.

The only network architecture that would theoretically offer the ability to detect eavesdropping is the ring architecture. Because the network is a closed circle it is possible to measure signal loss of both upstream and downstream channels. If an unauthorised ONU

is connected to the network the signal loss at the end of the circle is higher because of the additional attenuation caused by the intruder.

The security aspects of the upstream channel of EPONs look quite different. It is not possible to commit eavesdropping because each connected ONU is talking directly to the OLT and therefore the upstream traffic can be seen as more secure. However, even the upstream traffic is not completely secure. [17] lists a known problem of the splitter/combiner parts. These devices are used to distribute the downstream signal and to combine the incoming upstream signals towards the OLT. It is known that these parts suffer from a given signal reflection when receiving the upstream signal. This reflection is theoretically visible again on the downstream channel which could lead to the reconstruction of another ONU's upstream signal for an attacker. Another weak spot of the splitter/combiner is its logical aspect. These devices are manucatured as fully reciprocal devices [17]. This means that one port of the device is connected to the trunk towards the ONU and many ports are available for connections to the ONUs. Not all of these ports might be in active use. If an attacker gains the chance to break in to a cabling room where these devices are located (usually they are spread outside the central offices), it is possible to connect to an unused port and to pretend to belong to this network. Such unused ports therefore have to be well protected. Actual splitter/combiner devices are built in a way that ports can be disabled by software and then, if someone tries to gain physical access to the unused ports he has to destroy a security chasing. This would then destroy the whole device which gives some security guarantees against break-ins. This mechanism is called secure packaging.

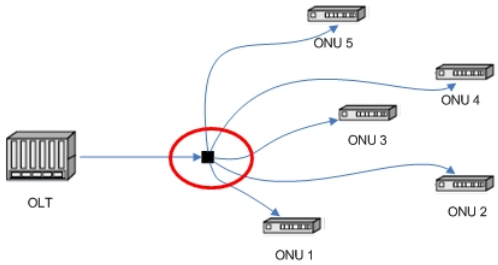


Figure 2.11: Critical Component for Reflection and Intrusion - The Splitter/Combiner

Besides the physical security leaks of an EPON there are still many more weak spots on the network side. If an attacker once gained access to a device which can be used for eavesdropping he also gets the possibility to start attacks by using the upstream channel. The attacker could use masquerading attacks to pretend the identity of another network unit and request in its name the highest available bandwidth - all the time. This would then lead to a Denial-of-Service attack where regularly registered devices suffer from a potential loss of network and service quality availability. For example, DoS could be used to overload the OLT's CPU resources or to flood the upstream channel by simply sending random data patterns. Another type of attack is the Theft-Of-Service where the attacker attempts to impersonate another legitimate customer and uses his network resources.

Because of the above security issues, many discussions about responsibility have been conducted. There is a wide range of proposed solutions such as the implementation of RADIUS server authentication as a high-level authentication or even scrambling the

whole payload of the Ethernet frames [17]. Each method has its advantages and drawbacks. RADIUS authentication would provide a high-level authentication method which is known to be very secure and finds its application in many other network types such as wireless networks for example. But RADIUS is not yet compatible with the current MPCP specifications and would therefore require very special configurations against all standard efforts. Full payload encryption sounds like a very good solution but can cause quite expensive installations. Encryption then had to be done at the physical layer which requires dedicated hardware. [17] concludes that however, hardware attacks cannot be avoided without the introduction of a dynamic wavelength management system. These systems can change the operating wavelength of a network dynamically and therefore make it nearly impossible for the intruder to find the correct laser frequency to even start an attack. But such systems are expensive and unwidely spread as of today. The National Institute of Standards and Technology (NIST) currently proposes an AES algorithm to encrypt both user-data and system-sensitive information on the physical layer [21].

2.9 Hardware Issues

EPONs are future-safe networks that offer high bandwidth at relatively low cost. But this technique is not yet very mature and requires highly sensitive parts. With the even further increasing bandwidth perfect calibration of all components is required. To understand the need for calibration and the issues the following section gives a short explanation about some hardware issues.

Near-far problem: The near-far problem results in the long distances in EPONs. Some network units can be more than 20 kilometers away from the central office while others are located closely. Network units located further away from the central office result in much weaker signals. Lasers have to be tuned to be able to deal quickly with very different signal strengths.

Data bursts: A network unit stores its incoming data from the connected computers in its internal buffer. When the sending permission arrives, it bursts out the whole buffer content in a very short amount of time, at full channel speed. To have sender and receiver able to burst, very sensitive and fast lasers are required. ONUs only receive continuous data streams broadcasted by the OLT. The OLT on the other hand needs a so-called burst mode receiver which is able to adjust its zero-one threshold at the beginning of each received time slot [1].

Frequency changes: In a Wave Division Multiplexing environment network units operate at different wavelengths. The OLT can either consist of an array of lasers which operate at different wavelengths or it uses a tunable laser. This laser then has to be able to change very quickly its frequency. This might sound easyier in theory than it is in practice. A laser requires some time to calibrate a frequency. It is therefore importent that the laser is able to stabilize very quickly after being turned on [1].

2.10 Conclusion

Despite of all hardware maturity problems, the EPON technology is spreading quickly all over the world. New proposals for high-speed PONs are in pipelines, such as a 10G-EPON call for interest [15]. EPONs are a very attractive solution for access networks which rely on the 802.3 Ethernet protocol and build up on the BPON standard. They are a cost-effective way of deploying broadband connections to the home and office users. The most commonly used technique for sharing the bandwidth on a physical channel is the Time Division Multiplexing technique, because it is cheaper and simpler to implement than other multiplexing techniques. To improve bandwidth availability and to overcome bandwidth waste caused by idle transmissions, dynamic bandwidth allocation mechanisms are implemented. It can be stated that EPONs are not yet very mature, but already offer a new way of building modern, fast, stable and cost-effective networks. With the increasing bandwidth offerings, requirements for the engineering of hardware get more and more complex. At the same time new methods are required to achieve the most efficient sharing of the available channel speed. Even in Switzerland, the first prototypes for passive optical networks started. Orange is offering a new service in cooperation with the EWZ which seems to pave the way for further EPON installations [22].

Bibliography

[1] Glen Kramer and Gery Pesavento: *Ethernet Passive Optical Network (EPON): Building a Next-Generation Optical Access Network*, IEEE Communications Magazine, February 2002.

[2] P.E. Green Jr: *Paving the Last Mile with Glass*, IEEE Spectrum, pp. 13-14, December 2007.

[3] P. Ossieur, X.Z. Qiu, J. Bauwelinck, D. Verhulst, Y. Martens, J. Vanderwege, B. Stubbe: *An Overview of Passive Optical Networks*, IEEE Communications Magazine, March 2003.

[4] J.R. Stern et. al: *Passive Optical Local Networks for Telephony Applications and Beyond*, Elec. Lett., vol. 23, pp. 1255-1257, November 1987.

[5] Yochi Maeda: *FSAN OAN-WG Status Report April 2003 - May 2004*, FSAN OAN-WG, June 2004.

[6] FSAN homepage, `http://www.fsanweb.com`, date of visit: 03.10.07.

[7] IEEE homepage, `http://ieeexplore.ieee.org/Xplore/dynhome.jsp`, date of visit: 03.10.07.

[8] ITU homepage, `http://www.itu.int/net/home/index.aspx`, date of visit: 03.10.07.

[9] EFM homepage, `http://www.ieee802.org/3/efm`, date of visit: 03.10.07.

[10] IEEE Std 802.3.ah now included in IEEE Std 802.3-2005.

[11] IEEE Std 802.3.av, `http://www.ieee802.org/3/av/index.html`, date of visit: 03.10.07.

[12] IEEE Std 802.11.n (Draft). P802.11n/D2.00, February 2007.

[13] ITU-T G.983.3 (BPON) standard, March 2001.

[14] ITU-T G.983.4 (GPON) standard, November 2001.

[15] Marek Hajduczenia, Henrique J.A. da Silva, Paulo P. Monteiro: *10G EPON Development Process*, Transparent Optical Networks, 2007. ICTON '07. 9th International Conference on. Volume 1, pp 276 - 282, 1-5 July 2007.

[16] IEEE 802.3, *Call For Interest: 10 Gbps PHY for EPON*, online report, available at: `http://www.ieee802.org/3/cfi/0306_1/cfi_0306_1.pdf`.

[17] Marek Hajduczenia, Pedro R.M. Inacio, Henrique J.A. Da Silva, Mario M. Freire, Paulo P. Monteiro: *On EPON Security Issues*, IEEE Communications Surveys and Tutorial, 1st Quarter 2007.

[18] Glen Kramer, Biswanath Mukherjee, Gerry Pesavento: *IPACT: A Dynamic Protocol for an Ethernet PON (EPON)*, IEEE Communications Magazine, February 2002.

[19] ASM Delowar Hossain, H. Erkan, R. Dorsinville, M. Ali, A. Shami, C. Assi: *A Novel Ring-Based EPON Architecture*, Broadband Networks, 2005 2nd International Conference on, Vol., Iss., 3-7 Oct. 2005, Pages: 1535-1540 Vol 2.

[20] R. Hui, B. Zhu, R. Huang, C.T. Allen, K.R. Demarest, D. Richards: *Subcarrier Multiplexing for High-Speed Optical Transmission*, Journal of Lightwave Technology, Vol. 20, No. 3, March 2002.

[21] Federal Information Processing Standard 197, Advanced Encryption Standard. National Institute of Standards and Technology, U.S. Department of Commerce 2001.

[22] NZZ Online: *Das EWZ ist mit dem Bau des Glasfasernetzes auf Kurs.* Neue Züricher Zeitung AG, October 2007.

[23] N. Ghani, A. Shami, C. Assi, M.Y.A. Raja: *Quality of Service in Ethernet Passive Optical Networks*, Advances in Wired and Wireless Communication, 2004 IEEE/Sarnoff Symposium on. Pp 161 - 165 26-27 April 2004.

[24] G. Kramer, B. Mukherjee, A. Maislos: *Ethernet passive optical networks*, IP Over WDM (Ed: S. Dixit), John Wiley, pp. 229-275, 2003.

Chapter 3

VPNs and Their P2P Alternative P2P@i

Thomas Ineichen

Every day the number of participants in the Internet increases and so does the number of services. For secure communication between two participants there exist several methods. In a first part Virtual Private Networks – a well established standard in the industry – and its requirements are analysed. The second part first explains the basics of peer-to-peer networks, as this is important to understand the functionality of P2P@i, a peer-to-peer approach for encrypted networks.

Contents

3.1 Introduction

In a more and more connected world people want to have access to their data from everywhere at anytime. Some twenty years ago employees worked at their desk, some folders behind them in a cabinet and a huge archive downstairs. Nowadays, customs and business models have changed. Many companies have branches abroad, employees work at home or on the way.

But since the Internet is an open network you have no control about where the data-packets are led through. To protect your traffic against interferences and eavesdropping you need to take certain measures. In the following, there will be presented some techniques to shield your private data.

3.2 Virtual Private Networks (VPNs)

3.2.1 Definition

> "A virtual private Network (VPN) is a computer network used to transport private data over a public network (e.g., the Internet). It enables a secure transport over an insecure network. Participants are able to exchange data as if they were in a internal LAN. The individual user does not have to be connected directly." [1]

There are many other VPN-technologies which use other networks than the Internet. But todays VPNs mostly use the Internet, because of its highavailability.

It is available (nearly):

anywhere In 2004, over 60 % of Swiss households had access to the Internet [2]. There are more and more Wireless-LAN-Hotspots (e.g., in public places, trains) and with new technologies like UMTS or HSDAP you will have access wherever there is mobile phone coverage.

at anytime Due to the structure of the Internet it is very unlikely that it will break down. Nevertheless it is still possible that there is a failure in the connection on either side of the VPN.

on any device more and more devices (e.g., computers, notebooks, handhelds, mobile phones) are able to connect

3.2.2 VPN architectures

VPN architectures can be divided in three categories:

- End-to-End
- Site-to-Site
- End-to-Site

A VPN-environment however is not limited to one architecture. Especially Site-to-Site and End-to-Site architectures are often used in the same VPN.

3.2.2.1 End-to-End

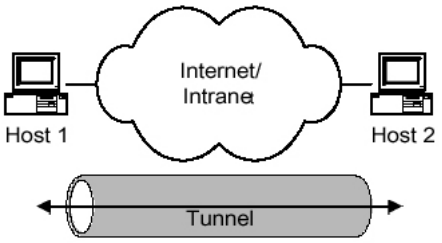


Figure 3.1: End-to-End [10]

The most secure connection is an end-to-end tunnelling of the data packages. As the name says, the packages are encrypted from end to end. That means, that all the de- and encryption is done by the hosts and no one else is able to read the information exchanged. But it is also the most extensive, because in a network every host needs a direct connection to the other hosts and therefore has to manage multiple VPN-connections at a time.

3.2.2.2 Site-to-Site

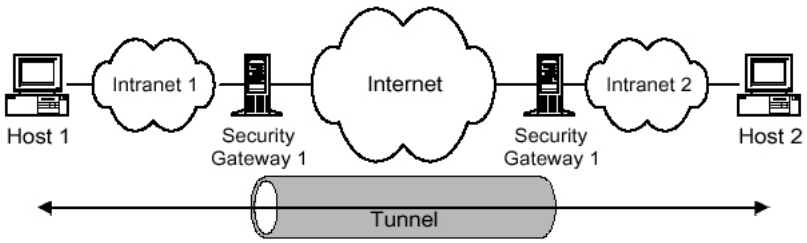


Figure 3.2: Site-to-Site [10]

In a Site-to-Site-VPN the de- and encryption is managed by a VPN-gateway. They connect two or more intranets with a secure tunnel over the Internet. A Site-to-Site-VPN is much easier to administrate because the VPN-software does not run on the individual hosts but only on the gateway. But it is also less secure, because any (physical) intruder could place a device inside one of the intranets and get access to the net.

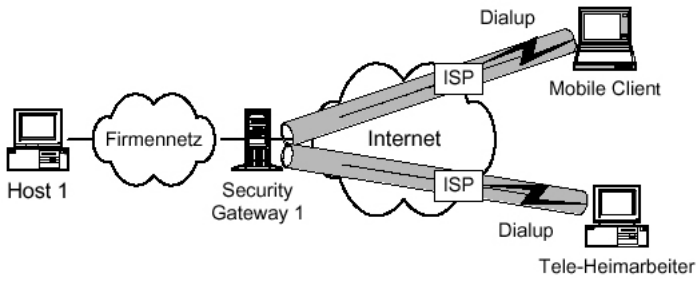


Figure 3.3: End-to-Site [10]

3.2.2.3 End-to-Site

An End-to-Site-VPN is often used for home offices, remote access and similar application. A remote station connects to the intranet trough a VPN gateway. This configuration is typical if there is only one device per place that needs access to the companies network. In many cases an Internet connection is cheaper than a direct connection (e.g., per ISDN) to the enterprises servers.

3.2.3 Why use a VPN?

"Businesses today are faced with supporting a broader variety of communications among a wider range of sites even as they seek to reduce the cost of their communications infrastructure. Employees are looking to access the resources of their corporate intranets as they take to the road, telecommute, or dial in from customer sites. Plus business partners are joining together in extranets to share business information, either for a joint project of a few months' duration or for long-term strategic advantage.

At the same time, businesses are finding that past solutions to wide-area networking between the main corporate network and branch offices, such as dedicated leased lines or frame-relay circuits, do not provide the flexibility required for quickly creating new partner links or supporting project teams in the field. Meanwhile, the growth of the number of telecommuters and an increasingly mobile sales force is eating up resources as more money is spent on modem banks, remote-access servers, and phone charges. The trend toward mobile connectivity shows no sign of abating; Forrester Research estimated that more than 80 percent of the corporate workforce would have at least one mobile computing device by 1999." [4]

The "virtual" in VPN means, that the network is not static. Connections are set up according to the need of the company. Still, the network is formed logically, no matter, what the structure of the underlying network is. Unlike the leased lines used in traditional corporate networks, VPNs do not maintain permanent links between the end points that make up the corporate network. Instead, when a connection between two sites is needed, it is created; when the connection is no longer needed, it is torn down, making the bandwidth and other network resources available for other uses. Thus the connections making up a VPN do not have the same physical characteristics as the hard-wired connections used on the LAN, for instance.

3.2.4 Requirements for a VPN

There is a broad range for the use of a virtual private network. Following "VPN - Virtuelle Private Netzwerke" [3] there are several main aspects, which differ from case to case and have to be evaluated separately forevery case.

3.2.4.1 Security

Security is normally divided into:

Data confidentiality "Ensuring that information is accessible only to those authorized to have access." [5]

Often companies not only want to encrypt the content of a data package, but also information about the internal structure of their network (e.g., source and target address, port number). Therefore, the complete package has to be encapsulated in a new package. This procedure is called "tunnelling".

Key management To enable a secure and automatic distribution of symmetric keys, a reliable key management is needed. Its task is to generate the required keys and distribute them to the right opponents in the VPN.

Packet authentication It has to be guaranteed that the arriving packets derive from the authentic sender and that not a third person with faked sender address.

Similar to a user authentication, every incoming packet has to be authenticated. This is normally realised by either symmetric keys or Pre-Shared Secrets (confidential data that just the sender and the receiver know).

Data integrity "Condition existing when data is unchanged from ists source and has not been accidentally or maliciously modified, altered, or destroyed." [6]

Normal checksum methods do not suffice, as a intruder could recalculate the checksum of a package after the change. So the checksum has to be inserted into the encrypted package.

User authentication This is very important in Remote-Access-VPN. A user that wants to have access to the intranet has to authenticate himself reliably. This can be done by [7]:

- Something the user has
  Example: ID card, security token, software token, phone, or cell phone
- Something the user knows
  Example: a password, pass phrase, or personal identification number (PIN)
- Something the user is or does
  Example: fingerprint or retinal pattern, DNA sequence, signature or voice recognition, unique bio-electric signals, or another biometric identifier

Obstruction protection A VPN-Gateway has to be secured against attacks aiming to reduce or interrupt its functionality.

