Hannes Federrath, Kai Martius: Anonymität und Authentizität im World Wide Web. ITG-Fachbericht 153, Vorträge der ITG-Fachtagung 'Internet - frischer Wind in der Telekommunikation', VDE-Verlag, 1998, 91-101.

Anonymität und Authentizität im World Wide Web

Hannes Federrath[1], TU Dresden, Fakultät Informatik, Institut für Theoretische Informatik,
01062 Dresden, E-Mail: federrath@inf.tu-dresden.de
Kai Martius[2], TU Dresden, Medizinische Fakultät, Institut für Medizinische Informatik und Biometrie,
01062 Dresden, E-Mail: kai@imib.med.tu-dresden.de

Kurzfassung

Wir beschreiben erstens Lösungsmöglichkeiten zur Sicherung der Anonymität und Unbeobachtbarkeit von Internetnutzern beim Surfen im World Wide Web. Der Schutz der Nutzer soll sowohl gegen Angreifer aus dem Internet (Outsider) als auch gegen Angreifer im eigenen lokalen Netz (Insiderangriffe im Intranet) und Kombinationen aus Beiden (Insider und Outsider) wirken. Einfache Proxies bieten diesen Schutz nicht, sie können jedoch um entsprechende Funktionen erweitert werden.
Wir stellen zweitens das Konzept eines dynamischen Firewalls (dynamischer IP-Filter) vor, der Internetverbindungen aufgrund gesicherter Daten (Digitale Signaturen und Zertifikate) durchschaltet. In herkömmlichen Firewalls fallen sicherheitsrelevante Entscheidungen bisher meist anhand von ungesicherten Daten (IP-Adressen und Portnummern), wodurch bestimmte Angriffsmöglichkeiten nicht abgewehrt werden konnten. Diesen Nachteil beseitigt unsere Lösung.

1 Einführung

Die Vernetzung von Computern macht heute nicht mehr Halt an den Grenzen einer Organisation. Vielfach besteht der Wunsch, sich an internationale Netze anzubinden, ohne dadurch das Gefahrenpotential für die Organisation zu erhöhen.
Leider führt die Vernetzung von Computern jedoch zu einer Reihe von Risiken, die mit dem Verlust der Vertraulichkeit, Integrität und Verfügbarkeit einhergehen können. Neben dem unberechtigten Zugriff auf organisationsinterne Informationen kann auch das Einschleusen von Daten von außen Gefahren mit sich bringen. Hacker könnten in Computerspielen und anderen zunächst unverdächtigen externen Daten Computerviren und Trojanische Pferde untergebracht haben, um mit ihrer Hilfe unberechtigt an interne Daten zu gelangen.
Darüber hinaus läßt die Beobachtbarkeit des Nutzerverhaltens auch Rückschlüsse auf die Interessenslage einer Organisation zu (z.B. Zugriff auf bestimmte Webseiten, Patentschriften, elektronisch veröffentlichte Forschungspapiere).
Sicherheit gewinnt auch bei den Nutzern mehr und mehr an Bedeutung. Nach einer Umfrage des Georgia Institute of Technology setzten über 30 % von mehr als 10.000 Befragten den Schutz der Privatsphäre an die erste Stelle der Herausforderungen, die das Internet hervorbringt. Letzten Sommer waren es noch etwa 26 % (Chronicle of Higher Education 30. Januar 1998).

Dieses Papier ist folgendermaßen aufgebaut: In den folgenden Abschnitten 1.1 und 1.2 wird eine Übersicht über Schutzziele gegeben, erst allgemein, dann speziell auf die hier behandelte Problematik bezogen. In Abschnitt 2 wird die Lösung für Anonymität und Unbeobachtbarkeit im World Wide Web beschrieben. Abschnitt 3 stellt die Lösung des dynamischen Firewalls vor. In den Abschnitten 4 und 5 werden zusammenfassende Bemerkungen gemacht, zunächst zur Leistungsfähigkeit der Verfahren und schließlich noch allgemeiner.

1.1 Was soll geschützt werden?

Es gibt inzwischen eine Reihe von Einteilungen für Schutzziele, die gegen einen intelligenten Angreifer durchgesetzt werden sollen [1]. Eine Einteilung ist z.B.:

Schutz der Vertraulichkeit

- der Nachrichteninhalte,
- der Unbeobachtbarkeit von Kommunikationsbeziehungen,
- Ermöglichen von anonymen Kommunikationsformen,
- Schutz von Aufenthaltsorten (insbesondere in mobilen Netzen).

Schutz der Integrität

- der Nachrichteninhalte.

Schutz der Zurechenbarkeit

- des Senders zu einer Nachricht,
- Möglichkeit zum Beweis von Sendung und/oder Empfang von Nachrichten (Quittungen),
- Korrekte und nicht fälschbare Abrechnungen über die Dienstnutzung bzw. -erbringung, sowohl für Betreiber als auch für Nutzer sicher.

Schutz der Verfügbarkeit

- Das Netz soll Kommunikation zwischen allen Partnern ermöglichen, die dies wünschen und denen dies nicht verboten ist.

Mit den in diesem Papier vorgestellten Lösungen wird die folgende Auswahl und konkrete Ausprägung der genannten Schutzziele erreicht:

Schutz der Inhalte von internen Webseiten bei der Übertragung über unsichere Netze

- Schutz der Inhalte durch starke kryptographische Verschlüsselung bei der Übermittlung über das unsichere Internet.

Unbeobachtbarkeit und Anonymität von Webzugriffen

- Verbergen von Interessensdaten, d.h. es wird verborgen, wer welche Internetadressen (URLs) aufruft.

Zugangsschutz zum Intranet aus dem unsicheren Internet

- Dynamische Filterung von IP-Paketen auf der Basis von Zertifikaten und digitalen Signaturen.

1.2 Gegen welche Angreifer wird geschützt?

Aussagen über den erzielten Schutz können nur im Zusammenhang mit der unterstellten Stärke eines Angreifers gemacht werden. Bezogen auf die im vorigen Abschnitt genannten Schutzziele soll daher jeweils ein Angreifermodell angegeben werden. Es gibt die maximal mögliche Stärke des Angreifers an, gegen den der Schutz gerade noch gewährleistet ist.