The most known problem are DDoS-Attacks (Distributed Denial of Service). Because the sender of a "normal"' DoS-Attack is relatively easy to trace, a DDoS works in two steps:

1. Build a net of bots (normally computer whose user do not know that they are infected).
2. Start the attack from all the bots at the same time.

It is much harder to find the origin of such an attack.

Penetration protection A VPN-Gateway must prohibit unauthorised access to the companies intranet trough its public interface. This would be the direct way to the information an invader wants to copy or manipulate. Most hackers are not satisfied with the data that is transported trough the public network but want to have access to the intranet, where all the corporate secrets are stored and processed.

Often a VPN-Gateway is the only interface between the intranet and the Internet. Because of the millions of possible intruders, a VPN-gateway needs special access protection. Normally one divides the different methods in three areas:

- Physical security

  The systems have to run in a secure environment. The security of the service space is crucial, they must not be operated in an office or a server room with all the other technical equipment. A good system is also protected against unauthorised changing or even opening and sends automatically an alert message to the network management system.

- Interface security

  Interfaces connected to the Internet should have mechanism to protect the interface against the different attacks from the Internet. Mostly such interfaces have a reduced IP stack which lowers the contact points and therefore enhances the immunity.

- Operational security

  One should not forget about attacks from the inside of a system. According to several studies, most of the attacks against a VPN gateway have its seeds in the intranet. So it is for example very important, that the communication between the gateway and the administrator is secured (e.g., via SSL, SSH or IPSec).

3.2.4.2 Availability

A virtual private network should support or eliminate traditional forwarding or remote access solutions. Therefore it has to be as available as conventional WAN-infrastructures. Old techniques as point-to-point connexions or ISDN-lines have a very high availability of over 99.999%. In other words: A digital line between the intranet of a company and

the telephone extension of a clerks home office is down for a maximum of ca. 5 minutes of a year!

Normally one does not invest in a technology that is less reliable than the antecessor. But if a solution is considerably lower priced, one should probably rethink the needed availability. Usually a point-to-point connection was not implemented because of its good availability, but because there were no other solutions at that point in the past.

Questions to ask are:

- How often is the VPN used? (24 hours a day (worldwide infrastructure) or only during local business hours?)
- How important is the VPN connection? (Is it possible to work on other things during a break down or is it my lifeline and the company is dependent on it?)

3.2.4.3 Quality of Service

Quality of Service (QoS) becomes more and more important in todays business communication. The trend is to use convergent nets, which means, that speech, data, videos and other streaming contents are sent trough the same medium. In the past, speech and video were exchanged in point-to-point connections (e.g., telephone line) with reliable quality. On the Internet, without static routing of packets, data packages do not necessarily arrive in the same order as they were sent.

There are several characteristics to measure the QoS in a VPN [11]:

- Dropped packets

  It is not possible to determine what will happen to packages that arrive to a router when its buffer is already full. It is very likely that they will be dropped an retransmitted by the sender. This ofthen causes severe delays in the overall transmission.

- Delay

  For real-time applications the time difference between sending and receiving a data package should not be to long. For example in telephony the difference between the speaker saying something and the listener hearing it should not be more than 250 ms. Otherwise the pauses are to long and the conversation stumbles.

- Jitter

  Packets from source will reach the destination with different delays. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably. This variation in delay is known as jitter and can seriously affect the quality of streaming audio and/or video.

- Out-of-order delivery

  When a collection of related packets is routed through the Internet, different packets may take different routes, each resulting in a different delay. The result is that the packets arrive in a different order than they were sent. This problem necessitates special additional protocols responsible for rearranging out-of-order packets to an isochronous state once they reach their destination. This is especially important for video and VoIP streams where quality is dramatically affected by both latency or lack of isochronicity.

- Error

  Sometimes packets are misdirected, or combined together, or corrupted, while en route. The receiver has to detect this and, just as if the packet was dropped, ask the sender to repeat itself.

3.2.4.4 Scalability

Even tough (or: because!) the future of a network is hard to predict, it should be designed openly. Both observing standards and using modular components is important for a later expansion of a network. While a gateway in a branch office does not need to handle as many connections as the gateway at the companies headquarters, both need to support the same level of security! For a central component it is also important to respect the increasing number of mobile devices such as laptops and handhelds, which presumably suggests an increasing use of VPN connections.

3.2.4.5 Integrability

Only seldom a network is build from scratch. This means that a VPN often has to be integrated in an existing environment with local and wide area networks, remote services and corresponding systems.

3.2.4.6 Addressmanagement

The bigger a network is, the more important is an efficient addressmanagement. Each joining participant has to be given an unique IP address. This is mostly done by DHCP (Dynamic Host Configuration Protocol).

3.2.4.7 Interoperability

Interoperability is a crucial specification for a VPN gateway (and all information technology). In todays business world mergings and reorganisations of divisions are the order of the day. So no computer system will be static for its lifetime but will be changed from time to time. If a device does not observe a standard, it probably will not be possible to connect it to new hardware and it has to be exchanged.

3.3 Use Case: VPN@UZH

The UZH provides access to its intranet trough a VPN. It is often used to allow access to restricted areas, such as teaching materials.

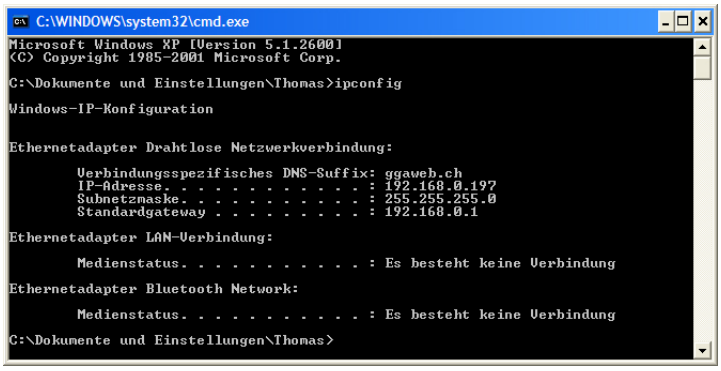


Figure 3.4: ipconfig before

Before connecting to the VPN an overview of the example computer: It is connected trough a wireless connection to a router. Its own (private) IP address is 192.168.0.197, whereas the IP of the router is 192.168.0.1.

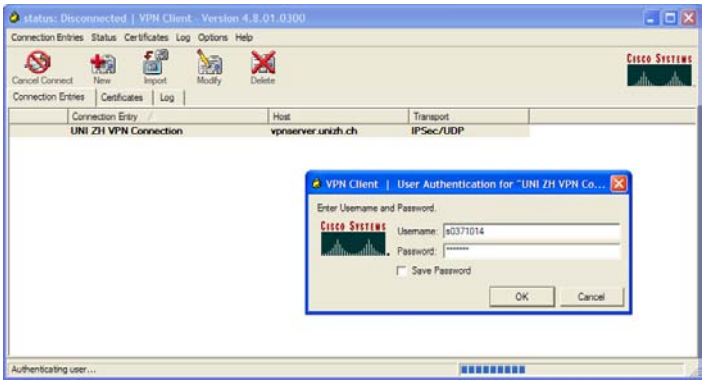


Figure 3.5: Cisco VPN Client

The VPN software is preconfigured and only needs an username and a password.

After successfully connecting to the VPN, the machine gets a new IP address from the internal network of UZH. All the Internet traffic will now be routed trough the UZH-Router and the private router at home is not reachable anymore.

Such a central authentication is a simplification for many operations inside and outside the university. It allows lecturers to publish their data to all students without having to care about distributing passwords to access the files. On the other hand it is also possible for the university to grant students access to international databases. Furthermore the students do not have to hand on their private data to other institutions.

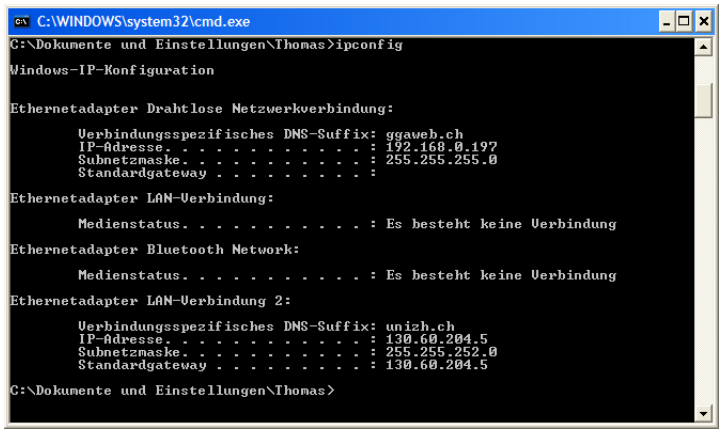


Figure 3.6: ipconfig after

3.4 Peer-to-Peer Networks

"A peer-to-peer (or "P2P") computer network exploits diverse connectivity between participants in a network and the cumulative bandwidth of network participants rather than conventional centralized resources where a relatively low number of servers provide the core value to a service or application. Peer-to-peer networks are typically used for connecting nodes via largely ad hoc connections. Such networks are useful for many purposes." [16]

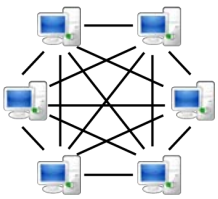


Figure 3.7: Peer-to-Peer network [16]

3.4.1 Background

Most known applications for P2P-Networks are file sharing programs like Gnutella and KaZaA. But there are other fields of application for a P2P-implementation, where users often do not know, what technique is used.

Some examples:

- Voice over IP (e.g., Skype, SIP)
- media streaming (e.g., Zattoo, Joost)
- discussion forums (e.g., Usenet)

3.4.2 Centralisation

A P2P-Network can not only be distinguished by its purpose, but also by its centralisation. In a purely decentralised network, every peer is equal to the others. That means it acts at the same time as a server and a client. Thus there is no need for a superior entity to keep track of the traffic in between the peers. Best known example of a decentralised network is Gnutella, the third-most-popular among file sharing networks [8].

But there is also wide range of hybrid systems. Many of them use one or more central servers that do not store downloadable files but the information on which peers the data is stored.

Such a centralised network is much more vulnerable against attacks from outside. For example Napster could only be shut down by its owner in 2001 because of its structure. Gnutella on the other hand has no such possibility. In the worst case, a node could just look up every IP address for a responding peer.

3.4.3 Overlay network

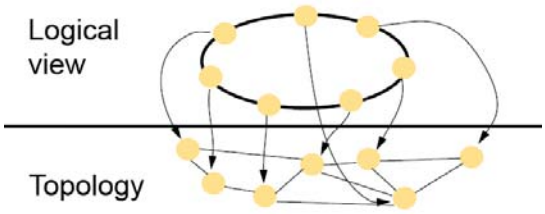


Figure 3.8: Logical View - Topology [12]

An overlay network is a logical view for a set of nodes which are connected physically to each other (compare figure 3.8). If two nodes know each other there is a link between them. There are unstructured and structured P2P-networks, depending on how the peers are linked in the overlay network [16].

3.4.3.1 Unstructured networks

In an unstructured network, the overlay links between the peers are built at random. Any joining peer just copies the existing links of a node he knows and connects to them by itself. A main disadvantage of unstructured networks is their poor support for search functions. If a peer is looking for a piece of data, it sends a query to each node it knows. If those nodes do not know the file,they just spread the query by asking their neighbours and so on. In the case ofa well spread file, the chances are high that a nearby node has the dataavailable. But if the file is rare, there is no guarantee that it will be foundby such a search operation, since there is no correlation between a peer andits administrated content. Such search operations produce a lot of signallingtraffic and thus unstructured networks normally are inefficient. Examples forunstructured networks are Gnutella and FastTrack [16].

3.4.3.2 Structured Networks

To assure an efficient search for files (even for rare ones), a structured network needs a globally consistent protocol. The most used instrument is the distributed hash table (DHT). A DHT uses a special way of consistent hashing for allocating files to a specified peer, similarly to traditional hash tables. Common DHTs are Chord, Pastry and CAN.

DHTs characteristically emphasize the following properties [9]:

Decentralisation As mentioned above, the nodes organize themselves without the need for acentral server to coordinate.

Scalability More participants in a network should not weaken its efficiency, e.g., a search for a file among 10.000 nodes should not take 100 times longer than among 100 files.

Fault tolerance As most of the P2P-networks do not have a constant number of participants, the DHT should be able to endure continuously joining, leaving and failing nodes.

Load balancing If a file is well spread and often demanded, a DHT-implementation shoulddistribute the traffic between the nodes, so that every possessing node isequally used for distribution of the file.

Robustness A P2P-network should be stable against an intruder who tries to disturb the network by sending false data. There are rumours that the music industry has servers that send out faked mp3-files to put off users.

A key technique used to achieve these goals is that any one node needs to coordinate with only a few other nodes in the system - most commonly, O(log n) of the n participants (see below) - so that only a limited amount of work needsto be done for each change in membership.

Some DHT designs seek to be secure against malicious participants and to allow participants to remain anonymous, though this is less common than in many other peer-to-peer (especially file sharing) systems; see anonymous P2P.

Finally, DHTs must deal with more traditional distributed systems issues such as load balance, data integrity, and performance (in particular, ensuring that operations such as routing and data storage or retrieval complete quickly) [9].

3.4.3.3 An overlay network: Chord

> "The Chord project aims to build scalable, robust distributed systems using peer-to-peer ideas. The basis for much of our work is the Chord distributed hash lookup primitive. Chord is completely decentralized and symmetric, and can find data using only log(N) messages, where N is the number of nodes in the system. Chord's lookup mechanism is provably robust in the face of frequent node failures and re-joins." [17]

In a Chord-network, the nodes are placed on a virtual ring. Each node gets an ID, which is a hash value of its IP address. With this scenario, two different nodes will never have the same ID. The nodes are then placed on the ring clockwise in ascending order. Each key (or information) is then also hashed and given an ID. The keys are managed by the node with the ID succeeding the keys ID. Figure 3.9 shows an example of a Chord-ring with 10 nodes and 5 keys.

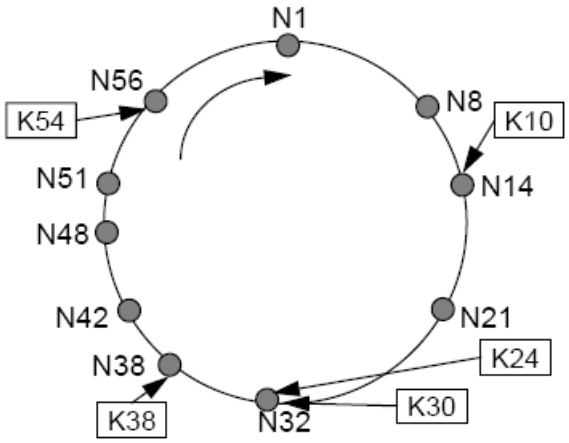


Figure 3.9: 10 nodes, 5 keys [12]

Because every node knows its direct successor, a query for a key is forwarded up to the first node with a higher ID then the key. This then is the node which manages the key.

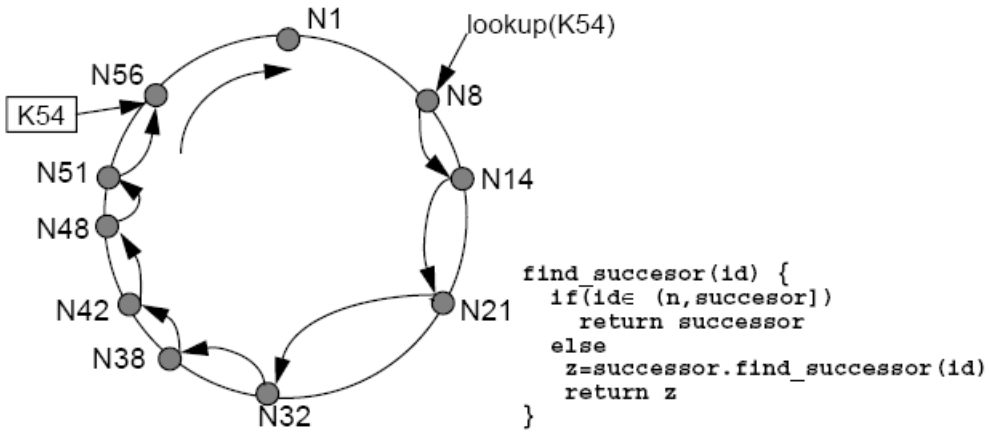
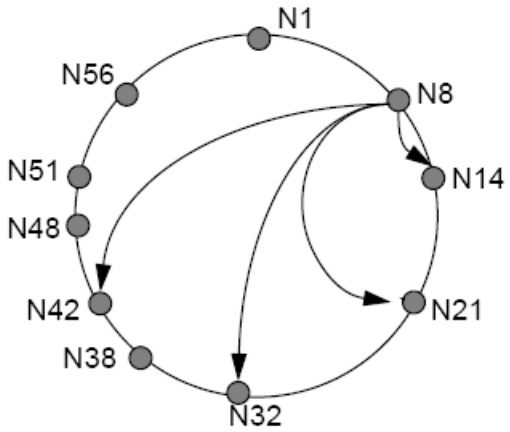


Figure 3.10: Lookup key-ID 54 [12]

To make the retrieval of a key scalable for every size of ring, every node is given additional information: Every node entertains a finger table where the IDs of responsible nodes for a set of following keys is saved. In figure 3.11 there is a finger table for node 8 with six entries. The IDs normally are calculated by adding 2^k to the node-ID (whereas k ranges from 1 to the number of nodes).



ID	Verantworlicher Knoten
8+1	14
8+2	14
8+4	14
8+8	21
8+16	32
8+32	42

Figure 3.11: Finger-table [13]

3.4.3.4 Symphony

A similar approach to establish a logical view is Symphony. Unlike Chord, a node in a Symphony-network can choose its ID at random in the range [0,1). So the circumference of the imaginary ring is 1. As in Chord, each node maintains the keys with an ID between the node itself and its predecessor. To scale the routing, each node maintains a table with long distance links to several IDs the node again chooses randomly.

3.5 P2P@i

P2P@i by the Japanese Yuuki Takano is a project to provide a network virtualization software to construct decentralized and structured virtual IP networks. It was started in Jannuary 2007 [15].

The program is available for Windows, MacOS X, NetBSD and Linux. As it is published under a BSD License, everyone is free to use, change and redistribute the source code of the program.