1.2.1 Schutz der Inhalte von internen Webseiten

Bezogen auf den Schutz der Inhalte soll von einem aktiven Angreifer ausgegangen werden. Er soll in der Lage sein, gefälschte (bzw. unechte) Nachrichten einzuspielen. Die Verbreitung des Angreifers beschränkt sich auf das Internet (Outsider). Ein Insider wird bezüglich des Schutzgutes (Inhalt interner Webseiten) nicht als Angreifer gesehen, da er berechtigten Zugang zu den publizierten Inhalten hat und diese auch verändern können soll. Davon unberührt bleiben natürlich etwaige Sicherungsmaßnahmen, wie z.B. Zugangs- und Zugriffsschutz (Schreibzugriffe, Verändern der Inhalte durch Berechtigte) zum Server. Diese sind jedoch nicht Untersuchungsgegenstand dieses Papiers.
Wir gehen insbesondere davon aus, daß die durch Exportbeschränkungen reduzierte Schlüssellänge (meist 40 Bit) der in den Browsern US-amerikanischer Herkunft fest eingebauten Verschlüsselungsmechanismen zur Sicherung der Vertraulichkeit bei der Übertragung nicht den gestellten Anforderungen genügt.

1.2.2 Schutz vor Beobachtbarkeit

Bezogen auf die Beobachtbarkeit der Webzugriffe wollen wir Schutz vor einem passiven Angreifer bieten. Der Angreifer soll auf allen Leitungen alle Kommunikation abhören können. Verkehrsanalysen sind für ihn möglich. Auch Insider (Nutzer/Beobachter im Intranet) werden als Angreifer betrachtet.
Eine Konsequenz für den Schutz vor Beobachtbarkeit ist, daß bei diesem Angreifermodell die Nutzung von http-Proxies zur Verschleierung von Webanfragen nicht ausreicht (**Bild 1**), da der Angreifer auch im Intranet verbreitet sein soll.

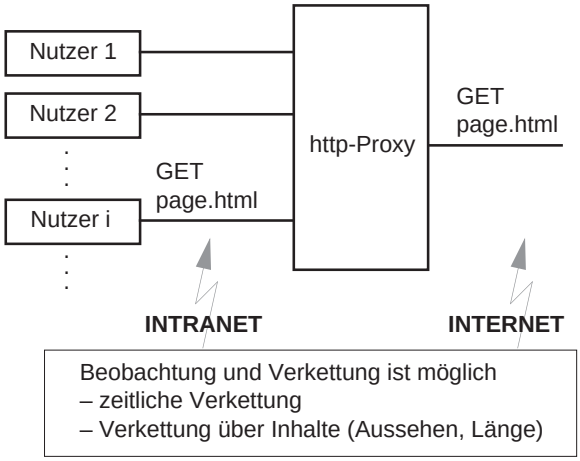


Bild 1. Unterstellte Verbreitung des Angreifers

In Abschnitt 2 werden einige Lösungen aus der Literatur mit ihren Vor- und Nachteilen beschrieben und die Lösung eines Mix-Proxys vorgestellt, die noch gegen den oben genannten Angreifer sicher ist.

1.2.3 Zugangsschutz zum Intranet

In vielen Intranets kommen Firewalls zum Einsatz, um einerseits das Intranet gegen unberechtigte Zugriffe von außen zu schützen und andererseits einen unkontrollierten Informationsfluß von innen nach außen

weitgehend zu verhindern. Bestimmte Angriffsarten (z.B. Fälschen von IP-Adressen, Abfangen und „Einklinken“ in berechtigte Verbindungen) können jedoch selbst mit herkömmlichen Firewalls nur schwer verhindert werden oder gehen, wenn sie verhindert werden, zu Lasten einer flexiblen und effizienten Nutzung der vorhandenen Kommunikationsmöglichkeiten. Gründe hierfür sind:

– Sicherheitsrelevante Entscheidungen fallen an Hand ungesicherter Daten (IP-Adressen und Ports).
– Wenn überhaupt Authentisierungsdienste angeboten werden, sind diese proprietär und basieren meist auf symmetrischen Kryptoverfahren.

Folgendes Szenario soll dies verdeutlichen: Ein (berechtigter) Mitarbeiter im Außendienst, der sich derzeit bei einem Kunden aufhält, möchte Daten aus seinem Firmennetz abrufen. Der Firewall der eigenen Firma erlaubt jedoch keinen expliziten Zugriff aus dem Netz des Kunden. Entweder läßt der Außendienstmitarbeiter jeweils unmittelbar „am Fall“ den Firewall von seinem Administrator freischalten und später wieder sperren, was zwar weitgehend sicher, jedoch sehr umständlich und unflexibel ist, oder der Administrator konfiguriert (aus Bequemlichkeit) seinen Firewall weniger streng (d.h. öffnet das Intranet für weite Teile des Internet) mit der Konsequenz eines erhöhten Angriffspotentials.
In Abschnitt 3 wird als Lösung für den flexiblen und trotzdem streng geregelten Zugang ein Authentisierungsdienst in Kombination mit einem dynamischen IP-Filter vorgestellt.

2 Anonymität und Unbeobachtbarkeit im Web

Je nach Anwendungsfeld lassen sich Schutzziele wie Anonymität und Unbeobachtbarkeit definieren. Sender und/oder Empfänger von Nachrichten sollen voreinander anonym bleiben können, und Unbeteiligte (möglicherweise inklusive des Netzbetreibers) sollen nicht in der Lage sein, sie zu beobachten. Adressierungs- und Routingdaten enthalten jedoch gewöhnlich Information über Sender und Empfänger von Nachrichten sowie über Kommunikationsbeziehungen zwischen den Nutzern.
In der Praxis kann die Unterstützung anonymer Kommunikationsformen erheblich zur Steigerung der Akzeptanz von Informationsangeboten führen: Beispielsweise könnte die Tatsache, daß der Abruf von Beratungsdienstleistungen (z.B. Suchtberatung, Schuldenberatung, medizinische Dienstleistungen) vom heimischen Modem über WWW bisher stets beobachtbar ist (sowohl durch den Betreiber des Servers als auch durch den Betreiber des Transportmediums), das Nutzerverhalten entscheidend prägen. Mit der Bereitstellung wirklich unbeobachtbarer Kommunikationsformen wäre das möglicherweise anders.

2.1 Existierende Lösungen und ihre Grenzen

In der Literatur bzw. im Internet existieren derzeit zumindest drei Ansätze, die den Schutz vor Beobachtung von Webzugriffen gewährleisten sollen:

– Anonymizer (www.anonymizer.com),
– Crowds (www.research.att.com/projects/crowds),
– Onion-Routing (www.onion-router.net).

Obwohl alle drei Ansätze annähernd das gleiche Ziel verfolgen, unterscheiden sie sich insbesondere in ihrem erreichten Schutz gegenüber einem Angreifer. Anders formuliert: Die Angreifermodelle der Verfahren sind unterschiedlich.
Ziel der Verfahren ist, gegenüber dem Server und teilweise auch gegenüber Beobachtern, die Verkehrsanalysen durchführen, zu verbergen, wer welche Webseiten aufruft.
Die oben genannten Verfahren werden im folgenden kurz beschrieben und dann insbesondere im Hinblick auf den erreichten Schutz miteinander verglichen.
In Abschnitt 2.2 wird schließlich eine Lösung beschrieben, die unter einem noch stärkeren Angreifermodell Schutz vor Beobachtung bietet.