As P2P@i is based on Symphony as underlying network, it does not need to have acentral authorisation like VPNs. To connect to a virtual network you just need to know the IP address of one of the participating nodes.

3.5.1 Sample installation

After installing the program on your computer, a process is listening on port 9200 of your network connection. Open the web user interface at `http://localhost:9200/` to change the default settings. In the Section “P2P Network” you can define to which host and port

you want to connect. You can either choose from the default list on the right side, or just type the IP of any other machine where P2P@i is running (compare figure 3.12).

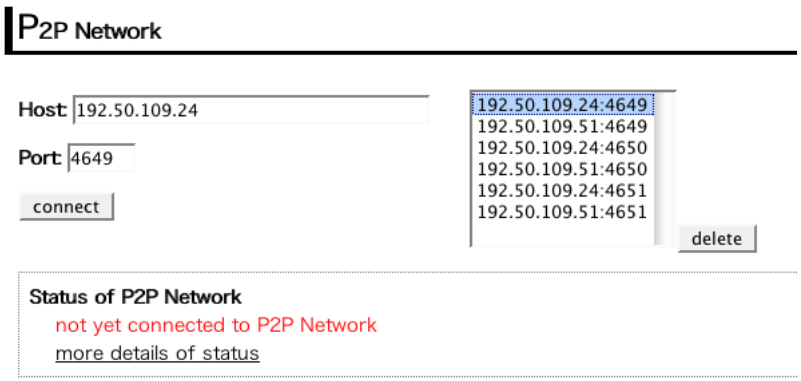


Figure 3.12: Connect to a network [18]

In a next step (figure 3.13), you can choose your "channel" in the P2P@i-environment. So it is possible to have different logical networks on one physical machine. Again there is a variety of choice on the right side. Click then "connect" to join the encrypted channel.

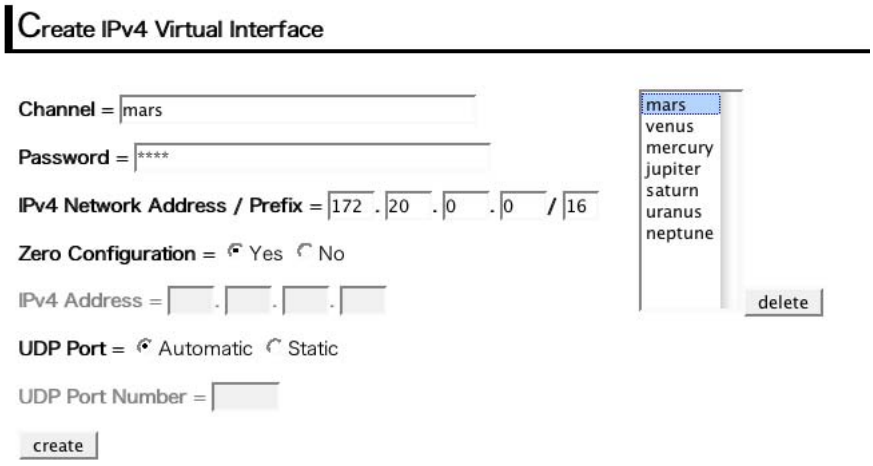


Figure 3.13: Virtual Interface [18]

Shortly after that your computer is connected and the P2P@i is ready to use. For example in Windows, there is now a new virtual network interface with the chosen IP. Any network application has now access to the P2P@i-network an can exchange their data encrypted.

3.6 Comparison and Outlook

P2P@i is a perfectly neat program for small user groups with no obligation for buying expensive hardware or installing complicated software. With its peer-to-peer technology it is much more flexible than a virtual private network. Unfortunately, it is not well known,

even among computer specialists. Also it seems, that there is no further development at the moment, as the last change dates back to June 2007 - half a year after it was started.

A short poll during class also showed, that many of the students do not use encryption. They neither utilize PGP for e-mails nor TrueCrypt (or similar programs) to secure their harddisk. So it is not surprising that they also see no need for P2P@i at their home. With this lack of interest it is difficult for small projects to get established. Only the ongoing discussion about privacy (especially in Germany) can probably change something about the way users think.

Bibliography

[1] Wikipedia: *Virtual Private Network*, http://de.wikipedia.org/wiki/Virtual_Private_Network, last visited October 2, 2007.

[2] Bundesamt für Statistik: *Internetnutzung in den Haushalten der Schweiz*, http://www.bfs.admin.ch/bfs/portal/de/index/news/publikationen.Document.87094.pdf.

[3] Lipp, Manfred: *VPN Virtuelle Private Netzwerke, Aufbau und Sicherheit*, Addison-Wesley, 2006.

[4] The International Engineering Consortium: *Virtual Private Networks (VPNs)*, http://www.iec.org/online/tutorials/acrobat/vpn.pdf, last visited October 2, 2007.

[5] International Standardisation Organisation: *ISO 17799*.

[6] Committee on National Security Systems: *National information assurance glossary*, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.

[7] Wikipedia: *Authentication*, http://en.wikipedia.org/wiki/Authentification, last visited October 2, 2007.

[8] Wikipedia: *Gnutella*, http://en.wikipedia.org/wiki/Gnutella, last visited December 1, 2007.

[9] Wikipedia: *Distributed Hash Table*, http://en.wikipedia.org/wiki/Distributed_hash_table, last visited December 1, 2007.

[10] Gärtner, Oliver und Uenal, Berkant: *Virtual Private Network, Mit sicherem Tunnel durchs Internet*, Diplomarbeit 1999, http://ipsec.gosecurity.ch/unterlagen/DA99_gaertner_uenal.pdf.

[11] Wikipedia: *Quality of Service*, http://en.wikipedia.org/wiki/Quality_of_Service, last visited October 4, 2007.

[12] Reiser, Hans P.: *Verteilte Algorithmen*, Vorlesungsscript 2003, http://www4.informatik.uni-erlangen.de/Lehre/WS03/V_VA/Skript/VA-6b.pdf.

[13] Otto, Karsten: *Verteilte Systeme*, Vorlesungsscript 2007, http://www.inf.fu-berlin.de/lehre/SS07/VS/folien/vs5.5.pdf.

[14] Manku, G. S., Bawa, M., and Raghavan, P.: *Symphony: Distributed Hashing in a Small World*, `http://www-db.stanford.edu/~manku/papers/03usits-symphony.pdf`.

[15] Y. Takano: *P2P@i Project*; `http://p2pati.sourceforge.net/`.

[16] Wikipedia: *Peer to peer*, `http://en.wikipedia.org/wiki/Peer_to_peer`, last visited October 4, 2007.

[17] MIT: *Chord*, `http://pdos.csail.mit.edu/chord/`, last visited December 1, 2007.

[18] P2P@i wiki: *Simplest Example*, `http://p2pati.wikidot.com/simplest-example`, last visited December 1, 2007.

Kapitel 4

Web Services – Technology and Security

Adrian Kobler

Web Services sind zur Zeit viel diskutiert in der Informatik und beinahe jeder hat den Begriff bereits an verschiedenen Stellen gelesen oder gehört. Die vorliegende Arbeit gibt in einem ersten Teil einen allgemeinen Überblick über dieses Themengebiet. Dabei werden auch die ihr zu Grunde liegenden Standards erklärt. In einem zweiten Teil wird auf aktuelle Sicherheitsprobleme eingegangen und es werden mögliche Lösungsansätze diskutiert. Der Fokus in diesem Teil liegt auf den Konzepten des Zonenmodells, der Policies, XML Signaturen, Sicherheitstokens und dem Trust-Serv Modell. Abschliessend werden auch mobile Web Services analysiert und an Hand dieses Beispiels das mehrschichtige Sicherheitsmodell aufgezeigt.

Inhaltsverzeichnis

4.1 Einleitung und Überblick

Die vorliegende Arbeit beschäftigt sich mit Web Services und den damit verbundenen Sicherheitsaspekten. In diesem Abschnitt wird zunächst die Relevanz des Themas erläutert. Anschliessend wird in die Thematik eingeführt und schliesslich ein Überblick über den Gesamtaufbau der Arbeit gegeben.

4.1.1 Motivation

Der Begriff „Web Services“ ist zur Zeit in aller Munde. Sei es im Zusammenhang mit dem Modewort „Web 2.0“ oder gar mit „Service oriented architecture (SOA)“, einer neuen Möglichkeit, Informatik in Unternhemen einzusetzen. Dabei wird aber oft übersehen, dass diese Technologie neben vielen Chancen auch einige ernstzunehmende Gefahren in sich birgt. Deswegen ist es wichtig, zum einen die zu Grunde liegenden Standards zu kennen, zum anderen aber auch über die Sicherheitsprobleme informiert zu sein. Diese beiden Punkte abzudecken ist das Ziel dieser Arbeit.

4.1.2 Einleitung in die Problematik

Die Idee hinter Web Services ist prinzipiell nicht neu, denn bereits CORBA verwendet ähnliche Prinzipien. Neu ist in erster Linie die Einfachheit der Kommunikation, deren Grundlage das Versenden von standardisierten Nachrichten bildet. Zudem wurden früh neue Möglichkeiten entdeckt, wie Services miteinander interagieren können. Allerdings bergen Web Services auch einige Risiken in Bezug auf Sicherheitsaspekte, die noch nicht vollständig geklärt sind. Dies erklärt auch die zur Zeit eher geringe Verbreitung.

4.1.3 Überblick

Das Ziel dieser Arbeit ist daher zweigeteilt: In einem ersten Abschnitt soll ein kurzer Überblick über Web Services an sich gegeben werden. Insbesondere werden auch die wichtigsten damit verbundenen Technologien vorgestellt. In einem zweiten Teil wird dann auf bekannte Sicherheitsprobleme hingewiesen und es werden auch diverse Ansätze zu deren Lösung vorgestellt. Abschliessend folgt eine Analyse der vorgestellten Probleme und Lösungen sowie ein Ausblick.

4.2 Überblick über Web Services

Wie bei neuen Internet Technologien üblich, hat sich auch im Fall von Web Services das „World Wide Web Consortium“ oder kurz „W3C“ darum gekümmert, eine verbindliche Definition des Begriffes „Web Services“ auszuarbeiten. Bereits früher wurde der Begriff

„XML“ eingeführt, der aber auch für Web Services eine zentrale Bedeutung hat. Zudem war es auch nötig, weitere Begriffe zu standardisieren, die für diese neue Technologie zentral sind. So zum Beispiel „SOAP“, „WSDL“ und „UDDI“. Um eine Grundlage für die nachfolgenden Sicherheitsaspekte zu bilden, werden alle diese Begriffe auf Basis der Definitionen des W3C nachfolgend genauer erläutert.

4.2.1 Definition Web Services

Die für die Standardisierung von neuen Web Technologien zuständige Organisation ist das „World Wide Web Consortium“ oder kurz „W3C“. Dieses Gremium hat in [1] folgende Punkte als zentral für Web Services definiert:

- Es muss sich um ein Software System handeln.
- Dieses muss über eine URI identifiziert sein.
- Die Grundlage der öffentlichen Schnittstellen bildet XML.
- Andere Systeme können über Internet Protokolle mit diesem System interagieren.

Ein klassisches Beispiel für einen Web Service ist das Angebot von Google. Nebst dem Zugriff über die herkömmliche Weboberfläche lassen sich Suchanfragen auch direkt via XML an einen Web Service adressieren, der über eine URL erreichbar ist. Entsprechend sind alle oben genannten Bedingungen an einen Web Service erfüllt.

4.2.2 Definition XML

Da Web Services auf XML aufbauen, ist auch deren Definition grundlegend für das Verständnis. Gemäss der Defition des W3C in [2] bietet XML die Möglichkeit, dass Dienstanbieter und Dienstkonsument mittels strukturierten Dokumenten miteinander kommunizieren können. Dies eignet sich sehr gut auch für Web Services, da die Kommunikation im Idealfall ad hoc statt findet und somit das Format des Nachrichtenaustausches standardisiert sein muss. Entsprechend hat sich XML als Standardform in der Kommunikation im Bereich Web Services durchgesetzt.

Der Aufbau von XML Dokumenten ist streng hierarchisch gestaltet. Als Strukturelemente werden so genannte „Tags“ verwendet, die die eigentlichen Parameter einschliessen. Entsprechend treten diese Tags immer paarweise auf, dürfen sich aber gegenseitig nicht überschneiden. Sehr wohl ist aber eine Verschachtelung möglich, was am Beispiel von Abbildung 4.1 ersichtlich ist.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE CONTACTLIST SYSTEM "contacts.dtd">
<CONTACTLIST>
   <CONTACT>
      <NAME>Michael Naef</NAME>
      <ADDRESS>Rosenstrasse 28, 8001 Zuerich</ADDRESS>
      <PHONE type="mobile">079 123 4567</PHONE>
      <PHONE type="private">01 123 4567</PHONE>
      <MAIL>naef@acm.org</MAIL>
   </CONTACT>
   <CONTACT>
      <NAME>Werner Hartmann</NAME>
      <PHONE type="office">01 987 6543</PHONE>
      <PHONE type="fax">01 222 2222</PHONE>
      <MAIL>hartmann@inf.ethz.ch</MAIL>
   </CONTACT>
</CONTACTLIST>
```

Abbildung 4.1: XML Beispiel

4.2.3 Definition SOAP

Um die Kommunikation zwischen Web Services zu ermöglichen, ist eine gemeinsame Spezifikation über die wichtigsten Parameter unerlässlich. Aus diesem Grund hat das W3C das „SOAP“ Protokoll entwickelt. Das Akronym steht für „Simple Object Access Protocol“. Gemäss der Definition des W3C in [3] eignet sich SOAP ideal als Standard zur Kommunikation zwischen Web Services. Auf der Grundlage von XML basiert die Kommunikation der Beteiligten somit auf den Austausch von standardisierten XML-Nachrichten. Da Web Services zudem definitionsgemäss auf Internetprotokollen basieren, kann als Grundlage der Kommunikation die bestehende und bereits vorhandene Technologie weiter genutzt werden.

Detaillierter betrachtet verwendet SOAP im Kern immer das gleiche Muster. Grundlage ist ein sogenannter „Envelope“ Teil als Hülle, der alle anderen Elemente enthält. Diese sind entweder im optionalen Header oder im zwingend benötigten Body enthalten, der auch die Nutzdaten beinhaltet. Eventuell ist im Body auch ein <FAULT> Element vorhanden, das über mögliche Fehler und die Reaktion darauf informiert. Bildlich ist dies in der Abbildung 4.2 gezeigt.

Abbildung 4.2: SOAP Grundmuster

Ein konkretes Beispiel eines Aufrufes und der dazugehörigen Antwort ist in Abbildung 4.3 dargestellt. In beiden Fällen sind sowohl die XML-, als auch die SOAP-Struktur des Envelopes und des eingebetteten Bodys ersichtlich. Der Header wurde in diesem einfachen Beispiel weg gelassen.

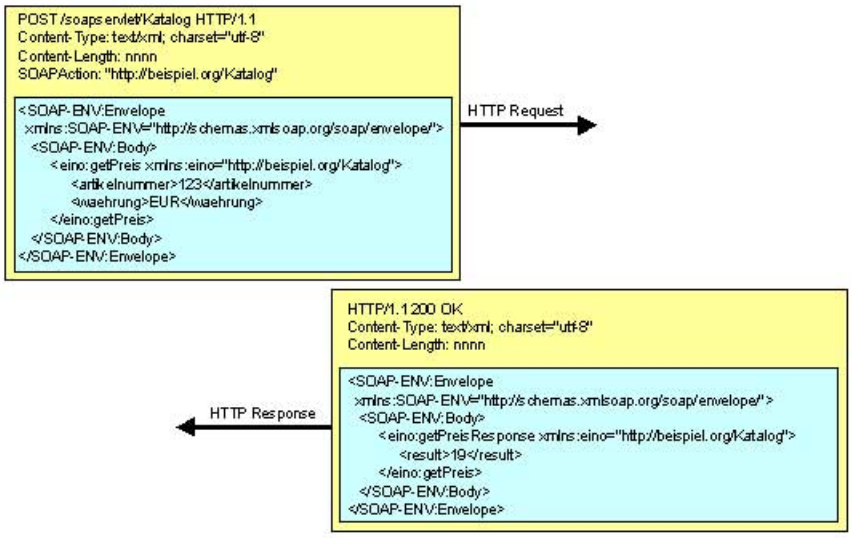


Abbildung 4.3: SOAP Beispiel

4.2.4 Definition WSDL

Gemäss der Defintion des W3C in [4] bildet die Web Service Description Language (kurz WSDL) die Grundlage für die Beschreibung eines Web Services. Die Idee ist es, dass ein zukünftiger Benutzer eines Web Services alle nötigen Informationen in dieser Beschreibung findet. Diese können zum Beispiel Angaben über den Zugriff oder über die Rückgabewerte enthalten. So sollte es im Prinzip möglich sein, Dienste von neuen, unbekannten Anbietern sofort nutzen zu können ohne dass eine menschliche Interaktion nötig ist. Ein Anwendungsbeispiel wird später im Rahmen eines Gesamtüberblicks über Web Services aufgezeigt. In Abbildung 4.4 ist ein Beispiel einer WSDL Beschreibung zu sehen.

4.2.5 Definition UDDI

Das „Universal Description, Discovery, and Integration protocol“ wird durch das W3C in [5] definiert als ein Protokoll, mit welchem es möglich wird, ein Verzeichnis über verschiedene Dienste und Diensteanbieter aufzubauen. Dies entspricht der Idee, dass Anbieter von Diensten erst bei einem konkreten Bedarf bekannt sein müssen und entsprechend zu diesem Zeitpunkt ad hoc gesucht werden können.

Als konkretes Beispiel ist denkbar, dass innerhalb eines Programmes ein Währungsumrechner gesucht wird. Da dem Programm die URL des UDDI Verzeichnisses bekannt ist, kann es sich selbständig mit diesem Dienst verbinden und dort nach einem passenden Web

```
- <definitions targetNamespace="http://tempuri.org/">
  - <types>
    - <s:schema elementFormDefault="qualified" targetNamespace="http://tempuri.org/">
      - <s:element name="Datum">
          <s:complexType/>
        </s:element>
      - <s:element name="DatumResponse">
        - <s:complexType>
          - <s:sequence>
              <s:element minOccurs="0" maxOccurs="1" name="DatumResult"
              type="s:string"/>
            </s:sequence>
          </s:complexType>
        </s:element>
        <s:element name="string" nillable="true" type="s:string"/>
      </s:schema>
    </types>
```

Abbildung 4.4: WSDL Beispiel

Service suchen. Als Ergebnis dieser Suche liefert der Dienst des Verzeichnisses eine WSDL Beschreibung zurück, mit Hilfe derer sich das ursprüngliche Programm automatisch mit dem eigentlichen Web Service verbinden kann. So kan ein externer Dienst in Anspruch genommen werden, ohne dass seine genaue Adresse oder Spezifikation im Voraus bekannt sein müssen.

4.2.6 Zusammenhang der Technologien

In Kombination mit WSDL lässt sich an Hand von UDDI die Grundidee hinter dem Zusammenspiel verschiedener Web Services aufzeigen. Im Prinzip geht es darum, dass ein Servicekonsument zu einem gewissen Zeitpunkt einen Bedarf nach einem bestimmten Dienst feststellt. Um einen passenden Anbieter zu finden, kontaktiert er deshalb einen Servicebroker, der in einem Verzeichnis eine Vielzahl von Anbietern indexiert hat. Zu jedem Anbieter speichert der Broker zudem eine Beschreibung in WSDL, die er vom Serviceanbieter zugestellt bekommt. Diese Beschreibung wird dem Konsumenten zurückgeschickt, welcher nun alle nötigen Informationen hat um direkt den eigentlichen Servicenabieter kontaktieren zu können und den Service zu verlangen. Diese Kommunikation zwischen Konsument und Anbieter läuft üblicherweise über SOAP ab, wobei auch andere Alternativen denkbar sind. Dieser Ablauf wird in Graphik 4.5 übersichtlich dargestellt.

4.2.7 Zusammenfassung

Das Thema Web Service bringt eine neue Art der Interaktion zwischen verschiedenen Dienstanbietern und Nutzern. Dabei kommen verschiedene, zum Teil einzigartige Technologien zum Einsatz. Die Grundlage bildet dabei XML, welches auch in anderen Bereichen bereits bekannt ist. Auf dieser Basis wurde SOAP entwickelt und eingeführt als der Kommunikationsstandard für Web Services. Damit die verschiedenen angebotenen Dienste auf

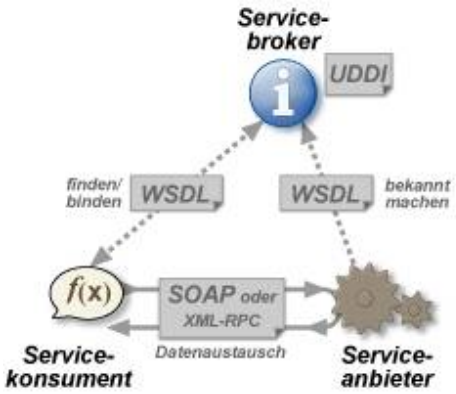


Abbildung 4.5: Überblick Web Services

eine einheitliche Weise beschrieben werden können, wurde zudem die WSDL definiert. Und schliesslich wurde mittels dem UDDI Protokoll eine Möglichkeit geschaffen, Dienste verschiedner Anbieter auf einfache Art und Weise zu finden.

4.3 Überblick der Sicherheitsaspekte von Web Services

Auch für Web Services ist der Aspekt der Sicherheit zentral. Dabei reicht das Spektrum von der Analyse der zu Grunde liegenden Technologien bis hin zu Mustern die aus anderen Bereichen bereits bekannt sind. Zunächst wird eine von Demenchenko vorgeschlagene Gliederung in 5 Sicherheitsgruppen vorgestellt, die einen Überblick über die möglichen Sicherheitsprobleme gibt. Anschliessend folgt eine Untersuchung zweier Schichten des OSI Modells, die für Web Services zentral sind. Als dritter Punkt wird das Zonenmodell beschrieben, gefolgt von Erläuterungen über die Anwendungen von Policies auf Web Services. Da XML mit den XML Signaturen bereits einige Sicherheitsmerkmale aufweist, werden auch diese genauer untersucht. Anschliessend werden mit dem Konzept der Sicherheitstokens und „Trust-Serv“ zwei Möglichkeiten vorgestellt, um die Vertrauenswürdigkeit des im Voraus unbekannten Partners zu erhöhen. Abschliessend folgt eine Unterschung über Web Services im mobilen Bereich und im Zuge dessen wird auch ein mehrschichtiges Sicherheitsmodell vorgestellt.

4.3.1 5 Gruppen von Sicherheitsproblemen

Demenchenko et al gliedern in [10] Web Services prinzipiell in 5 Gruppen, je nach Ort des Angriffes:

Bei *Attacken auf Benutzerebene (UCA)* handelt es sich um den Diebstahl von Benutzerdaten, so dass sich ein Angreifer als anderer Benutzer ausgeben kann.

Vor allem in unkontrollierten Umgebungen können *Attacken auf der Übertragungsebene (WIA)* auftreten. Dabei handelt es sich um Angriffe auf den Übetragungskanal. Mögliche konkrete Bedrohungen sind unerlaubtes Mithören oder Abfangen von Nachrichten.

So genannte *„Malefactor initiated attacks (MIA)“* können sowohl über traditionelle als auch Web Service spezifische Methoden erfolgen. Beispiele hierfür sind Brute-Force Attacken oder WSDL-probing. Erschwerend kommt hinzu, dass die meisten Firewalls Textnachrichten nicht analysieren, also insbesondere auch schädliche SOAP Nachrichten ungehindert passieren können.

Attacken auf die Seitenverwaltung (SMA) basieren auf Fehlkonfigurationen des Servers. Beispiele sind ungenügendes Management und Privilegien oder ungenügende Auswertung von Logdateien. So kann es einem Angreifer möglich sein, seine eigenen Spuren zu verwischen oder unerlaubterweise höhere Privilegien zu erlangen.

Endservice Attacken (ESA) greifen Sicherheitslücken im Endservice an. Dabei werden verschiedene Techniken angwendet um schadhaften Serviceinput zu erzeugen, zum Beispiel XML oder SQL injections.

Die Graphik 4.6 zeigt die eben erwähnten Hauptgruppen in einer übersichtlichen Darstellung. Für konkretere Details sei auf Demenchenko et al in [10] verwiesen.

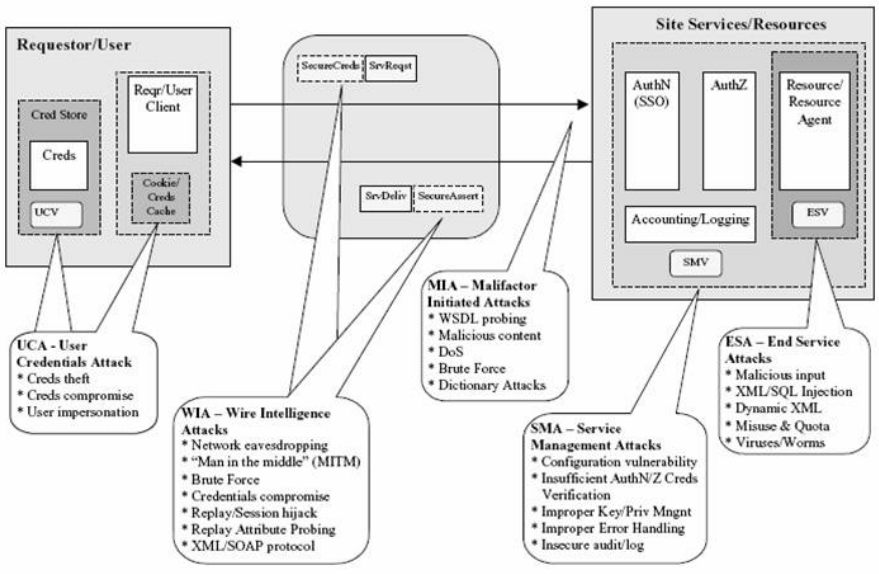


Abbildung 4.6: Sicherheitsaspekte bei Web Services

4.3.2 Sicherheit in der Kommunikation

Da Web Services definitionsgemäss über das HTTP Protokoll kommunizieren, nutzen sie implizit auch alle 7 Schichten des OSI Modells. Besonders interessant im Zusammenhang

mit Web Services ist dabei die Transportschicht. Zudem wird nachfolgend auch auf Sicherheitsaspekte eingegangen, die direkt in der Nachricht integriert sind (message level security).

4.3.2.1 Tansportschicht

Die Transportschicht kann sehr gut mittels SSL oder TSL abgesichert werden kann. So kann sichergestellt werden, dass alle Pakete auch ordnungsgemäss an ihrem Ziel ankommen und nur vom festgelegten Absender stammen. Allerdings bietet die Definition dieser Schichten keine Einflussmöglichkeiten auf die Verarbeitung an den Endpunkten. So bleibt nach wie vor ungeklärt, ob der Kommunikationspartner an sich überhaupt vertrauenswürdig ist. Auch gibt es Probleme an der Firewall, die verschlüsselte Paketströme nicht genauer analysieren und somit den Inhalt des Datenstromes nicht auf schädlichen Inhalt überprüfen kann. Entsprechend würde die Verantwortung vollständig auf dem Empfänger liegen. Eine mögliche Lösung wäre, die SSL Verbindung davor bereits zu beenden. Dies verursacht aber wiederum neue Sicherheitslücken.

4.3.2.2 Nachrichtenlevel

Auf dem Nachrichtenlevel wird insbesondere die Technik der XML Signatur eingesetzt, auf die später nochmals eingegangen wird. Dabei wird die SOAP Nachricht mit dem privaten Schlüssel des Senders signiert und anschliessend mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. So kann der Empfänger sicher sein, dass niemand die Nachricht verändert oder gelesen hat und dass sie auch wirklich vom Sender stammt. Dieses Verfahren kann auf die gesamte Nachricht angewendet werden, oder aber auch nur auf Teile davon. So ist es möglich, sie auch über mehrere Zwischenpunkte an einen Zielservice zu senden, wobei jeder Teilnehmer nur auf die für ihn relevanten Daten zugreifen darf.

4.3.3 Zonenmodell

Um besser auf die vorhin vorgestellten Sicherheitsprobleme reagieren zu können, stellen Yuri Demenchenko und Kollegen [10] ein Zonenmodell speziell für Web Services vor. Dieses ist in Abbildung 4.7 dargestellt und besteht aus folgenden 5 getrennten Bereichen:

- Zone R0 wird von der Ressource selbst kontrolliert.
- Zone R1 ist die Schnittstelle der Ressource zu den weiter aussen liegenden Zonen.
- In den Zonen RA und RAA bewegt sich der Benutzer eines Services. Um sich zu authentifizieren kann auf die Benutzerdatenbank zugegriffen werden.
- Zone RN steht in direktem Kontakt mit der Aussenwelt. Sie kann eine Firewall beinhalten, die die anderen Zonen vor Angriffen von aussen schützt. Ein von aussen auf diese Ressource zugreifender Benutzer kommt direkt nur mit dieser Zone in Kontakt.

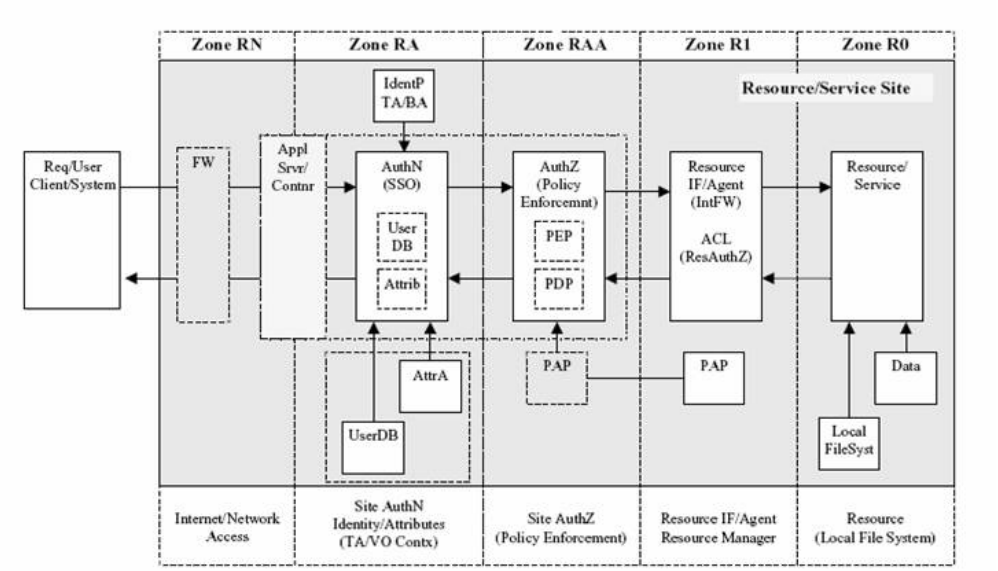


Abbildung 4.7: Zonenmodell

4.3.4 Policies

Policies können ein Teil eines weit gefassten Sicherheitsmodells sein, wie zum Beispiel dem oben vorgestellten Zonenemodell, oder können auch separat angewendet werden. In jedem Fall geht es darum, gewisse für die Sicherheit relevante Informationen eines Dokumentes an Hand festgelegter Regeln zu überprüfen. Die Sprache, die diese Regeln beschreibt muss zum einen mathematisch formal gehalten sein, damit die Regeln automatisch ausgeführt werden können. Auf der anderen Seite muss sie aber auch von Menschen, die diese Regeln aufstellen, verstanden werden. Die Interpretation der aufgestellten Regeln geschieht an den so genannten „policy decision points“. Diese fällen Entscheide an Hand der Vorgaben und leiten diese an so genannte „policy enforcment points“ weiter, die sie dann auf die konkrete Situation anwenden.

4.3.5 XML Signaturen

Im Standard von XML ist bereits eine Form von Sicherheitselementen definiert, so genannte XML Signaturen. Da Web Services definitionsgemäss auf XML basieren, lässt sich diese Technik auch problemlos auf diesen Bereich anwenden. Dies wird unter anderem von Michael McIntosh und Paula Austel in [13] vorgestellt. Die Idee ist, die Nutzdaten im Header der Nachricht mittels eines Schlüssels zu signieren und so die Authentizität und Datenintegrität zu sichern. Besonders vorteilhaft ist der Umstand, dass sich einzelne Elemente separat signieren lassen.

Diese Methode hat allerdings gewisse Sicherheitslücken, insbesondere im Zusammenhang mit kopierten Signaturen. Das Problem sind hierbei die Referenzen, die auf bestimmte Elemente zeigen und der Umstand, dass unbekannte Elemente innerhalb des SOAP Headers übersprungen werden. Kombiniert ein Angreifer diese zwei Punkte, kann er eine

gültige Singatur einer SOAP Datei in eine andere kopieren und muss dabei lediglich ein „Wrapper“ Element einfügen, das die ursprüngliche Nutzlast enthält. Diese ist zwar für die Signatur gülitg und löst somit bei der Überprüfung keinen Fehler aus. Bei der eigentlichen Verarbeitung wird das „Wrapper“ Element aber übersprungen, da es nicht bekannt ist. Statt dessen wird die Verarbeitung unterhalb mit dem neuen, veränderten Bodyelement fortgesetzt. So ist die Signatur zwar weiterhin gültig, es wird aber mit komplett anderen Nutzdaten gearbeitet als vom ursprünglichen Sender eigentlich vorgesehen.

Dieser Sachverhalt ist auch in Abbildung 4.8 dargestellt. In Zeile 008 wird eine Referenz auf „#theBody“ definiert, die sich auf Zeile 018 bezieht. Wenn wie in Zeile 015 gezeigt ein Wrapper Element eingefügt wird, so stört dies die Sicherheitsüberprüfung nicht. Allerdings wird so das „<soap:Body>“ Element aus Zeile 018 bei der Verarbeitung ignoriert, da das Wrapper Element nicht bekannt ist und somit übersprungen wird. Entsprechend wird neu das „<soap:Body>“ Element aus Zeile 023 als relevant angesehen und verwendet, was nicht die Idee des ursprünglichen Codes war.