2.1.1 Anonymizer

Anonymizer ist ein Proxydienst. Über ein Webinterface (einfacher Aufruf einer Webseite, in die eine URL eingegeben werden muß) kann der Dienst genutzt werden.
Der Nutzer muß dem Betreiber des Anonymizer vertrauen, daß er keine Interessensdaten sammelt. Theoretisch können mehrere Anonymizer hintereinander geschaltet (kaskadiert) werden. Dann weiß nur noch der erste Anonymizer direkt, wer (genauer: welche IP-Adresse) den Dienst nutzt.
Technisch gesehen arbeitet der Anonymizer wie ein herkömmlicher http-Proxy, jedoch mit dem Unterschied, daß der Anonymizer alle potentiell personenbezogenen Informationen (z.B. Cookies) in den Headern der Webanfragen entfernt. Verschlüsselung wird beim Anonymizer nicht verwendet.
Bezüglich eines Angreifers, der alle Kommunikation im Netz abhören kann bzw. Verkehrsanalysen durchführt, ist der Anonymizer nicht sicher. Somit gelten sinngemäß die Aussagen zu http-Proxys aus Abschnitt 1.2.2 und Bild 1 (Verkettbarkeit der Anfragen über das „Aussehen“ der Nachrichten, deren Länge und zeitliche Korrelationen).

2.1.2 Crowds

Crowds „versteckt“ die Webanfragen eines Benutzers in denen der anderen Crowds-Dienstnutzer. Um am Dienst teilzunehmen, meldet sich der Nutzer bei einer zentralen Stelle, dem sog. Blender, an.
Auf dem lokalen Rechner hat jeder am Dienst teilnehmende Nutzer ein Programm installiert, den sog. Jondo. Die Idee von Crowds ist, daß eine Webanfrage nicht direkt an den Server gestellt wird, sondern vorher mehrere Jondos anderer Teilnehmer durchläuft. In jedem Jondo wird eine Anfrage zufällig entweder zu einem weiteren Jondo geschickt oder direkt an den Server.
Ein negativer Aspekt von Crowds ist, daß ein Teilnehmer fälschlicherweise für den Absender einer Anfrage gehalten werden kann. Ein Vorteil ist jedoch, daß ein Teilnehmer stets abstreiten kann, der Initiator einer Anfrage gewesen zu sein.
Ein Angreifer, der die Kommunikationsinhalte unmittelbar mitlesen will, hat bei Crowds im Gegensatz zum Anonymizer keine Möglichkeit, da die Anfragen zwischen den Jondos mit einem symmetrischen[3] Kryptosystem verschlüsselt sind. Eine Verkettung über die (verschlüsselten) Nachrichteninhalte und damit die Beobachtung ist jedoch nach wie vor möglich, wenn der Angreifer Verkehrsanalysen durchführt. Gegen Angriffe über die zeitliche Verkettung von eingehenden Nachrichten eines Jondos und deren Ausgabe wurden keine Schutzmaßnahmen vorgesehen.

2.1.3 Onion-Routing

Die Unbeobachtbarkeitslösung von Onion-Routing beschränkt sich nicht auf Webzugriffe. Sie ist ebenfalls für Filetransfer (ftp), remote login und andere verbindungsorientierte Dienste nutzbar. Sie arbeitet als Proxydienst mit einem sog. Initiator-Proxy auf der Nutzerseite und einem Responder-Proxy auf der dem Internet „zugewandten“ Seite. Zwischen Initiator- und Responder-Proxy sind mehrere Onion-Router geschaltet.
Onion-Routing soll folgendes Schutzziel erfüllen: Ein Angreifer, der alle Kommunikation im Netz abhören kann, soll nicht in der Lage sein, ein- und ausgehende Nachrichten eines Onion-Routers miteinander zu verketten. Dieses Angreifermodell entspricht praktisch dem von David Chaum aus [2]. Die technische Lösung für das Onion-Routing ähnelt in vielen Punkten Chaums Idee der Mixe sehr stark, weshalb hier zunächst kurz das Mix-Verfahren erläutert wird und dann einige Erweiterungen und Modifikationen, aber auch Einschränkungen an die erreichte Sicherheit für das Onion-Routing genannt werden.

2.1.3.1 Chaums Mixe

Die Idee der Mixe wurde in [2] vorgestellt. Das Mix-Konzept kommt in Vermittlungsnetzen zum Einsatz. Ein Mix verbirgt die Kommunikationsbeziehung zwischen Sender und Empfänger einer Nachricht. Hierzu muß ein Mix eingehende Nachrichten speichern, bis genügend viele Nachrichten von genügend vielen Absendern vorhanden sind, ihr Aussehen verändern, d.h. sie umkodieren, und die Reihenfolge der ausgehenden Nachrichten verändern, d.h. sie umsortieren und in einem Schub ausgeben.