```
001 <soap:Envelope ...>
002   <soap:Header>
003     <wsse:Security>
004       ...
005       <ds:Signature>
006         <ds:SignedInfo>
007           ...
008           <ds:Reference URI="#theBody">
009             ...
010           </ds:Reference>
011         </ds:SignedInfo>
012         ...
013       </ds:Signature>
014     </wsse:Security>
015     <Wrapper
016       soap:mustUnderstand="0"
017       soap:role=".../none">
018   <soap:Body wsu:Id="theBody">
019     <getQuote Symbol="IBM"/>
020   </soap:Body>
021     </Wrapper>
022   </soap:Header>
023   <soap:Body wsu:Id="newBody">
024     <getQuote Symbol="MBI"/>
025   </soap:Body>
026 </soap:Envelope>
```

Abbildung 4.8: Umgehen der XML Signatur

4.3.6 Sicherheitstokens

Die Idee hinter Web Services ist es, einen passenden Serviceanbieter von einem Servicebroker zu erfahren und sich dann ad hoc mit diesem Anbieter zu verbinden. Sowohl dieser als auch der Benutzer stehen nun vor dem Problem, dass sie sich gegenseitig noch nie zuvor gesehen haben und somit auch nicht wissen, ob sie sich gegenseitig vertrauen können. Das Hauptproblem liegt darin, dass sich der Service Provider mit den Daten des Benutzers maskieren und sich damit seinerseits an einem anderen Web Service als seinen Klienten ausgeben könnte. Um dieses Situation zu beheben, schlagen Kearney und Kollegen [9] vor, die von Kerberos bekannten Token zu benutzen. Der Ablauf ist in 4.9 dargestellt und sieht wie folgt aus:

- Schritt 1: Der Benutzer fordert einen „identity token“ von einer vertrauten Instanz an. Dieser Schritt ist nur ein Mal nötig.
- Schritt 2: Der Benutzer fordert vom Dienstanbieter einen „service token“ an.
- Schritt 3: Diese beiden Token schickt der Benutzer nun wiederum an die vertraute Instanz. Darauf erhält er einen servicespezifischen Identitätstoken.
- Schritt 4: Dieser für jeden Benutzer und Service spezifischen Token schickt der Konsument dann an den Service.
- Schritt 5: Der Service validiert mit Hilfe der vertrauten Instanz des Benuzters.

Somit ist sichergestellt, dass der Benuzter keine sensitiven Daten (zum Beispiel eine Kombination aus Benutzername und Passwort) an den Web Service senden muss und kann trotzdem vom Web Service Anbieter identifiziert werden kann. Dieser Ablauf ist in der Abbildung 4.9 ersichtlich.

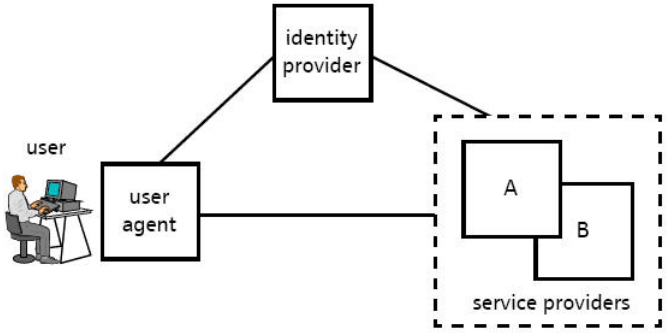


Abbildung 4.9: Ablauf des Token Prozesses

4.3.7 Trust-Serv

Auch das von Skogsrud und Kollegen [12] entwickelte Konzept von Trust-Serv befasst sich mit der Problematik, dass die meisten Benutzer dem Servieanbieter nicht bereits bekannt sind und somit noch kein Vertrauensverhältnis besteht. Skogsgrud löst dies, in dem in einer zustäzlichen Schicht die konkreten Berechtigungen von zwei Verhandlungssteuerungen ausgehandelt werden. Diese Schicht ist transparent für den Web Service, der davon also nicht direkt betroffen ist. (siehe Abbildung 4.10)

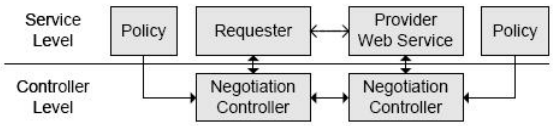
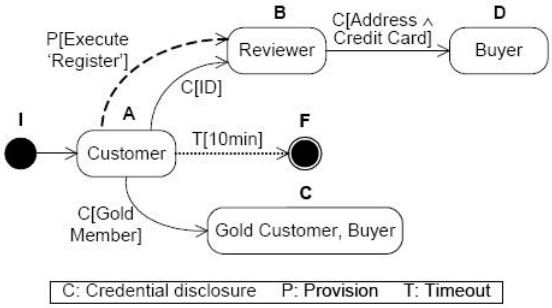


Abbildung 4.10: Unterschiedliche Levels bei Trust-Serv

Auf Seiten des Diensteanbieters basiert das System auf einer Zustandsmaschine. Der Benutzer startet in einem Grundzustand und wechselt dann in andere Zustände mit erhöhten Privilegien, je nachdem welche zusätzlichen Daten er übermittelt. So kann die Vergabe von Berechtigungen vollkommen ausserhalb des Systems der Web Services geschehen.

Im konkreten Beispiel aus Abbidlung 4.11 startet der Benutzer im Grundzustand „Customer (A)“. Wenn er sich mit einer ID identifiziert oder eine Registrierung durchführt, kommt er in den Zustand „Reviewer (B)“. Falls er dann seine Adresse und Kreditkartendaten eingibt, wechselt er in den Zustand „Buyer (D)“. Falls er sich aus Zustand A aber als Gold Member identifizieren kann, wechselt er direkt in den Zustand „Gold Customer, Buyer (C)“ und erhält die entsprechenden Rechte. Falls aus Zustand A heraus keine weitere Aktion seitens des Benutzers statt findet, tritt nach 10 Minuten ein Timeout auf und es wird der Endzustand F erreicht.



Role	Operation	Credential
Customer	Register, Search	Verified by Visa
Reviewer	Write review	Elite Bookshops Member
Gold Customer	Special offers	
Buyer	Purchase	

Abbildung 4.11: Beispiel einer Zustandsmaschine

4.3.8 Mobile Web Services

Auf Grund der begrenzten Ressourcen mobiler Endgeräte liegt es nahe, auch in diesem Bereich Web Services zu nutzen. So kann man rechenintensive Anfragen oder umfangreiche Geschäftslogik sehr einfach auf einen viel leistungsstärkeren Server auslagern. Mittels XML-Nachrichten können auf einfache Weise Anfragen an diese Server übermittelt und somit die gewünschten Informationen direkt bezogen werden. Allerdings bestehen auch Gefahren in dieser Form der Nutzung und es könnte vorkommen, dass unbewusst sensible Daten an bislang unbekannte Web Services gesendet werden. Aus diesem Grund schlagen Weippl und Essmayr [11] ein mehrschichtiges Sicherheitsmodell vor. Dieses basiert auf dem „need-to-know“ Prinzip, so dass jeder Service nur genau auf jene Ressourcen zugreifen kann, die für eine korrekte Ausführung unbedingt benötigt werden. Die drei vorgeschlagenen Schichten sind:

- System
- Benutzer, kann unterteilt werden in verschiedene Bereiche

- Web / Netzwerk, kann unterteilt werden in „vertraut“, „teilweise vertraut“ und „nicht vertraut“, je nach Zugriff

Die Idee ist, diese drei Bereiche strikte zu trennen, so dass ein Programm aus dem Netzwerkbereich weder Zugriff auf die Daten des Benutzers, noch auf das System hat. Der grosse Nachteil in einer solchen strikten Trennung ist aber, dass der Benutzer seine persönlichen Daten entsprechend immer wieder neu eingeben muss, wenn ein Service dies verlangt. Erweitert man dieses Konzept jedoch um die Idee der Webidentitäten, dann lässt sich auch dieses Problem lösen. Dabei definiert man drei Level von Anonymität, die der Benutzer dynamisch auswählen kann:

- Vollständig Anonym: Das Mobile Gerät erstellt Zufallsdaten und übermittelt diese an den Web Service. Anschliessend werden diese Daten gelöscht.
- Maskiert: Das Mobile Gerät erstellt Zufallsdaten, speichert diese allerdings nach der Übermittlung an den Web Service. So können die gleichen Daten wieder verwendet werden und der Service kann den Benutzer wiedererkennen.
- Identifiziert: Der Benutzer gibt seine richtigen Daten ein.

Mit diesen drei Abstufungen ist wiederum gewährleistet, dass die wirklichen Daten des Benutzers bestmöglich verborgen bleiben, bis diese wirklich benötigt werden.

4.3.9 Zusammenfassung

In diesem Kapitel wurde deutlich, dass im Bereich Web Services verschiedene Methoden zur Verbesserung der Sicherheit bereitstehen. Allerdings sind nicht alle Probleme vollständig gelöst, insbesondere im Bereich von XML Signaturen.

4.4 Analyse und Schlussfolgerungen

4.4.1 Analyse

Wie erwähnt, ist eine der Grundideen hinter Web Services, dass Dienste bei Bedarf ad hoc gesucht und bezogen werden können. Dabei ist zum Zeitpunkt des Bedarfs der Anbieter eines Services noch nicht bekannt, sondern muss erst über den Service Broker ermittelt werden. Dieses Szenario weist eine hohe Dynamik auf und ermöglicht die Nutzung von Diensten von bislang unbekannten Anbietern. Das bedeutet aber gleichzeitig, dass die Vertraunswürdigkeit der gegenüberliegenden Stelle (sowohl Konsument als auch Anbieter) nicht im Voraus bekannt sein kann. Somit wird erst im Schadensfall wirklich bemerkt, dass das entgegengebrachte Vertrauen missbraucht wurde. Keine der in dieser Arbeit vorgestellten Technologien kann dies komplett verhindern, was die grosse Schwäche von Web

Services darstellt. Dies zeigt sich auch in der aktuellen Marktsituation. Anders als erwartet wurde gibt es zur Zeit keine grossen Netze von kooperierenden Firmen, die dynamisch Angebote anderer Firmen nutzen. Web Services werden zur Zeit in folgenden Bereichen eingesetzt:

- Unternehmensintern
- Zwischen zwei Unternehmen die sich vertrauen und deren Beziehung sich in stabilen Verhältnissen bewegt
- Bei unkritischen Anwendungen im Internet, zum Beispiel Suchanfragen oder Lieferstati

4.4.2 Schlussfolgerungen

In der Analyse konnte gezeigt werden, dass sich Web Services auf Grund von Sicherheitsbedenken zur Zeit noch nicht für den Praxiseinsatz in unternehmenskritischen Geschäftsbereichen geeignet sind. Ein grosses Problem ist die dynamische Suche nach Servicepartnern, so dass vor der Benutzung eines Services die Vertraunswürdigkeit des Partners nicht geprüft werden kann. Dies stellt jedoch genau die Grundidee dieser neuen Technologie dar. Mittels der Verwendung des Trust-Serv Konzepts oder Sicherheitstokens lässt sich dies jedoch eindämmen, es bedeutet jedoch einen höhere Implementierungsaufwand und im Falle von Tokens braucht es eine zusätzliche externe Vermittlungsstelle. Weitere Probleme können mutwillige Angriffe verursachen, welche aber mittels der Konzepte des Zonenmodells und effizienten Policies bekämpft werden können. Es bleiben die Probleme mit XML Signaturen, die bislang noch nicht vollständig gelöst werden konnten.

4.4.3 Ausblick

Auf Grund der gravierenden Sicherheitsmängel insbesondere im Zusammenhang mit den XML Singaturen wird sich diese Technik in breiter Front vermutlich nicht durchsetzen können. Allerdings besteht ein grosses Potenzial in bereits sehr gut abgesicherten Umgebungen.

In der Forschung gibt es zwei Tendenzen: Zum einen wird eine „Security Assertion Markup Language (SAML)“ erarbeitet um insbesondere dem Problem mit den XML Singaturen zu begegnen. Zum anderen sollen Web Services um die Konzepte des Semantic Web erweitert werden, so dass das Auffinden und Ausführen von neuen Web Services automatisiert werden kann.

Literaturverzeichnis

[1] Web Services Architecture Requirements; http://www.w3.org/TR/2004/NOTE-wsa-reqs-20040211/, November, 2007.

[2] Extensible Markup Language (XML) 1.0; http://www.w3.org/TR/REC-xml/, November, 2007.

[3] SOAP Version 1.2 Part 1: Messaging Framework; http://www.w3.org/TR/soap12-part1/, November, 2007.

[4] Web Services Description Language (WSDL); http://www.w3.org/TR/wsdl/, November, 2007.

[5] UDDI 101, http://uddi.xml.org/uddi-101/, November, 2007.

[6] Will Iverson: Real World Web Services, O'Reilly Medai, 2005.

[7] Rickland Hollar, Richard Murphy: Enterprise Web Services Security; Thomson Delmar Learning, 2006.

[8] Inderjeet Singh et al.: Designing Web Services with the J2EETM 1.4 Platform - JAX-RPC, SOAP, and XML Technologies, http://java.sun.com/blueprints/guidelines/designing_webservices/html/index.html, June, 2007.

[9] P. Kearney et al.: An Overview of Web Services Security; BT Technology Journal, Volume 22, Issue 1 (2004), Kluwer Academic Publishers.

[10] Y. Demchenko et al.: Web Services and Grid Security Vulnerabilities and Threats Analysis and Model, GRID archive, Proceedings of the 6th IEEE/ACM International Workshop on Grid Computing, IEEE Computer Society.

[11] Edgar Weippl, Wolfgang Essmayr: Personal trusted devices for web services: revisiting multilevel security, Mobile Networks and Applications, Volume 8, Issue 2 (April 2003), Kluwer Academic Publishers.

[12] Halvard Skogsrud, Boualem Benatallah, Fabio Casati: Trust-serv: model-driven lifecycle management of trust negotiation policies for web services, ACM Press 2004.

[13] Michael McIntosh, Paula Austel: XML signature elent wrapping attacks and countermeasures, Workshop On Secure Web Services, Proceedings of the 2005 workshop on Secure web services, ACM Press.

Kapitel 5

BioLANCC und die Datenschutzgesetze

Leandra Graf

BioLANCC ist ein Verwaltungsprogramm für biometrische Zutrittssysteme. Diese Systeme ersetzen die traditionelle Überprüfung mittels Wissen (Passowort, PIN) und/oder Token (SmartCard) durch ein biometrisches Merkmal wie den Fingerabdruck oder einen Irisscan. Das Programm BioLANCC ist die Schnittstelle zwischen dem Zentralspeicher, in dem die Datenbank gespeichert ist, und den Sensoren, die die biometrischen Merkmale lesen. Mit BioLANCC kann man Templates verteilen und Zutrittsrechte für bestimmte Türen vergeben. Die biometrischen Daten werden von BioLANCC in einer Datenbank gespeichert, was Konflikte mit dem Datenschutzgesetz hervorrufen kann. Eine einfache Lösung für dieses Problem wäre, keine Datenbank anzulegen, sondern die Daten auf SmartCards zu speichern und den betroffenen Personen abzugeben. Wird hingegen eine zentrale Datenbank angelegt, muss unbedingt der Anwender informiert werden. Damit die Daten nicht unbefugt verändert, gefälscht oder gelesen werden, sollte man die Daten im zentralen Speicher und alle Kommunikationswege zu verschlüsseln. Verlust, Löschung und Vernichtung aller Daten kann man vermeiden, indem man ein Backup anlegt, mit dem sich die Daten wieder herstellen liessen.

Inhaltsverzeichnis

5.1 Einleitung

Pässe mit Fingerabdruck, Zugangskontrollen per Iris-scan und Überwachung mittels Gesichtserkennung: in allen möglichen Bereichen nimmt die Verwendung von biometrischen Daten zu. Sogar in Badeanstalten[23] und ZOOs [18] werden zur Eingangskontrolle biometrische Daten verwendet. Längst hat sich die Biometrie von Spionagefilmen über Hochsicherheitskontrollen zum Alltag entwickelt. Biometrische Systeme werden immer billiger und Sensoren sind sogar schon im Fachhandel im Angebot [5].

In Deutschland wird seit dem 1. November 2007 der Pass mit zwei Fingerabdrücken versehen. Von offizieller Seite wird betont, dass der biometrische Pass sicher sei, was jedoch von verschiedenen Seiten angezweifelt wird. Unter anderem wird kritisiert, dass der Chip mit den biometrischen Daten, der sich im Pass befindet, zerstört werden kann und ein Kontrolleur den Pass trotzdem akzeptieren muss, da nicht nachzuprüfen ist, ob er durch Absicht oder einen Unfall zerstört wurde - letzteren hätte ein Benutzer kaum bemerken können [24]. Ein weiterer Kritikpunkt ist, dass der Pass mit der Umwelt per Funk kommuniziert, was ein deutlich leichteres Abhören (und damit Kopieren, Lesen und Stehlen) ermöglicht als bei leitungsgebundener Kommunikation [15]. Ein weiterer Diskussionspunkt ist der Datenschutz dieser sensiblen Daten.

In der vorliegenden Arbeit wird vor allem die Zugangskontrolle genauer untersucht. Dabei ist es zweitrangig, ob es sich um den Zugang zu einem Gebäude, einem Gerät oder einem Dienst (z. B. e-Banking) handelt. Bei der traditionellen Zugangskontrolle wird meistens nach einem Passwort oder einem PIN, die geheimes Wissen darstellen, gefragt. Manchmal zusätzlich nach dem Vorweisen eines Tokens (z. B. einer Smartcard), das sich im Besitz einer Person befindet. Das Problem von diesen Kontrollmechanismen ist, dass damit nicht geprüft werden kann, ob es sich tatsächlich um die betreffende Person handelt. Ein Dieb oder Vertrauter kann in Besitz des Tokens kommen und den PIN oder das Passwort kennen. Helmut Reimer bezeichnet PIN und Passwort als „*personenbezogen*, aber nicht *personengebunden*“.[14] Biometrische Merkmale können im Gegensatz zu PIN und Token nicht gestohlen, verraten oder grob fahrlässig aufbewahrt werden. Die Sicherheit ist aber auch bei biometrischen Systemen nicht perfekt. Einige Spezialisten sind jedoch der Ansicht, dass die Biometrie ein sehr sicheres Mittel sei [16].

Ein anderes Problem, das bei biometrischen Sicherheitssystemen auftaucht, ist die Tatsache, dass man biometrische Daten zur Kontrolle in Datensammlungen speichert. Biometrische Daten sind in doppelter Hinsicht sensibel: Zum einen ändern sie sich nie. Dies kann zum Problem werden, wenn eine Person in ein Zeugenschutzprogramm müsste. Beim biometrischen Pass bliebe das biometrische Merkmal (z. B. der Fingerabdruck) weiterhin mit ihrer alten Identität verbunden. Zum anderen kann man aus vielen Rohdaten Rückschlüsse auf die ethnische Herkunft oder den Gesundheitszustand ziehen [10]. Solche Daten werden im schweizerischen Datenschutzgesetz als „besonders schützenswerte Personendaten“ bezeichnet (DSG Art. 3c).

Die europäischen Staaten bemühen sich daher, den Schutz solcher sensibler Daten gesetzlich zu garantieren. In dieser Arbeit sollen zu Beginn die Datenschutzgesetzgebung der Schweiz und die Datenschutzrichtlinie der EU untersucht werden, um zu sehen, wie Daten geschützt werden müssen. Die beiden Rechtstexte werden inhaltlich verglichen, wobei

die generelle Ähnlichkeit und einzelne Unterschiede aufgezeigt werden. Danach sollen die biometrischen Systeme ausführlich in ihrer historischen Entstehung und der Funktionsweise beschrieben werden. Es wird ebenfalls gezeigt, wie der Ablauf der Installation eines biometrischen Systems aussieht. Zum Schluss wird ein Programm, das die Verwaltung biometrischer Zugangsdaten organisiert, untersucht. Bei diesem Programm (BioLANCC) soll geklärt werden, was bei einer Anwendung getan werden muss, damit die Datenschutzgesetze eingehalten werden. Und ob es für das Programm in dieser Hinsicht technisches Verbesserungsmöglichkeiten gibt. Es soll geklärt werden, wo Änderungen im Programm vorgenommen werden sollten.

5.2 Die Datenschutzgesetze

In der Schweiz gibt es neben dem Datenschutzgesetz (DSG) auch eine Verordnung zum Bundesgesetz über den Datenschutz (VDSG), die das Gesetz detailliert behandelt. Sie stammen aus den Jahren 1992 und 1993, wurden jedoch ständig aktualisiert. Diese Arbeit bezieht sich auf den Stand vom Dezember 2006 [1] [2]. Als Grundlage für die EU-Richtlinie wird die deutsche Version des offiziellen Gesetzestextes vom 24. Oktober 1995 verwendet [3] [4].

Da BioLANCC vor allem im privatwirtschaftlichen Bereich Anwendung finden wird, konzentriert sich diese Arbeit auf das Untersuchen der Abschnitte mit allgemeinen Bestimmungen oder Bestimmungen für die Bearbeitung durch private Personen. Das schliesst das Bearbeiten von Personendaten durch Bundesorgane (Abschnitt 4 des DSG) aus.

5.2.1 Entstehung und Ziele der Datenschutzgesetze

Im Laufe der Industrialisierung nahm die Bevölkerungszahl zu. Ausserdem erhöhte sich die Mobilität, internationale Reisen waren nicht mehr abenteuerliche Unternehmen Einzelner. Dies führte dazu, dass eine Ausweisung nötig wurde. Eine andere besonders wichtige Neuerung war die Trennung von Arbeitsplatz und Wohnraum. Dadurch entstand erst eine Privatsphäre, die vom öffentlichen Lebensraum getrennt werden konnte. Es entwickelte sich die Idee, die private Sphäre schützen zu müssen. Gleichzeitig erhöhte sich der Bedarf an Informationen über Personen, v.a. in Firmen und der staatlichen Verwaltung. Man könnte diesen Vorgang als Bürokratisierung bezeichnen. Das Bedürfnis nach Übersicht konnte nur noch mit systematischer Registrierung befriedigt werden.

Am Anfang wurden Daten auf Karteikarten oder in Hängeregistern gesammelt. Dadurch war der Umfang der Sammlung aus Platzgründen und vom Bearbeitungsaufwand her begrenzt. Sortier- sowie Suchvorgänge waren wesentlich schwerer zu bewerkstelligen als dies mit digitalisierten Daten möglich ist. James Thomas Peter zählt einige technische Eigenschaften von Rechnern auf, die sich problematisch auf den Datenschutz auswirken können: Es kann eine grosse Menge von Daten zeitlich unbeschränkt gespeichert werden; die Daten können nach verschiedenen Kriterien gleichzeitig sortiert werden; die Bearbeitung erfolgt äusserst schnell; Datenbanken lassen sich vernetzen und Daten können sehr

rasch um den ganzen Globus übermittelt werden. Dabei ist den Datenbearbeitern immer weniger bewusst, was für Daten sie bearbeiten und wozu. Informationen sind längst zu einer Ware geworden, die bedenkenlos getauscht, verarbeitet, gespeichert, gesucht oder auch gelöscht werden [8].

Ein unproblematisches Beispiel einer solchen Datenbank ist ein Bibliothekskatalog. Es lässt sich mit verschiedenen Kriterien nach einem Werk suchen (Autor, Signatur, Titel...), manche Bibliotheken sind in einem Verbund zusammengefasst und die Bibliothek kann durchaus weit entfernt sein. Ausserdem geht die Suche sehr schnell. Früher wurden die Kataloge in Zettelform geführt. So konnten sie nur nach einem Kriterium sortiert werden, für ein weiteres Kriterium brauchte man einen weiteren Katalog. Dies kostete viel Platz, während für das neue System ein Computer mit Zugriff zur Datenbank reicht.

In der Anfangszeit des Datenschutzes wurde vor allem die Überwachung durch den Staat gefürchtet, was daran lag, dass computergestütze Datenbanken vor allem in den Verwaltungen eingesetzt wurden [11]. 1978 wurde in einer Fernsehsendung mit dem Titel „Computer können nicht vergessen“ auf die Problematik der Personendaten aufmerksam gemacht. Damals war die Angst vor einem Szenario, wie es George Orwell in seinem Roman *1984* beschrieben hatte, vorherrschend. Höhepunkt der Diskussion war das in Deutschland 1977 verabschiedete erste Datenschutzgesetz [13]. 1980 folgte schon das Datenschutzgesetz in Österreich [9], erst 1993 verabschiedete das Schweizer Parlament als eines der letzten westeropäischen Länder ein Datenschutzgesetz (DSG) [6]. Die EU versuchte, die Datenschutzgesetze in Europa zu harmonisieren, um einen internationalen Austausch von Daten zu erleichtern. Sie erliess eine Datenschutzrichtlinie, deren Frist für die Umsetzung in nationales Recht 1998 abgelaufen ist [7].

Die Richtlinie soll den internationalen Austausch von Daten in Europa erleichtern. Der Transfer ist nur gestattet, wenn das Land des Empfängers Datenschutzgesetze erlassen hat, die den europäischen vergleichbar sind. In den USA ist dies beispielsweise nicht der Fall, weshalb man sich anders behelfen muss. Will eine amerikanische Firma Daten aus Europa, muss sie sich den hier geltenden Richtlinien unterwerfen. Sie gilt dann als „safe harbour“ und darf Daten aus Europa empfangen [11]. Aus diesem Grund gab es heftigen politischen Wiederstand gegen den Transfer von Passagierdaten in die USA [12].

5.2.2 Datenschutz in der Schweiz

Entgegen häufiger Annahmen gilt das Datenschutzgesetz auch, wenn man als private Person Daten sammelt (Art. 2 Abs. 1 DSG), es sei denn, man sammelt sie *ausschliesslich* für den privaten Gebrauch und gibt sie nicht an Aussenstehende weiter (Art. 2 Abs. 2a DSG). Das Gesetz wird also nicht auf ein privates Adressbuch angewendet, selbst wenn bei jedem Namen ein Fingerabdruck aufgeführt ist, solange man diese Daten an niemanden weitergibt und sie nicht gewerbsmässig verwendet.

Als „besonders schützenswerte Personendaten“ gelten Dinge, die nicht öffentlich sind, die man also z. B. nicht im Telefonbuch findet. Einzeln aufgeführt werden religiöse, weltanschauliche, politische und gewerkschaftliche Ansichten oder Tätigkeiten, ebenso Dinge, die zur Intimsphäre gehören wie die Gesundheit, oder Dinge, die eine Diskriminierung

zur Folge haben könnten, wie die ethnische Herkunft. Auch der Empfang der Sozialhilfe und administrative oder strafrechtliche Verfolgungen sind sensible Daten. (Art. 3c DSG) Dieser Regelung liegt der Gedanke zu Grunde, dass jeder selber entscheiden darf und soll, was über ihn bekannt ist und was nicht. Wenn eine offizielle Funktion ausgeübt wird (z. B. ein Pfarramt oder ein politisches Amt) werden selbstverständlich sensible Daten öffentlich bekannt - jedoch mit Wissen und (meistens vorausgesetztem) Einverständnis der betroffenen Person.

Sensible Daten werden erst dann zu einem rechtlichen Problem, wenn sie gesammelt werden. Unsere ethnische Herkunft ist oft auf einen Blick erkennbar, ebenso lassen wir überall unsere Fingerabdrücke zurück. Doch erst wenn diese Daten gespeichert werden, ist es ein Eingriff in unsere Privatsphäre. Eine *Datensammlung* ist erst dann gegeben, wenn von den Daten auf die betroffenen Personen geschlossen werden kann. Eine anonyme Umfrage gehört also nicht dazu, wenn man nur Alter und Geschlecht angeben muss.

Die wichtigsten Bestimmungen des schweizerischen Datenschutzgesetzes sagen aus, dass man die Daten **rechtmässig beschaffen und verarbeiten muss** (Art. 4 DSG), die **Daten richtig**, d. h. korrekt, sein sollen (Art. 5 DSG) und **vor Verlust bzw. Veränderung und Löschung gesichert** sein sollen (Art. 7 DSG). Vor welchen genauen Risiken die Daten gesichert sein müssen, wird in der Verordnung zum DSG ausgeführt. So muss man die Daten vor allem vor Vernichtung (unbefugte oder zufällige), Verlust, Fehler, Fälschung und Diebstahl, sowie unbefugtes Zugreifen, Ändern oder Kopieren schützen (Art. 8, insbes. Abs. 1 VDSG).

Die meisten Datensammlungen mit besonders schützenswerten Daten müssen beim eidgenössischen Datenschutzbeauftragten registriert werden. Wenn die betroffenen Personen wissen, dass Daten von ihnen gesammelt und gespeichert werden, und der Sammlung zustimmen, ist die Anmeldung nicht nötig. Werden jedoch die Daten an Dritte weitergegeben, ist eine Registrierung wieder notwendig (Art. 11 Abs. 3 DSG). Wenn also eine Firma Daten ihrer Mitarbeiter sammelt und sie an eine Partnerfirma weitergibt, ist die Datensammlung registrierpflichtig. In der Verordnung zum DSG werden der Ablauf und die Modalitäten der Anmeldung ausgeführt (Art. 3 VDSG). Die Weitergabe an Dritte kann auch ein Auftrag zur Verarbeitung sein. Wird die Bearbeitung der sensiblen Daten Dritten überlassen, muss der Auftraggeber sicherstellen, dass die Daten nur so bearbeitet werden, wie er selbst es tun dürfte (Art. 14 Abs. 1 DSG). Der Auftraggeber trägt also immer noch die Hauptverantwortung für den Umgang mit den Daten.

Der Datenschutzbeauftragte ist die wichtigste Institution im Datenschutz. Er führt nicht nur das Register aller meldepflichtigen Datensammlungen, er übt auch eine Beratungsfunktion für Private und Firmen aus. Der Datenschutzbeauftragte darf von sich aus Systeme überprüfen, doch er tut dies auch zwingend, wenn Daten ins Ausland gegeben werden (Art. 29 Abs. 1 DSG, s. a. Art. 5-7 VDSG). Dies geschieht zum Beispiel bei internationalen Firmen mit mehreren Standorten. Wichtig ist, dass der Beauftragte keine Gewalt hat, er kann lediglich Empfehlungen geben. Werden diese nicht befolgt, leitet er den Fall ans Bundesverwaltungsgericht weiter (DSG Art. 29 Abs. 3-4).

5.2.3 Datenschutzbestimmungen der EU

Die Richtlinie der EU definiert ausführlich, was „personenbezogene Daten“ genau sind. Damit sind alle Informationen gemeint, mit denen eine Person identifiziert werden kann (Art. 2a). Ganz ähnlich wie in der Schweiz existiert nur dann ein rechtliches Problem, wenn sie über Angaben wie Alter und Geschlecht hinausgeht. Genauso gilt die Richtlinie nicht für Tätigkeiten, die in persönlichem und familiärem Umfeld stattfinden (Art. 3 Abs. 2). Das heisst, auch hier wäre ein privates Adressbuch nicht im Bereich des Gesetzes. In Artikel 6 werden ähnliche Grundlagen festgelegt, die auch im schweizerischen DSG vorhanden sind: Die Verarbeitung soll rechtmässig sein, die Daten dürfen nur für einen bestimmten Zweck erhoben werden, sie müssen sachlich richtig sein und dürfen nicht länger als nötig gespeichert werden (Art. 6 Abs. 1).

Gewisse Daten dürfen *gar nicht* verarbeitet werden. Dazu gehören Daten, aus denen die rassische/ethnische Herkunft, politische, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit ablesbar sind, ebenso private Daten über die Gesundheit und Sexualität (Art. 8 Abs. 1). Von dieser strengen Regel gibt es eine Reihe von Ausnahmen, die wichtigste ist, dass man solche Daten verarbeiten darf, wenn die Person ihre Zustimmung gegeben hat (Art. 8 Abs. 2a). So weiss man von Politikern immer, welcher Partei sie angehören. Eine andere Ausnahme betrifft die Ärzte, die in ihrer Patientenkartei Daten zum Gesundheitszustand gespeichert haben müssen.

Eine Person, über die Daten gespeichert werden, muss über den Zweck und den Verarbeiter informiert werden, egal, wo die Daten erhoben wurden (Art. 10-11). Das heisst, wenn eine Firma Daten von einer anderen Firma bekommt, muss die betroffene Person darüber informiert werden. Das gilt allerdings nicht für statistische, historische oder andere wissenschaftliche Forschung (Art. 11 Abs. 2).

Ebenso wie das schweizerische Gesetz sieht auch die EU-Richtlinie vor, dass die Daten vor Zerstörung, Verlust, unbefugter Änderung, unberechtigter Weitergabe oder unberechtigtem Zugang geschützt sind. Allgemein wird von „technischen und organisatorischen Massnahmen“ gesprochen (Art. 17 abs. 1), die zum Schutz der Daten getroffen werden müssen. Wie genau dies implementiert werden soll, hängt vom System und den Daten ab.

Auf der nationalstaatlichen Ebene sieht die Richtlinie eine Kontrollstelle vor, wo der für die Verarbeitung Verantwortliche die Datensammlung anmeldet (Art. 18 Abs. 1). Diese Kontrollstelle existiert neben dem Datenschutzbeauftragten, der freiwillig als Berater hinzugezogen werden soll (Art. 18 Abs. 2, sowie Art. 20 Abs. 2).

5.2.4 Vergleich der EU-Richtlinie und der schweizerischen Gesetzgebung

Das schweizerische und das europäische Recht ähneln sich auf den ersten Blick recht stark, doch es gibt einige Unterschiede. Sowohl in der europäischen Richtlinie als auch im schweizerischen nationalstaatlichen Gesetz gelten die Bestimmungen nur, sobald sie den Bereich des privaten Bereiches verlassen. Doch während das schweizerische Recht gewisse

Daten nur als *„besonders schützenswert“* bezeichnet, verbietet die europäische Richtlinie deren Verarbeitung ganz. Die schweizerische Variante ist weniger präzise formuliert, doch sie bietet den Vorteil, keine Ausnahmen machen zu müssen. Die europäische Richtlinie macht mehrere Ausnahmen, so für Ärzte oder bei Zustimmung der betroffenen Personen.

Die Daten, die unter die Verarbeitungsbestimmungen fallen, sind grösstenteil gleich:

- religiöse Überzeugung
- weltanschauliche bzw. philosophische Überzeugung
- politische Überzeugung
- die rassische oder ethnische Herkunft
- Mitgliedschaft in einer Gewerkschaft
- Gesundheit

Die europäische Richtlinie führt ebenso die Sexualität auf, was im DSG der Schweiz fehlt, dafür zählt die Schweiz auch Empfang der Sozialhilfe und strafrechtliche Verfolgung zu den besonders schützenswerten Daten.

Die generellen Bestimmungen sind vom Gedanken her gleich, in der Formulierung unterscheiden sie sich leicht. Die wichtigsten Punkte sind die rechtmässige Verarbeitung und die sachliche Richtigkeit, dazu kommt in der europäischen Richtlinie noch die Zweckgebundenheit und dass die Daten nicht länger als nötig gespeichert werden dürfen. Die Richtlinie ist in diesem Punkt also noch etwas strenger als das Schweizerische Gesetz. Beide Texte sehen einen Schutz gegen Verlust, Änderung und Löschung vor. Die möglichst konkrete Verordnung ist etwas ausführlicher in der Aufzählung der unerlaubten Handlungen als die grobe Richtlinie der EU.

Ein weiterer wichtiger Unterschied ist die Rolle des Datenschutzbeauftragten. In der Schweiz ist er als Berater tätig, doch er führt auch das Register mit Datensammlungen und kontrolliert von sich aus solche. Die EU sieht für diese Funktionen zwei Stellen vor: die Anmeldung (was im schweizerischen DSG Registrierung genannt wird) erfolgt bei der nationalen Kontrollstelle. Der (ebenfalls nationale) Datenschutzbeauftragte fungiert danach lediglich als Berater, den man freiwillig konsultieren darf, er hat keine Kontrollfunktion.

5.3 Biometrische Systeme

5.3.1 Geschichte Biometrischer Systeme

Seit Jahrhunderten dient die Unterschrift auf Verträgen als Nachweis der persönlichen Zustimmung. Schon im Corpus Iuris Civilis aus dem Jahr 533 wurde die Unterschrift als Mittel der Willensäusserung erwähnt. Der Fingerabdruck wurde als Erkennungsmittel sogar schon vor 9000 Jahren verwendet. Töpfer kennzeichneten in China und bei den

Assyrern die Keramik mit ihrem Fingerabdruck, um sich als Hersteller zu identifizieren. Ebenfalls sehr alt ist die Verwendung eines Tokens, das üblicherweise ein einfacher Schlüssel war.

Seit dem 17. Jahrhundert wurden erste wissenschaftliche Untersuchungen zu Fingerabdrücken unternommen und schon seit 1901 setzt Scotland Yard Fingerabdrücke bei ihren Ermittlungen ein. In den späten 60er Jahren des 20. Jahrhunderts begann das amerikanische FBI, registrierte Fingerabdrücke mit Computern zu verarbeiten.[16]

Im 19. Jahrhundert begannen Ärzte, Kriminalisten und Psychiater mit der systematischen Erfassung von biometrischen Merkmalen. Am Anfang ging es vor allem darum, herauszufinden, was man am menschlichen Körper überhaupt vermessen konnte und ob diese körperlichen Merkmale wirklich einzigartig waren. Ebenso oft war der Hauptzweck, Verbindungen von körperlichen Merkmalen mit Charakereigenschaften und Veranlagungen (z. B. zu Krankheiten oder Kriminalität) herzustellen. Heute betrachtet man solche Verbindungen als problematisch, nicht zuletzt wegen den Geschehnissen im Dritten Reich, wo die Rassenzugehörigkeit aus biometrischen Merkmalen (v.a. im Gesicht) gelesen wurde.