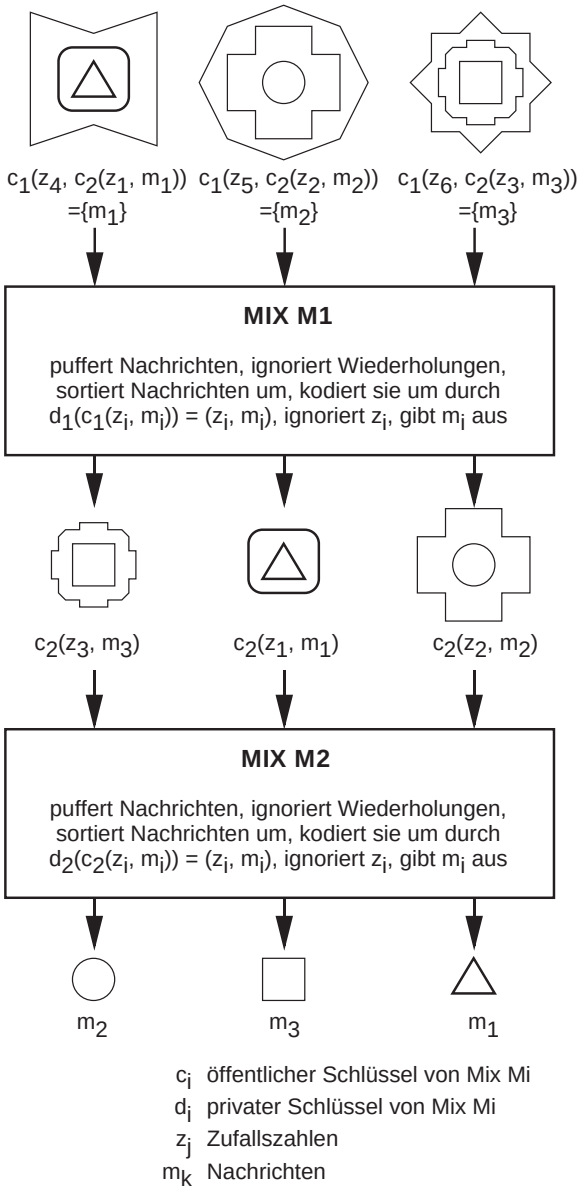


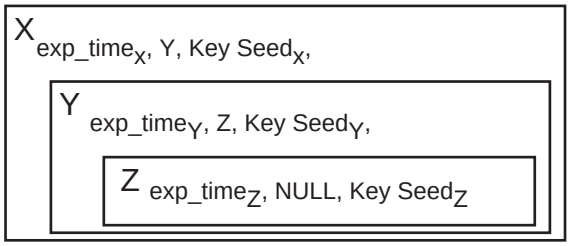
Bild 2. Umkodieren gemixter Nachrichten

Um Angriffe durch Nachrichtenwiederholung zu verhindern, muß zu Beginn noch geprüft werden, ob eine eingehende Nachricht bereits gemixt wurde. Da ein Mix deterministisch arbeitet, würde eine Nachrichten-

wiederholung z.B. in einem nächsten Schub zur Ausgabe der gleichen umkodierten Nachricht führen. Somit wäre eine Verkettung von Ein- und Ausgabe möglich.
Damit keine Verkettung zwischen eingehenden und ausgehenden Nachrichten über deren Länge möglich ist, sollten alle (eingehenden) Nachrichten die gleiche Länge haben, ebenso die ausgehenden.
Eine Nachricht, die einen Mix durchläuft, ist nur innerhalb eines Schubes anonym. Deshalb muß sichergestellt sein, daß ein Angreifer nie alle Nachrichten außer einer kennt, denn das käme der Deanonymisierung gleich. Arbeiten alle anderen Sender und Empfänger der in einem Schub gemixten Nachrichten zusammen, ist die Kommunikationsbeziehung ebenfalls aufgedeckt.
Falls nicht genügend eingehende Nachrichten vorhanden sind, müssen künstliche erzeugt werden, damit die Verzögerungszeit einer Nachricht minimiert wird (Dummy Traffic). Durch Dummy Traffic kann ein Angreifer nicht mehr feststellen, wann ein Sender wirklich senden will und wann nicht.
Die Kernfunktion eines Mixes ist das Umkodieren der Nachrichten. Hierzu wird mit Hilfe eines asymmetrischen[4] Kryptosystems jede zu mixende Nachricht mit dem privaten Schlüssel des Mixes entschlüsselt (umkodiert) und an den nächsten Mix weitergeschickt (**Bild 2**).
Mehrere unabhängige Betreiber der zwischengeschalteten Mixe garantieren die Unbeobachtbarkeit der Kommunikationsbeziehungen. Solange mindestens ein Mix gutartig ist, bleibt die Kommunikationsbeziehung geschützt.
Das Mix-Konzept war in den letzten Jahren Gegenstand vieler Forschungsarbeiten, zum Teil mit Grundlagencharakter, siehe z.B. [3, 4, 5, 6], aber auch mit einer deutlichen Anwendungsorientierung, siehe z.B. [7, 8, 9, 10, 11, 12].

2.1.3.2 Modifikationen bei Onion-Routing

Chaum hatte damals als Dienst die Elektronische Post gewählt. Sie hat den Vorteil, nicht von Echtzeitanforderungen und Verbindungen abhängig zu sein. Für das World Wide Web benötigt man jedoch eine zumutbare Verzögerungszeit, bis die Antwort auf eine Anfrage im Browser zu sehen ist. Daher waren Modifikationen des Gundkonzeptes notwendig, die zum Teil zu Lasten des erreichten Schutzes gehen.
Beim Onion-Routing wird zunächst über eine Kanalaufbaunachricht (create) eine Onion (Aufbau für drei Onion-Router X, Y, Z, siehe **Bild 3**) gesendet. Die Onion enthält eine Zeitangabe (exp_time), die angibt, wann eine Onion verfällt. Die Zeitangabe dient der Abwehr von Nachrichtenwiederholungen. Solange exp_time noch nicht abgelaufen ist, speichert der Onion-Router die Onion und testet auf Nachrichtenwiederholung. Weiterhin enthält die Onion die Adresse des nächsten Onion-Routers sowie Schlüsselmaterial, das für die nachfolgende Etablierung des „anonymen Kanals“ verwendet wird.
Bei Ihrem Lauf durch das Netz wird die Onion Schritt für Schritt abgebaut, d.h. im jeweiligen Onion-Router entschlüsselt, und gleichzeitig der anonyme Kanal aufgebaut. Hierzu merkt sich jeder Onion-Router, woher er eine Onion erhalten hat und wohin er die verbleibende Onion geschickt hat und zusätzlich ein Kennzeichen, die sog. Pfad-ID. Empfängt ein Onion-Router Daten für eine bestimmte ID, so verschlüsselt er die erhaltenen Daten mit einem symmetrischen Kryptosystem, dessen Schlüssel er aus dem Schlüsselmaterial (Key Seed) der Onion gewonnen hat.



Jede „Schale“ ist mit dem public key des nächsten Onion-Routers verschlüsselt.

Bild 3. Aufbau einer Onion

Dummy Traffic wird nur zwischen den Onion-Routern erzeugt und bietet somit bei geringer Auslastung des Dienstes keinen (bzw. nur geringen) Schutz gegen Beobachtung, da die Enden eines Kommunikationskanals allein über die ausgetauschte Datenmenge verkettet werden können.
Da die über die anonyme Verbindung laufenden Daten eine beliebige Länge haben können, ist eine Verkettung über die Länge der über den anonymen Kanal gesendeten Nachrichten möglich.

2.1.4 Vergleich unter Sicherheitsaspekten

Sofern überhaupt eine Metrik über dem erreichten Schutz der drei vorgestellten Verfahren sinnvoll ist, kann man feststellen, daß Crowds gegen stärkere Angriffe schützt als Anonymizer, und Onion Routing stärker schützt als Crowds.
In **Tabelle 1** werden die genannten Verfahren noch einmal nach dem erreichten Schutz gegenüber Verkehrsanalysen zusammengefaßt.

Tabelle 1. Schutz gegen Verkehrsanalysen

	Zeitliche Verkettung	**Verkettung über Inhalt**
Anonymizer	keine Vorkehrungen dagegen	keine Vorkehrungen, lediglich Headerinformationen werden entfernt
Crowds	keine Vorkehrungen, aber wenigstens Zusammenfassung von Anfragen in Jondos	keine Vorkehrungen, aber wenigstens sind Inhalte verschlüsselt
Onion Routing	schwache Vorkehrungen, lediglich Dummy-Traffic zwischen Onion-Routern	für Kanalaufbau keine Verkettung, für Datenaustausch jedoch Verkettung über Nachrichtenlänge möglich

2.2 Unbeobachtbarkeit gegen starke Angreifer

Im Abschnitt 2.1 wurden die Ansätze Anonymizer, Crowds und Onion Routing vorgestellt. Dabei orientiert sich Oninon Routing bereits am Mix-Konzept, das auch einen gewissen Schutz gegenüber einem Netzbetreiber gewährleistet, während die anderen Konzepte von schwächeren Angreifermodellen ausgehen.
Zur Anonymisierung von Webzugriffen wird in der hier vorgestellten Lösung ebenfalls das Mix-Konzept in Kombination mit einem Proxyservice verwendet. Dabei wird der Proxy um die Mix-Funktionalität erweitert. Leider können die klassischen Mixe aus [2] nicht ohne Modifikationen verwendet werden. Gründe hierfür sind bereits bei der Vorstellung von Onion Routing genannt worden.

Mix-Proxy

Beim Einsatz von Mixen zum Schutz von Verbindungen (nicht nur im World Wide Web) vor Beobachtung müssen folgende konkrete Probleme gelöst werden.

1. Es treten unterschiedliche Nachrichtenlängen auf. Unterschiedlich große Objekte (Webseiten, Bilder etc.) müssen übertragen werden.
2. Das Verkehrsaufkommen schwankt.
   – nutzerbezogen: Normalerweise entstehen beim Aufruf einer Webseite sog. Anfragebursts, nachdem eine Webseite mit vielen eingebundenen Objekten geladen wurde und die Objekte selbst angefordert werden.
   – netzbezogen: die Anzahl der Dienstnutzer ist nicht ständig konstant.

Ansätze zur Lösung der genannten Probleme sind:

zu 1. Gleiche Nachrichtenlängen:
   – Traffic Padding, d.h. Auffüllen aller Nachrichten auf die Länge der längsten Nachricht. Als Paddingbits werden Zufallszahlen verwendet.
   – Zeitscheiben analog [7], d.h. Zerstückelung einer Nachricht (so daß die gemeinsam bearbeiteten Teilnachrichten eines Schubs die gleiche Länge haben) und Zusammensetzen der ursprünglichen Nachricht beim Empfänger (Nur er kann die Verkettung der Teilnachrichten vornehmen).

zu 2. Einsatz von Dummy Traffic:
   – unter Einbeziehung der Auslastung des Dienstes bzw. des Netzes
   – direkt durch die Teilnehmer, da ansonsten das Senden „echter“ Nachrichten beobachtbar ist.

Ziel der Lösung ist es, möglichst nicht vom Angreifermodell der klassischen Mixe abweichen zu müssen. Das bedeutet, ein Angreifer muß

– entweder alle Mixe beherrschen, die eine Nachricht durchlaufen,
– oder, bei m bearbeiteten Nachrichten pro Schub, m-1 Nachrichten selbst erzeugt haben, damit er die eine verbleibende verfolgen kann.

Ein Mix selbst wehrt aufgrund seiner Funktionen folgende Angriffe ab:

– zeitliche Verkettung ein- und ausgehender Nachrichten,
– Verkettung über deren Aussehen und Länge,
– Replay (Wiederholung durch Angreifer) von Nachrichten.

Über die Grundfunktion der Mixe hinaus wurden die in **Tabelle 2** genannten Elemente der Lösung vorgesehen, die dann im Einzelnen erklärt werden.

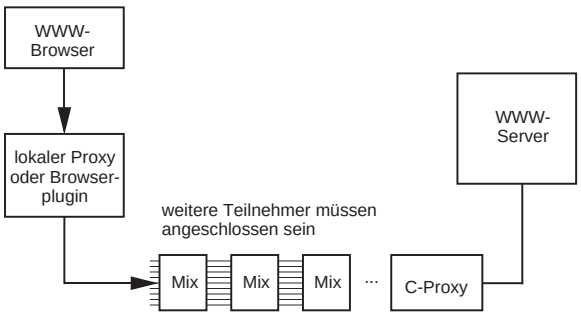


Bild 4. Architektur des Dienstes

In **Bild 4** ist die Architektur des Dienstes dargestellt. Auf dem lokalen System ist ein sog. lokaler Proxy

installiert, der die Anfragen für die Mixe vorbereitet, d.h. jeweils mit den öffentlichen Schlüsseln der Mixe verschlüsselt (allgemeines Schema siehe Bild 2). Die Mixe entschlüsseln jeweils die Nachrichten. Der C-Proxy stellt die Anfrage an den Server. Bei der Antwort des Servers können nun folgende Probleme auftreten:

– Die Antwort kann beliebig lang sein.
– Sie kann langsam bzw. verzögert eintreffen.
– Die Daten müssen vom C-Proxy schon weitergegeben werden, obwohl die Gesamtlänge der Antwort noch unbekannt ist.

Tabelle 2. Funktionslemente des Mix-Proxys

Element	Funktion	Probleme
Dummy Traffic	Vergrößern der Anonymitäts-gruppe, notwendig bei geringem Verkehrsaufkommen	zusätzlicher Bandbreiteaufwand
– durch die Mixe erzeugt		Mixe arbeiten nicht mehr deterministisch und damit nicht teilnehmerüberprüfbar
– durch die Teilnehmer erzeugt	zusätzlich: Verbergen, wer wann sendet (Senderanonymität)	möglicherweise nicht ständig alle Teilnehmer am Netz
Anonyme Kanäle	für Verbindungen notwendig	alle Kanäle müssen gleichlang existieren und gleiche Kapazität haben
Zeitscheiben	Unverkettbarkeit bei unterschiedlich langen Nachrichten	Overhead durch Fraktionierung der Nachrichten

Adaptives Zeitscheibenprotokoll

Die genannten Punkte gelten sinngemäß auch bereits für die Anfrage an den Server, wenn auch nicht so drastisch. Das im folgenden vorgestellte adaptive Zeitscheibenprotokoll (**Bild 5**) ist auch in der Lage, den „Hinweg“ zu sichern. Dies wird im folgenden zur Vereinfachung der Darstellung weggelassen.
Über den anonymen Kanal wird ein Datenblock mit einer (innerhalb des Schubes) festgelegten Länge als Rückantwort übermittelt. Danach wird der anonyme Kanal abgebaut. Das bedeutet, daß Nachrichten, die länger als die Blockgröße sind, in einer weiteren Zeitscheibe übermittelt werden müssen. Hierfür wird dem lokalen Proxy vom C-Proxy ein Kennzeichen KZ übermittelt und über ein Flag (wait) mitgeteilt, daß noch weitere Daten zur Übermittlung bereitliegen bzw. vom Server erwartet werden.
Sind nicht genug Daten vorhanden, um den Block zu füllen, werden Paddingbits angefügt.
Da die innerhalb des Schubes festgelegte Blockgröße von der aktuellen Antwortsituation im C-Proxy abhängig ist, entscheidet der C-Proxy über die aktuelle Bockgröße und wann die nächste Antwortzeitscheibe beginnt. Eine extreme Situation wäre z.B., daß eine Antwort sehr lang ist, aber viele Antworten sehr kurz oder noch nicht vorhanden sind.