Um die Identität einer Person zu *überprüfen*, wurden zu Beginn vor allem Fingerabdrücke verwendet. Jedoch war vor dem Zeitalter der Digitalisierung ein Abgleich mit einer grossen Datenbank nahezu unmöglich. Man verwendete Fingerabdrücke hauptsächlich dazu, zu prüfen, ob er zu einem bestimmten Verdächtigen gehörte oder nicht (die sogenannte Verifikation). Mit dem Fortschritt der Computertechnologie wurde auch die Identifikation (das Suchen einer passenden Person in einer Datenbank) möglich. Es wurden schliesslich weitere Verfahren entwickelt zur Blutuntersuchung, Haaranalyse etc., was den heutigen Forensikern ein breites Spektrum an Methoden bietet [21]. Diese werden wöchentlich in der US-amerikanischen Fernsehserie *CSI* eindrücklich vorgeführt. Auch in der öffentlichen Berichterstattung über die Polizeiarbeit nimmt man diese Methoden immer bewusster wahr. Im Fall Ylenia im Sommer 2007 wurde von der Polizei mehrfach auf DNA-Tests verwiesen.

Trotz dieser recht langen Entwicklungsgeschichte sind biometrische Systeme in ständiger Entwicklung. So gibt es für einige Systeme noch keine brauchbare Umsetzung, andere befinden sich noch in der Probephase. Ein solches Projekt, das eher in die Zukunft weist, ist die Verbindung von Kameras mit Gesichtserkennungssystemen. In Deutschland laufen schon verschiedene Versuche, u.a. am Mainzer Bahnhof. Ziel dieser Systeme ist es, gesuchte Verbrecher und Terroristen aus der Masse der Passanten herauszufiltern. Doch das Missbrauchs- und Überwachungspotential dabei ist extrem hoch. Ausserdem ist das Erkennungspotential im Moment noch nicht gross genug für eine wirkungsvolle Umsetzung.

5.3.2 Grundlagen der Biometrie

Gewisse Gebäude, Geräte und Dienste dürfen nur von bestimmten Personen verwendet werden. Zum Beispiel darf ein e-Banking Konto ausschliesslich vom Inhaber benutzt werden und ein Virenlabor ausschliesslich von Mitarbeitern betreten werden. Traditionell wird die Identität mithilfe eines Geheimnisses (PIN oder Passwort) und/oder eines Tokens (z. B. einer Karte oder eines Schlüssels) überprüft. Neben dem (geheimen) Wissen kann so

auch der (persönliche) Besitz oder aber das Können (z. B. durch die Unterschrift) geprüft werden [5].

Wollen wir einen Geldautomaten verwenden, so wissen wir genau, dass wir erst eine Karte verwenden müssen und danach den passenden PIN eintippen sollen. Auf diese Weise wird sichergestellt, dass die Dienstleistung (bzw. der Zugang zum Gebäude oder Gerät) nur demjenigen freigegeben wird, der in Besitz des Tokens *und* des Geheimnisses ist. Dies ist heute zu einer solchen Selbstverständlichkeit geworden, dass wir uns schon eine ganze Reihe Passwörter und PIN merken müssen. Da man sich so viele verschiedene Passwörter und Zahlenkombinationen nicht alle merken *kann*, schreibt man sie auf, verwendet mehrmals dieselben oder so einfache, dass sie leicht zu erraten sind. Ausserdem gibt es bei vielen Passwortkontrollen die Funktion „Passwort vergessen“. Wenn dort die Antwort auf eine Frage verlangt wird oder ein brauchbarer Hinweis auf das Passwort gegeben wird, lässt sich das Passwort leicht umgehen.

Man kann Passwörter natürlich auch ausspionieren, zum Beispiel mittels einer Kamera an einem Geldautomaten. Tokens erhöhen die Sicherheit nur bedingt, da auch sie gestohlen werden können. Dasselbe gilt für das Können, das mehr oder minder gut kopiert werden kann. Durch biometrische Überprüfung kann nachgewiesen werden, dass es sich *wirklich* um den Eigentümer handelt, denn biometrische Eigenschaften sind nicht stehl- und nur bedingt kopierbar.

Ein biometrisches System kann eine Verifikation durchführen oder eine Identifikation. Bei der *Verifikation* wird geprüft, ob jemand derjenige ist, den er behauptet zu sein. Der Benutzer wird mittels einer Karte, eines Codes o.ä. ermittelt und mit Hilfe des biometrischen Merkmales wird festgestellt, ob er auch tatsächlich diese Person ist. Es wird also ein 1:1 Vergleich durchgeführt. Bei diesem System bietet sich der Vorteil der dezentralen Speicherung, bei dem beispielsweise das biometrische Merkmal auf einer Chipkarte gespeichert wird, die der Besitzer vorweisen muss. Bei der *Identifikation* wird geprüft, ob jemand im System existiert, der genau das gemessene biometrische Merkmal besitzt. Es ist also ein 1:n Vergleich. Dieses Verfahren erfordert mehr Aufwand. Ausserdem müssen die biometrischen Daten zentral gespeichert werden, da immer alle zur Verfügung stehen müssen. Dafür bietet es den Benutzern mehr Bequemlichkeit.

Es gibt verschiedenste biometrische Merkmale, die für eine Authentifizierung verwendet werden können. Man unterscheidet zwischen aktiven, die eine Mitarbeit des Geprüften erfordern, und passiven, die ohne Zutun des Menschen „gelesen“ werden können. Zu den aktiven Merkmalen zählen unter anderem [16]:

- Unterschriftendynamik
- Lippenbewegung
- Stimmerkennung
- Bewegung
- Tastaturanschlag
- DNS

Zu den passiven Merkmalen zählen:

- Irismuster
- Fingerabdruck
- Gesichtserkennung
- Retinamuster
- Thermogramm
- Handgeometrie
- Form des Ohres
- Geruch

Ein Fingerscan System ist nicht immer geeignet, da es sehr anfällig ist für Schmutz (Finger werden rasch dreckig) und manche Anwender bei seltener Benutzung vergessen, welchen Finger sie einlesen sollten [18]. Ausserdem ist ein Fingerprintsensor nicht berührungslos, was bei einigen Benutzern hygienische Bedenken auslösen kann. Dafür ist die Bedienung einfach und die Erfahrungen mit diesem biometrischen Merkmal am grössten.

Ein anderes recht verbreitetes System ist die Gesichtserkennung. In gewissem Sinne wird sie schon seit Jahren verwendet, da viele Ausweise mit Fotos versehen sind. Bei einer Ausweiskontrolle, z. B. beim Kauf von Alkohol, wird der Vergleich jedoch vom Menschen vollzogen, nicht maschinell. Genau diese menschliche Fähigkeit, Gesichter auf einen Blick zuzuordnen, ist ein Vorteil dieses Systems. Im Notfall (z. B. einem Computerabsturz) kann der digitale Vergleich von einem Menschen vorgenommen werden. Die Gesichtserkennung bietet weiter den Vorteil, dass sie berührungslos (d. h. hygienisch) ist. Der Nachteil ist, dass die Lichtbedingungen und der Winkel für eine Aufnahme stimmen müssen. Und dass die Gesichter sich heute noch nicht so gut maschinell unterscheiden lassen; meistens wird die Gesichtserkennung daher nur für die Verifikation verwendet.

Ein weiteres häufiges Verfahren ist die Spracherkennung. Dazu darf die Umgebung nicht zu laut sein. Die Stimme ist zudem eines der wenigen Dinge, die sich ändern kann, zum Beispiel durch Altern oder durch eine Erkältung. Der Vorteil ist allerdings, dass die Technik dazu schon existiert; man kann für die Aufnahme gewöhnliche Mikrofone verwenden. Im Film *Mission Impossible II* überlistet Ethan Hunt ein solches System mittels einer Tonbandaufzeichnung. In der Realität versucht man dies zu vermeiden, indem die betroffene Person mehrere Codewörter aufnehmen muss. Bei einer Kontrolle wird dann per Zufall eines davon ausgewählt und angezeigt. So müsste ein Unbefugter, der sich Eintritt verschaffen will, mehrere Aufzeichnungen haben [16].

Eine andere Möglichkeit ist die Iriserkennung. Dieses System wird in letzter Zeit billiger - und damit auch beliebter. Heute sind sogar Brillen und Kontaktlinsen keine Hindernisse mehr [19]. Es gibt noch viele andere biometrische Merkmale, die verwendet werden können. Jedes dieser Systeme hat Vor- und Nachteile, die bei einer Verwendung berücksichtigt werden sollten. In Dan Browns Thriller *Illuminati* schneidet ein Mörder seinem

Opfer ein Auge heraus, um damit einen Retina-Scanner zu täuschen. Um so einem Szenario vorzubeugen, wird bei den meisten Systemen gleichzeitig mit der Überprüfung des biometrischen Merkmals eine *Lebenderkennung* vorgenommen. Es wird geprüft, ob auch wirklich eine lebende Person vor dem Apparat steht und ob das biologische Merkmal zu ihr gehört. Bei Fingerabdrucklesern beispielsweise wird die Temperatur oder der Puls gemessen, damit man das System nicht mit abgeschnittenen Fingern oder Gummiattrappen überlisten kann [10].

Eine weitere Sicherheitsüberlegung ist, dass jemand, der zutrittsberechtigt ist, eine andere Person mit in das Gebäude nehmen könnte. Das wird oft verhindert durch die Vereinzelung. Beim Eingang eines Gebäudes steht beispielsweise ein Drehkreuz, durch das nur eine Person gleichzeitig gehen kann. Auf diese Weise wird die Möglichkeit ausgeschlossen, dass jemand ohne Kontrolle hineinkann, indem ihn jemand (freiwillig oder nicht) „mitnimmt“. Dadurch wird auch das Risiko minimiert, dass jemand gezwungen wird, jemand anderes mitzunehmen. Vor allem wenn verschiedene biometrische Systeme kombiniert werden, kann dies fast ausgeschlossen werden.

Zwei Messungen eines biometrischen Merkmales sind nie ganz gleich, daher wird nur auf hinreichende Ähnlichkeit geprüft, nicht auf Gleichheit. Der Toleranzbereich, der festlegt, was noch als gleich gilt und was nicht, muss eingestellt werden. Ist er eng, werden oftmals Personen abgewiesen, die eigentlich zugangsberechtigt wären; ist er weit, werden auch Personen zugelassen, die eigentlich nicht zugangsberechtigt wären. Das eine System ist sicherer, das andere komfortabler. Die falschen Abweisungen (false non-match) und die falschen Erkennungen (false match) kann man statistisch messen. Diese Messungen geben die false rejection rate FRR und die false acceptance rate FAR, die beide von einander abhängen. Das Problem daran ist, dass diese Messungen aufwändig sind, da sie erst bei vielen Anwendern aussagekräftig sind. Die Resultate hängen von vielen Faktoren ab, unter anderem der Toleranzschwelle, der verwendeten Datenbank oder der Anzahl der Testmuster. Auch gibt es für diese Tests keine Normierung oder sogar staatliche Zertifizierung [10].

Der biometrische Vergleich wird selten mit den Rohdaten ausgeführt. Stattdessen werden nach verschiedenen Algorithmen *Templates* erstellt, die verglichen werden. Aus ihnen lassen sich die Rohdaten nicht mehr rekonsturieren. Jedoch ist es schwer, dafür zu sorgen, dass gleiche Rohdaten zu gleichen Templates und verschiedene Rohdaten zu verschiedenen Templates führen [21]. Werden in der Datenbank nur die Templates gespeichert, hat das mehrere Vorteile: man benötigt weniger Speicherplatz, weniger Zeit, da man das Template nicht jedes Mal neu erstellen muss, und vor allem werden keine sensiblen Daten gespeichert, da die Rohdaten vernichtet werden können. Ein Nachteil ist allerdings, dass die Rohdaten dann nicht für einen manuellen Vergleich zur Verfügung stehen, falls das System ausfällt. Wenn der Algorithmus gewechselt wird, muss man die Rohdaten neu enrollen und die Templates neu erstellen [21].

5.3.3 Ein biometrisches Projekt

Bevor ein biometrisches System eingesetzt wird, sollte überlegt werden, ob es verhältnismässig ist oder ob ein anderes System denselben Zweck erfüllen könnte. Nur die technische

Machbarkeit und der kostengünstige Preis reichen als Argumente nicht aus [5]. Angenommen eine Firma hat sich entschlossen als Zugangssicherung ein biometrisches System einsetzen. Der Ablauf eines solchen Projektes kann dann in drei Abschnitten geschehen [18]:

1. Zuerst sollte geprüft werden, welches System am geeignetsten ist. Dazu müssen folgende Fragen berücksichtigt werden:

   - Ist es draussen oder drinnen?
   - Kann es nass werden? Gibt es grosse Temperaturschwankungen?
   - Kann es schmutzig werden?
   - Benutzen es viele Personen oder nur eine Handvoll? Erwachsene oder Kinder?
   - Soll das System vor allem komfortabel, schnell oder sicher sein?
   - Soll nur ein biometrisches Merkmal verwendet werden oder mehrere?
   - Ist das primäre Ziel hohe Sicherheit oder Bequemlichkeit für den Benutzer?

   Ebenso spielt eine Rolle, wie teuer das System sein darf und wieviel Zeit in den Unterhalt investiert werden kann. Bei all diesen Fragen kann der Datenschutzbeauftragte mit seiner Erfahrung als Berater dienen.

2. Dann sollte zuerst ein Pilotprojekt (z. B. in nur einer Abteilung) gestartet werden. Dabei lässt sich prüfen, ob das System bei den Anwendern auf Akzeptanz stösst oder auf Ablehnung, wie gut es für den vorgesehenen Zweck geeignet ist und ob es funktioniert. Datenschutz kann bei Bedenken der Endbenutzer eine Rolle spielen, doch ebenso hygienische Vorbehalte oder die Angst vor einer Überwachung durch den Arbeitgeber. Es ist empfehlenswert, wenn spätestens in dieser Phase der Datenschutzbeauftragte beigezogen wird.

3. Wenn das System installiert ist (als Pilotprojekt oder als Festinstallation), kommt eine Verteilsoftware zum Einsatz. Es regelt die Verwaltung und Speicherung der Datensätze. Eine mögliche Verteilsoftware und was das Programm genau leistet, soll im nächsten Kapitel beschrieben werden.

5.3.4 BioLANCC

BioLANCC ist ein Programm, dass schon fast fertig ist. Es administriert, verwaltet und organisiert biometrische Systeme. Dabei wird der biometrische Vergleich des Referenztemplates mit dem zu prüfenden Template nicht von diesem Programm vorgenommen, sondern in den Sensorgeräten. BioLANCC ist für die Verteilung der biometrischen Daten zuständig. Das Programm arbeitet vorwiegend mit „self-contained“ Geräten, die die biometrischen Vergleiche vornehmen.

Wie man in der Grafik 5.1 sieht, wird das Programm von einem oder mehreren Administrator(en) gesteuert. Die Administratoren weisen die Templates auf die verschiedenen biometrischen Sensoren zu, indem sie festlegen, welcher Angestellte welche Zugänge benutzen darf. BioLANCC ist die Schnittstelle zwischen dem zentralen Speicher, wo sämtliche

Abbildung 5.1: Funktionsweise von BioLANCC

Referenztemplates in einer Datenbank angelegt sind, und den Sensoren, die den Vergleich vornehmen.

Ob Verifikationen oder Identifikationen durchgeführt werden, hängt vom Sensorgerät ab. Ebenso, um welche Art von biometrischen Daten es sich handelt. Das Programm unterscheidet nicht zwischen Iris-Scan oder Fingerabdruck oder einem anderen biometrischen System. Es kann auch mehrere parallel installierte Systeme gleichzeitig verwalten.

Das Programm verwaltet die Templates. Es speichert sie zentral und schickt sie an die Geräte, wo sie gebraucht werden. Wenn eine Person versetzt wird, werden die Daten entsprechend umsortiert. Wird jemand neu eingestellt oder verlässt die Firma, dann kann man die Daten zentral und einfach hinzufügen bzw. löschen. Dies funktioniert auch, wenn die Firma mehrere Standorte hat, und sogar, wenn diese sich in verschiedenen Ländern oder Kontinenten befinden. Das System kann auch andere administrative Funktionen vornehmen: so kann es festlegen, zu welchen Zeiten jemand ein Gebäude betreten darf und zu welchen Zeiten nicht.

Gesteuert wird das Programm von einem Administrator, der verantwortlich dafür ist, dass die Daten nicht unrechtmässig verändert oder gelöscht werden. Ein Administrator ist im Prinzip jeder, der Zugriff zu dem Programm hat. Jedoch können für einen Benutzer Berechtigungen eingeschränkt sein, so dass er oder sie nur gewisse Funktionen im Programm ausführen darf.

5.4 BioLANCC und Datenschutz

5.4.1 Analyse

Solange sich das Programm noch in der (wissenschaftlichen) Erprobung befindet, sollte es mit dem Gesetz keine Probleme geben. Doch sobald eine ökonomische Nutzung in Betracht gezogen wird, muss man sich mit dieser Problematik auseinandersetzen. Es gilt allerdings zu Bedenken, dass das Datenschutzgesetz sowie die Verordnung zum Datenschutzgesetz technisch unpräzise formuliert und in einer Rechtssprache verfasst sind. Die technische

Umsetzung der Forderungen ist nicht ganz einfach, da keine exakten Standards vorhanden sind. In Art. 7 DSG heisst es: „Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.“ Das Wort *angemessen* lässt viel Interpretationsspielraum. Daher wird von den Datenschützern jeder Fall einzeln beurteilt und untersucht. Dabei geht es vor allem darum, ob die gesammelten (auch biometrischen) Daten verhältnismässig sind, ob sie für den jeweiligen Zweck geeignet sind und ob die Daten alle erforderlich sind.