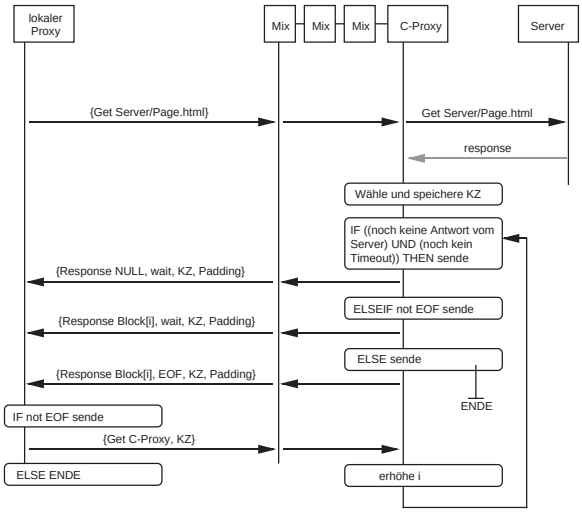


Bild 5. Protokoll zwischen lokalem und C-Proxy

Bedeutung der Nachrichten im Protokoll in Bild 5:

– **Get Server/Page.html**
http-Anfrage
– **Response NULL, wait, KZ, Padding**
C-Proxy hat bisher keine Daten vom Server erhalten (NULL), Zeitscheibe ist abgelaufen, jedoch noch kein Timeout (wait), deshalb Übermittlung des Kennzeichens KZ, um die Antwort in einer späteren Zeitscheibe vom C-Proxy zu erfragen.
– **Response Block[i], wait, KZ, Padding**
C-Proxy sendet an lokalen Proxy den Teil i der Serverantwort (Block[i]), weitere Daten verfügbar (wait).
– **Response Block[i], EOF, KZ, Padding**
C-Proxy sendet an lokalen Proxy den Teil i der Serverantwort (Block[i]), dies ist der letzte Block (EOF).
– **Get C-Proxy, KZ**
http-Anfrage, um weitere Daten vom C-Proxy für das Kennzeichen KZ anzufordern.

3 Authentizität, Verschlüsselung und Netzwerksicherheit

3.1 Problemstellung

Wie eingangs festgestellt, ist es für viele Organisationen und Unternehmen unumgänglich, das interne Netz in irgendeiner Form an das weltweite Internet anzubinden. Gründe dafür sind:

- Darstellung des eigenen Unternehmens, Produktinformationen, Kunden-Support etc.,
- Bereitstellung von Internet-Diensten (E-Mail, Webzugriff etc.) für Mitarbeiter zur effizienten Kommunikation und Informationsbeschaffung,
- Electronic Commerce, Anbieten von Waren und Dienstleistungen, evtl. mit Zahlungsmöglichkeit.

Besonders die beiden letzten Punkte erfordern eine enge Verknüpfung der vom Internet zugänglichen Systeme mit Datenbanken, Warenwirtschaftssystemen, letztlich mit jedem Mitarbeiter-PC. Dabei ist es illusorisch, jeden einzelnen PC und seine Anwendungen abzusichern. Vielmehr wird der Übergang in das offene Netz auf wenige Punkte konzentriert, an denen gezielt eine zu definierende Sicherheitspolitik durchgesetzt wird, die mindestens festlegt, wer welche Dienste nutzen darf.

Weitere Anwendungsfelder sind Remote Access und Virtual Private Networks (VPN), die das Internet als breit verfügbare und kostengünstige Kommunikationsinfrastruktur nutzen.

Die Sicherheitspolitik ordnet dabei i.A. bestimmten Nutzern Berechtigungen zu. Zu ihrer Durchsetzung ist es notwendig, den Nutzer zunächst sicher zu identifizieren, um ihm seine Rechte zuordnen zu können (Autorisierung). Oftmals sind die Daten, die dieser Nutzer dann überträgt, ebenfalls sicherheitsrelevant, so daß zusätzlich starke Verschlüsselungsmechanismen eingesetzt werden müssen.

3.2 Herkömmliche Lösungen und deren Nachteile

Zur Umsetzung von Sicherheitspolitiken an konzentrierten Übergangspunkten wurden Firewallsysteme entwickelt, die als Mauer und gleichzeitig als Bindeglied zwischen dem offenen und unsicheren Internet und dem zu sichernden Intranet dienen. Sie können auf verschiedenen Netzwerkschichten wirken (Paketfilter oder Application Level Gateways).

Paketfilter sind Router mit spezieller Filterfunktion. Der Filter läßt nur Pakete bestimmter Dienste (E-Mail, Filetransfer etc.) von und zu bestimmten Rechnern (bzw. Rechneradressen) passieren. Application Gateways lassen bzgl. einer Anwendung (z.B. News) verschiedene Steuermöglichkeiten offen (z.B. Blockung bestimmter Newsgruppen). Sie können auch als Proxies konfiguriert werden, d.h. es wird vor dem externen Netz verborgen, welcher organisationsinterne Rechner gerade die Anwendung nutzt.

Diese Lösungen haben jedoch gravierende Nachteile:

- Sicherheitsrelevante Entscheidungen fallen an Hand ungesicherter Daten: Paketfilter, oftmals aber auch Application Level Gateways, nutzen als identifizierende Information die IP-Adresse und den Port zum einen des Zugreifenden (Source), zum anderen des zu nutzenden Dienstes (Destination). Diese Informationen werden jedoch im IP-Paket ungeschützt übertragen, so daß diese von einem Angreifer beliebig manipuliert werden können [13].
- Eigentlich sollen durch die Sicherheitspolitik Nutzern bestimmte Rechte zugeordnet werden. Eine IP-Adresse identifiziert jedoch nur Computer, nicht den daran arbeitenden Nutzer.

Besonders im Bereich der Remote-Access-Server, die eine Untergruppe von Firewallsystemen speziell zur Absicherung von Wählzugängen darstellen, haben sich jedoch auch nutzerbezogene Authentisierungsprotokolle (RADIUS, TACACS, siehe [14, 15]) etabliert, die oft in Verbindung mit sog. Token-Systemen (z.B. SecureID) eingesetzt werden und zunehmend auch mit Internet-Firewalls zusammenarbeiten. Nachteilig an dieser Lösung ist jedoch, daß

- die Token-Systeme proprietär sind,
- die Authentisierungsmechanismen auf symmetrischen kryptographischen Verfahren beruhen,
- die Authentisierung nur beim Erstzugriff erfolgt, die folgenden Daten jedoch nicht zwangsläufig gesichert werden, und damit gegen sog. Hijacking-Angriffe verwundbar sind.

Auch VPN-Funktionen basieren derzeit auf proprietären Verfahren, so daß eine Interoperabilität zwischen Systemen unterschiedlicher Hersteller nicht gewährleistet ist.

Zusammenfassend kann festgestellt werden, daß die bisher gebotenen Verfahren zur Authentisierung für die immer komplexer werdenden Netzstrukturen nicht ausreichend flexibel und sicher sind. Zusätzlich sind Verschlüsselungsverfahren (z.B. bei VPN-Funktionen) proprietär und durch Exportrestriktionen oftmals ebenfalls sehr unsicher.

3.3 Sichere und flexible Authentisierung und Verschlüsselung

Zur Überprüfung von Zugriffs- und Nutzungsberechtigungen sowie zur Verschlüsselung und Integritäts-

sicherung von Daten wird eine Lösung vorgestellt, die auf der Grundlage des Internet-Standards SSL (Secure Socket Layer) arbeitet.
Mit SSL steht ein auf Verbindungsebene eingebauter Sicherheitsmechanismus bereit, der eine flexible und sichere, auf Zertifikaten basierte Authentisierung bereitstellt und gleichzeitig die nachfolgende Verbindung mit einem vom Client wählbaren Algorithmus verschlüsselt und authentisiert. Dazu wird zu Beginn einer Verbindung ein kryptographisches Authentisierungsprotokoll durchlaufen, in dem zusätzlich ein Schlüsselaustausch erfolgt.

Dynamischer IP-Filter

Die genannten Nachteile herkömmlicher Firewallsysteme veranlaßten uns dazu, deren Konzept um einen auf SSL basierenden Authentisierungsdienst zu erweitern und diesen mit einem dynamischen IP-Filter zu koppeln. (**Bild 6**)

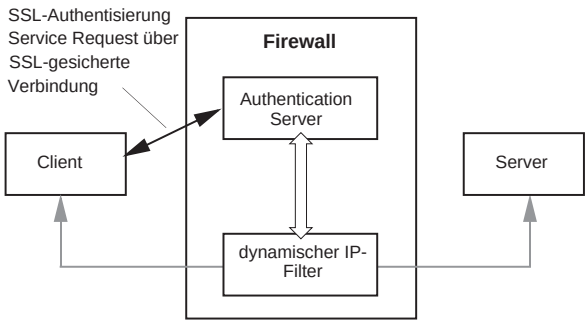


Bild 6. Netzwerksicherheit mit dynamischen IP-Filtern

Bevor ein Dienst genutzt werden kann, muß folgende Prozedur durchlaufen werden:

1. SSL-Verbindungsaufbbau zum Authentisierungsserver. Mit dem Aufbau einer SSL-Verbindung zum Authentisierungsserver ist eine kryptographisch sichere Prüfung des Client-Zertifikates und damit dessen Identität verbunden. Dem Authentisierungsserver steht nun das Zertifikat des Clients zur Verfügung.
2. Service Request. Über die SSL-geschützte Verbindung kann der Client sein gewünschtes Kommunikationsziel (IP-Adresse und -Port) bekanntgeben.
3. Rechteprüfung. Dem Authentisierungsserver stehen nun *zwei gesicherte Kriterien*, das Client-Zertifikat und der angeforderte Dienst, für eine Rechteprüfung zur Verfügung.
4. Akzeptieren/Ablehnen. Fällt die Prüfung der Zugriffsrechte positiv aus, wird eine entsprechende Meldung an den Client gesendet und genau für die geforderte Verbindung (Client-IP-Adresse, Client-Port, Server-IP-Adresse, Server-Port) ein IP-Filter freigeschaltet. Im negativen Fall wird die Verbindung zum Client abgebrochen.

Damit ist die Authentisierung des Zugreifenden unabhängig von der gerade verwendeten IP-Adresse möglich. Um den temporären authentisierten Kanal nicht der Gefahr des Hijacking auszusetzen, sollte SSL zusätzlich ende-zu-ende eingesetzt werden (SSL-Tunnel in **Bild 7**).

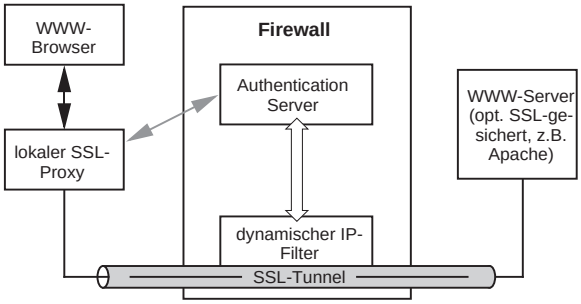


Bild 7. Authentizität und Verschlüsselung

4 Leistungsfähigkeit

4.1 Prototypimplementierung

Auf der CeBIT 98 in Hannover wurde der Prototyp vorgestellt (**Bild 8**), der die Funktionsfähigkeit des Konzeptes gezeigt hat, jedoch mit Einschränkungen an die erreichbare Dienstqualität (Durchsatz, Verzögerungszeiten, Flexibilität). Im Verlauf der Arbeiten soll dieser Prototyp erweitert und verbessert werden.