Wenn man mit den Datenschutzgesetzen keine Probleme haben möchte, wäre eine einfache Lösung, keine Datenbank zu haben, d. h. die Daten nicht zentral zu speichern. Wenn jeder Zugangsberechtigte einen Chip erhält, auf dem sein Template gespeichert ist, dann ist eine zentrale Speicherung hinfällig. Der Benutzer müsste dann nur seine Karte vorweisen und das eingelesene biometrische Merkmal wird mit dem Referenztemplate auf dem Chip verglichen. Eine solche Karte kann aber gestohlen werden, v.a. wenn sie der Eigentümer nicht immer auf sich trägt. Hat man eine Karte gestohlen, muss das biometrische Merkmal repliziert werden, was aber nicht einfach ist. Eine solche Authentifizierungsprozedur ist nicht bei jeder Tür machbar. Bei Reinräumen oder Operationssälen können die Zugangsberechtigten nicht mit einer Karte hantieren, da dies die vorangegangene Desinfektion zunichte machen würde.[11]

Bei einer solchen Anwendung würde natürlich auch die Funktion von BioLANCC anders aussehen. Da es keinen zentralen Speicher mehr gibt, fällt die Aufgabe der Verteilung der Templates weg. Das Programm übernimmt dann die Konfigurationen der Geräte und verteilt Berechtigungen (also die Zutrittsrechte zu bestimmten Türen). Statt der Templates verteilt das Programm die Namen und/oder eine Personalnummer. Diese sollten ebenfalls auf der SmartCard gespeichert sein. Dann wird zuerst festgestellt, um welche Person es sich handelt und ob diese Zugang zur Türe hat und dann der biometrische Vergleich durchgeführt. Ausserdem erhält das Programm Fehlermeldungen, wenn z. B. ein Sensor ausfällt. Das Programm führt ein Fehlerprotokoll und bei einem Geräteausfall wird der Administrator sofort informiert.

Für den Anwender ist das Handhaben einer Karte möglicherweise zu kompliziert und aufwändig - vor allem wenn Bequemlichkeit wichtiger ist als Sicherheit. Doch wenn man sich für eine Datenbank entscheidet, gilt es einige Punkte zu beachten:

Datensammlungen, die von einer Firma zur Zugangsberechtigung genutzt werden, sind nicht privat und fallen somit unter die Bestimmungen des Datenschutzgesetzes. Da neben den biometrischen Daten auch die Namen (und möglicherweise eine Funktion im Betrieb) gespeichert wird, ist auch immer auf die Person schliessbar. Eine Speicherung, die nur auf einer Nummer und dem biometrischen Merkmal beruht, wäre keine prekäre Datensammlung, doch dieses System ist im Alltag nicht praktikabel. Von einigen biometrischen Daten lässt sich auf die ethnische Herkunft oder den Gesundheitszustand schliessen[17][11], was sie „besonders schützenswert“ werden lässt. Wenn anstatt der biometrischen Rohdaten nur die Templates gespeichert werden, kann das die Sensibiltät der Daten senken.

Im privatrechtlichen Bereich kann man im Prinzip sammeln, was man will, solange man dafür einen Rechtfertigungsgrund anführen kann. Ein Rechtfertigungsgrund ist die Einwilligung der registrierten Personen. Sie müssen also auf jeden Fall Bescheid wissen und

ihre Zustimmung zur biometrischen Zutrittskontrolle geben. Am einfachsten wird dies gewährleistet, wenn man ein aktives biometrisches Merkmal verwendet. Dieses kann nicht gelesen werden, ohne dass der Betroffene es bemerkt. Dies kann nicht nur die Zustimmung jeden Tag aufs Neue bestätigen, sondern den Registrierten auch ein Gefühl von Sicherheit geben, da sie sich nicht überwacht oder sogar verfolgt fühlen.

Ist die Zustimmung der Betroffenen nicht vorhanden, sind die Daten in der Regel nicht rechtmässig beschafft worden, was gegen das DSG verstösst. Das Einlesen der Angestellten sollte an einer zentralen Station (bspw. im Sekretariat der Firma) geschehen, wobei die Angestellten über den Zweck und die Funktionsweise aufgeklärt werden müssen. Einige Menschen können Bedenken gegenüber einem biometrischen System haben, seien es datenschutzrechtliche oder hygienische oder sonstige. Es kann auch passieren, dass sich ein Merkmal nicht einlesen lässt oder dass die Personen Schwierigkeiten haben, das Merkmal zu erfassen (z. B. Rollstuhlgänger, für die die Sensoren zu hoch sind).[5] In diesen Fällen sollte eine Alternative prinzipiell möglich sein (z. B. in Form einer Magnetkarte oder eines Passwortes). Ansonsten verstösst der Anbieter gegen das Diskriminierungsverbot und die Rechtsgleichheit.[5]

Daten dürfen nicht länger als nötig gespeichert werden. Bei BioLANCC besteht die Funktion „löschen“. Wenn jemand die Firma verlässt, werden die Daten vom Administrator gelöscht. Wird eine Person wieder eingestellt, muss sie neu eingelesen werden. Dies gewährleistet, dass keine Daten mehr gespeichert werden, die nicht auch gebraucht werden.

Daten einer Datensammlung müssen gegen Verlust, unbefugte Löschung und Vernichtung geschützt sein. Geschieht ein Notfall (z. B. ein Feuer oder ein Systemabsturz), der die Daten vernichtet, können sie entweder neu enrollt werden oder mit einem Backup wieder hergestellt werden. Das Backup sollte allerdings verschlüsselt gespeichert werden.

Ein weiteres grosses Sicherheitsproblem ist die Kommunikation zwischen den Geräten und dem zentralen Speicher. Wenn man diese Kommunikation abhören kann, kann man Daten ändern, stehlen, oder kopieren. Diese Kommunikation sollte verschlüsselt werden. Nicht alle Geräte unterstützen eine Verschlüsselung von sich aus, doch durch ein Zwischengerät könnte eine SSL-Verschlüsselung verwendet werden. Dies würde auch eine Einspielung (Fälschung) von Daten verhindern.[22]

Das nächste Sicherheitsproblem ist, dass die Templates mindestens zweimal abgespeichert sind: im zentralen Speicher und im Sensorgerät. So kann die Anzahl der vorhandenen Templates einer Person ziemlich gross werden, wenn jemand bei allen Türen zugangsberechtigt ist. Ausserdem liesse sich so ein Sensor abmontieren und ein anderer installieren, der die Templates des/der Betrüger enthält. Der Vorteil bei dezentral abgespeicherten Templates ist, dass das System auch bei einem Netzausfall funktioniert. So kann niemand aufgrund eines nicht mehr funktionierenden Netzes ein- oder ausgesperrt werden. Allerdings liesse sich dieses Problem auch so lösen, dass z.B. bei einem Netzausfall alle Türen gegen aussen offen sind, gegen innen jedoch nicht.

Das letzte Problem stellt der Zugriff auf die Datenbank dar. Vor unbefugtem Zugriff müssen Daten geschützt werden. Ausserdem sollten die Daten in der Datenbank verschlüsselt gespeichert werden, damit sie nicht leserlich sind, wenn jemand sie aus der Datenbank stiehlt. Die Möglichkeit, die Daten auf einem Server zu speichern, empfiehlt sich v.a.

dann, wenn die Firma schon eine Datenbank ihrer Angestellten hat. Der Zugriff auf den Server müsste natürlich verschlüsselt und mit Kennwort und Passwort geschützt sein. Auf diese Daten sollte nur ein sogenannter Superadministrator Zugriff haben.

Eine weitere Frage, die zu klären ist, ist die Übergabe von Daten ins Ausland. Wenn eine Firma mehrere Standorte in ganz Europa hat und mit BioLANCC ihre biometrischen Datensätze steuern will, dann werden diese Daten über den ganzen Kontinent verteilt. Zwar werden sie möglicherweise zentral verwaltet, doch da die Daten *lokal* bei jedem biometrischen Gerät vorhanden sein müssen, werden sie ins Ausland gesendet. Dies erfordert möglicherweise eine Registrierung beim Datenschutzbeauftragten - vor allem dann, wenn das Partnerland keine vergleichbare Datenschutzgesetzgebung hat.

5.4.2 Empfehlungen

Auf Grund der Analysen sollen nun einige Punkte beschrieben werden, die beim Einsatz von BioLANCC besonders beachtet werden sollten.

1. Bei der Entscheidung für ein biometrisches System sollte die Möglichkeit geprüft werden, die Referenztemplates auf SmartCards zu speichern und den Anwendern zu überlassen. Dazu braucht es Sensoren, die diese Karten lesen können und ein Umfeld, das diese Anwendung unterstützt. Aus datenschutzrechtlicher Sicht wäre diese Alternative aber sinnvoll. Der Einsatz von BioLANCC würde sich dann so gestalten: So könnte das Programm festlegen, wer welche Tür benutzen darf, jedoch nicht mehr mit der Versendung des Templates sonder mit der Versendung des Namens, einer Personalnummer oder ähnlichem. Ausserdem würde das Programm die Konfigurierung der Sensoren vornehmen und auf Fehlermeldungen reagieren.

2. Es ist wichtig, dass die Einwilligung der erfassten Personen vorhanden ist. Eine zentrale Enrollmentstation mit einem ausführlichen Gespräch über Einsatz, Verwendung und Schutz der Daten wäre sinnvoll. Es wäre auch gut, das System so einzurichten, dass diese Einwilligung jeden Tag von Neuem gegeben wird, indem man ein aktives biometrisches Merkmal verwendet. Falls die Personen nach dem einführenden Gespräch nicht weiter bereit sind, ihr biometrisches Merkmal zu Zugangszwecken zur Verfügung zu stellen, sollte eine Alternative angeboten werden.

3. Der Administrator ist eine wichtige Person und sollte sorgfältig ausgewählt werden. Er ist der einzige, der Zugriff zu allen Daten hat. Er ist dafür verantwortlich, dass sie richtig verteilt und nach ihrem Gebrauch gelöscht werden. Sein Zugriff zum Programm muss mit einem Passwort geschützt sein.

4. Gegen Verlust, Löschung und Vernichtung kann man die Daten durch ein Backup schützen. Dieses sollte wenn möglich verschlüsselt gespeichert werden.

5. Die Kommunikation zwischen den Sensoren und dem Programm sollte verschlüsselt sein. Dies würde sowohl das Auslesen als auch das Einspielen von Daten verhindern.

6. Auch die Templates sollten in der Datenbank nur verschlüsselt gespeichert werden, um einen Zugriff zu erschweren.

7. Es sollte überlegt werden, ob eine doppelte Speicherung der Daten in der Datenbank und im Zentralspeicher wirklich nötig ist oder ob sie sich umgehen liesse.

5.5 Zusammenfassung

Datenschutzgesetze sollen dafür sorgen, dass jeder selbst entscheiden kann, wer welche Daten von ihm sammeln und bearbeiten darf. Damit soll eine Überwachungsgesellschaft schon im Keim verhindert werden. Die Bestimmungen der EU-Richtlinie sowie des schweizerischen Datenschutzgesetzes unterscheiden sich nur in Details.

Hauptsächlich müssen Daten, die in einer Datenbank verarbeitet werden, einerseits speziell geschützt werden vor Verlust, Vernichtung und Löschung, andererseits vor unberechtigtem Zugreifen, Ändern, Fälschen oder Kopieren. Diese ungenauen rechtlichen Bestimmungen sind bei der praktischen Programmierung eine grosse Herausforderung.

Biometrische Systeme beinhalten sensible Daten, weil von einigen biometrischen Daten Rückschlüsse auf die ethnische Zugehörigkeit, den Gesundheitszustand oder Drogenkonsum gezogen werden können. Ausserdem ändern sich biometrische Daten nie und das macht sie besonders gefährlich, wenn sie in kriminelle Hände geraten.

BioLANCC ist ein Verwaltungsprogramm für biometrische Zutrittssysteme. Das Programm ist die Schnittstelle zwischen dem Zentralspeicher, wo die Datenbank angelegt ist, und den Sensoren, in denen der Vergleich der Templates vorgenommen wird. BioLANCC regelt die Verteilung der Templates auf die Sensoren und die verschiedenen Zutrittsrechte, es erhält Fehlermeldungen und konfiguriert die Geräte.

Da das Programm die biometrischen Daten in einer Datenbank speichert, kann es zu Konflikten mit dem Datenschutzgesetz kommen. Auf jeden Fall ist die Zustimmung der Registrierten *unbedingt* nötig! Weigert sich jemand, seine Zustimmung zu geben, sollte über eine Alternative diskutiert werden.

Um die Daten gegen Verlust, unbefugte Löschung und Vernichtung zu sichern, kann man ein Backup anlegen, mit dem die Daten wiederhergestellt werden können. Zur Sicherheit sollte das Backup verschlüsselt gespeichert werden. Ebenfalls verschlüsseln sollte man die Daten in der Datenbank (v.a. die Templates) und die Kommunikationswege zwischen den Sensoren zu BioLANCC und zum Speicher. Diese beiden Massnahmen können das Risiko für unbefugten Zugriff und unbefugtes Lesen oder Ändern minimieren.

Ein Punkt, der dringend geprüft werden sollte, ist die doppelte Abspeicherung. Sie bietet die doppelte Angriffsfläche für einen kriminellen Angriff. Man sollte überlegen, ob es möglich ist, dass die Sensoren nur dann auf die Templates zugreifen könnten, wenn sie einen Vergleich vornehmen müssen. Dies liesse sich am einfachsten mit einer Verifizierung (d. h. einem 1:1 Vergleich) umsetzen. Eine andere Möglichkeit, viele datenschützerische Probleme zu umegehen, wäre die dezentrale Speicherung auf Chipkarten, die jeder Benutzer bei sich trägt.

Literaturverzeichnis

[1] Bundesgesetz über den Datenschutz; `http://www.admin.ch/ch/d/sr/2/235.1.de.pdf` , Oktober 2007.

[2] Verordnung zum Bundesgesetz über den Datenschutz; `http://www.admin.ch/ch/d/sr/2/235.11.de.pdf` , Oktober 2007.

[3] Richtlinie 95/46/EG; `http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_de.pdf` , Oktober 2007.

[4] Richtlinie 95/46/EG Fortsetzung; `http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part2_de.pdf` , Oktober 2007.

[5] Die Schweizerischen Datenschutzbeauftragten: *Leitfaden zur datenschutzrechtlichen Beurteilung von biometrischen Verfahren: Mit Checkliste für Projekte im öffentlich-rechtlichen Bereich*; Version 1.0, privatim, o.O., 2006.

[6] Urs Maurer, Nadine Faruque: *SRE Schweizerische Rechtserlasse: Datenschutz*; Helbig und Lichtenhahn, Basel und Frankfurt a. M., 1994.

[7] Ulrich Damman, Spiros Simitis : *EG-Datenschutzrichtlinie: Kommentar*; Namos Verlagsgesellschaft, Baden-Baden, 1997.

[8] James Thomas Peter: *Das Datenschutzgesetz im Privatbereich: Unter besonderer Berücksichtigung seiner motivationalen Grundlage*; (Zürcher Studien zum Privatrecht Vol. 115), Schulthess Polygraphischer Verlag, Zürich, 1994.

[9] Rainer Knyrim: *Datenschutzrecht: Leitfaden für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmen, Outsourcen, Werben uvm.*; MANZ-Verlag, Wien, 2003.

[10] Astrid Albrecht, Thomas Probst: *Bedeutung der politischen und rechtlichen Rahmenbedingungen für biometrische Identifikationssysteme*; in: Michael Behrens, Richard Roth (Hg.): *Biometrische Identifikation: Grundlagen, Verfahren Perspektiven*; Friedr. Vieweg und Sohn, Braunschweig, Wiesbaden, 2001. S. 27-54.

[11] Thomas Probst: *Biometrie aus datenschutzrechtlicher Sicht*; in: Veronika Nolde, Lothar Leger (Hg.): *Biometrische Verfahren: Körpermerkmale als Passwort: Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation*; Fachverlag Deutscher Wirtschaftsdienst, Köln, 2002. S. 115-128.

[12] *EU und USA schließen Abkommen über Weitergabe von Fluggastdaten*; Europäische Kommission; `http://ec.europa.eu/news/justice/061013_1_de.htm`.

[13] Gerhard Maurer, Henning Scheu: *Computer können nicht vergessen: Informationen zum Bundes-Datenschutzgesetz*; Europäische Verlagsanstalt, Köln, Frankfurt a. M., 1978.

[14] Helmut Reimer: *Biometrische Identifikation: Eine aussichtsreiche Innovation*; in: Michael Behrens, Richard Roth (Hg.): *Biometrische Identifikation: Grundlagen, Verfahren Perspektiven*; Friedr. Vieweg und Sohn, Braunschweig, Wiesbaden, 2001. S. 1-26.

[15] Andreas Pfitzmann: *Der ePass: Innovativ, aber ein Sicherheitsrisiko*; in: *iX Magazin für professionelle Informationstechnik*; No. 10/2007, Heise Zeitschriften Verlag, Hannover, 2007. S. 48.

[16] Veronika Nolde, Lothar Leger: *Einleitung*; in: Veronika Nolde, Lothar Leger (Hg.): *Biometrische Verfahren: Körpermerkmale als Passwort: Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation*; Fachverlag Deutscher Wirtschaftsdienst, Köln, 2002. S. 15-82.

[17] Walter Eigenstetter: *Grundlagen und Betrachtungen zur biometrischen Authentifizierung, Teil 1*; in: *Wissen Heute*; No. 10/2007, Neuer Kaiser Verlag, Klagenfurt, 2007. S. 4-18.

[18] Barbara Lange: *Vermessen: Systeme zur biometrischen Zutrittskontrolle im Einsatz*; in: *iX Magazin für professionelle Informationstechnik*; No. 10/2007, Heise Zeitschriften Verlag, Hannover, 2007. S. 50-56.

[19] John R. Vacca: *Biometric Technologies and Verification Systems*; Elsevier, Oxford, 2007. S. 1-17.

[20] Jan Krissler, Christiane Rütten: *Feine Linien - Wie leicht sich Fingerabdrucksensoren austricksen lassen*; in: *c't*; No. 12/2007, Heise Zeitschriften Verlag, Hannover, 2007. S. 102-103.

[21] Lotte Meuth: *Zulässigkeit von Identitätsfeststellungen mittels biometrischer Systeme durch öffentliche Stellen*; (Beiträge zum Informationsrecht Vol. 17), Duncker und Humblot, Berlin, 2006.

[22] Veronika Garcia: *Sicherheit für BioLANCC: Design und Implementierung*; Diplomarbeit Universität Zürich, 2007.

[23] futurezone beim ORF; `http://futurezone.orf.at/tipps/stories/153185` , Oktober 2007.

[24] Heise online news; `http://www.heise.de/newsticker/meldung/82845` , Oktober 2007.