Bild 8. Der Prototyp auf der CeBIT 1998

4.1.1 SSL-Authentisierung und Verschlüsselung

Auf Clientseite wurde in der Prototypimplementierung der Ansatz über einen lokalen Proxy realisiert. Durch den Einsatz einer außerhalb Nordamerikas implementierten SSL-Bibliothek (SSLeay von Eric

Young) kann innerhalb des Proxys auf starke kryptographische Verschlüsselungsverfahren zurückgegriffen werden. Auch auf Serverseite wird ein generischer SSL-Proxy eingesetzt, der eingehende SSL-Verbindungen entschlüsselt und an den eigentlichen Dienst weiterleitet. Zunächst wurde die Implementierung für den WWW-Dienst realisiert.
Die Nutzung als lokaler Proxydienst (auf dem eigenen PC) erlaubt damit den Einsatz von Standard-WWW-Browsern und -Servern, deren eigene SSL-Implementierungen durch amerikanische Exportbeschränkungen in ihrer Sicherheit stark eingeschränkt sind. Dieser Ansatz ist zudem für beliebige andere Internetdienste, die verbindungsorientiert arbeiten, nutzbar.
Zusätzliche Sicherheit wird durch Smartcards erreicht. So ist es möglich, sämtliche Berechnungen, die den geheimen Schlüssel des Nutzers benötigen, in einer gesicherten Rechenumgebung, der Chipkarte, ablaufen zu lassen. Auch auf Serverseite (Authentisierungsserver und WWW-Server) kann ein Smartcard-Modul zum Einsatz kommen, um ein Höchstmaß an Sicherheit zu gewährleisten. Aus Performancegründen wird hier jedoch eine PC-Card-Variante genutzt. Damit kann auch dem Server eine „nicht kopierbare“ Identität verliehen werden.

4.1.2 Anonymität und Unbeobachtbarkeit

Die Mixe wurden ebenfalls auf der Basis von SSL realisiert. Als asymmetrisches Verschlüsselungsverfahren kommt RSA mit einer Schlüssellänge von 1024 Bit zum Einsatz. Für die Verschlüsselung der Daten auf dem anonymen Kanal wurde IDEA eingesetzt. Die öffentlichen Schlüssel der Mixe erhält der lokale Proxy in Form von X.509-Zertifikaten. Über eine Konfigurationsdatei wird die Reihenfolge der zu durchlaufenden Mixe festgelegt.

4.2 Durchsatz und Verzögerungszeit

Der Einfluß der SSL-Nutzung für Netzwerk- und Ende-zu-Ende-Sicherheit wurde in einem Testaufbau untersucht, wobei als Server ein Apache-WWW-Server auf dem Betriebssystem Linux diente. Als Hardwareplattform kam ein Pentium 133 MHz-System mit 32 MB RAM und einer Netzwerkverbindung mit 100 MBit/s zum Einsatz.
Als Vergleichsmessung diente ein direkter Zugriff ohne Sicherheitsfunktionen, bei dem mit der verwendeten Hardware ca. 120 Verbindungen pro Sekunde möglich waren und die Datenübertragungsrate prinzipiell nur durch die Netzbandbreite begrenzt war.
Mit den SSL-Funktionen sank die Anzahl der möglichen Verbindungen auf ca. 5 pro Sekunde, da der SSL-Verbindungsaufbau einen sehr starken Overhead bedeutet. Bei größeren zu übertragenden Dateien ist der Performanceeinbruch jedoch relativ geringer, da der Overhead nur beim Verbindungsaufbau entsteht.
Zusätzliche Leistung kostet der Einsatz von Smartcards zur Authentisierung, da diese die Kryptofunktionen momentan noch relativ langsam ausführen.

5 Schlußbemerkungen

5.1 Mehrseitige Sicherheit

Im Mittelpunkt der vorgestellten Lösungen steht der Nutzer, der sich und seine Informationen schützen will. Die vorgestellten Lösungen verhindern die Erstellung von Kommunikationsprofilen und bieten auch Schutz vor neugierigen Blicken von Administratoren, Internetprovidern oder professionellen Lauschern. Durch die zunehmende Sensibilisierung der Nutzer wächst deren Interesse an Schutzkonzepten, die das Vertrauen in Netzbetreiber und Provider nicht unbedingt fordern.
Es ist nicht das primäre Interesse eines Betreibers, beispielsweise Daten über seine Teilnehmer zu sammeln, um diese anschließend mißbräuchlich zu verwenden. Im Gegenteil: Je weniger Daten ein Betreiber zur Diensterbringung benötigt, umso weniger Kosten fallen für deren Verarbeitung und Schutz an. Damit wird das Ziel von „Mehrseitiger Sicherheit“ klar:
Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung.
Die Realisierung von mehrseitiger Sicherheit führt nicht zwangsläufig dazu, daß die Interessen aller Beteiligten erfüllt werden. Sie gewährleistet jedoch, daß die Partner einer mehrseitig sicheren Kommunikationsbeziehung in einem geklärten Kräfteverhältnis bezüglich Sicherheit miteinander interagieren.

5.2 Offene Probleme und künftiger Forschungsbedarf

Die entwickelte Lösung auf der Basis von SSL bietet bereits ein hohes Maß an Sicherheit und Flexibilität, verfügt jedoch auch über einige Nachteile. Sie ist

- derzeit nur in einfachen Remote-Access-Szenarien einsetzbar,
- anfällig gegen Denial-of-Service-Angriffe,
- nur für verbindungsorientierte Dienste geeignet,
- nicht völlig anwendungstransparent, d.h. die Anwendung muß einen (lokalen) Proxy unterstützen.

Die Lösung für das unbeobachtbare Surfen im Internet läßt bezüglich ihrer Konfiguration und flexiblen Nutzung noch einige Wünsche offen. So wäre es z.B.

wünschenswert, die Reihenfolge der Mixe direkt in einem Dialog im Browser zu konfigurieren.
Künftig werden Sicherheitsfunktionen auf Netzwerkebene in Verbindung mit einem universellen Authentisierungs- und Key-Management-Protokoll einen großen Teil der Sicherheitsanforderungen in komplexen Netzstrukturen abdecken, und das völlig transparent für Anwendungen und Anwender. Mit IPSec stehen die Mechanismen bereit, Authentizität, Integrität und Vertraulichkeit auf dieser Ebene auch zwischen mehreren Systemen zu gewährleisten.
Das zugehörige Authentisierungs- und Key-Management-Protokoll ist momentan jedoch nur für eine Peer-to-Peer-Kommunikation ausgelegt. Derzeit wird untersucht, wie dieses Protokoll für beliebig komplexe Netzstrukturen zur Etablierung von Sicherheitsfunktionen zwischen mehreren Parteien genutzt werden kann.

6 Literatur

[1] Kai Rannenberg, Andreas Pfitzmann, Günter Müller: Sicherheit, insbesondere mehrseitige IT-Sicherheit. in: Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley-Longman 1997, 21-29.

[2] David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24/2 (1981) 84-88.

[3] Andreas Pfitzmann, Michael Waidner: Networks without user observability. Computers & Security 6/2 (1987) 158-166.

[4] Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Datenschutz garantierende offene Kommunikationsnetze. Informatik-Spektrum 11/3 (1988) 118-142.

[5] Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz. IFB 234, Springer-Verlag, Berlin 1990.

[6] Birgit Pfitzmann, Andreas Pfitzmann: How to Break the Direct RSA-Implementation of MIXes. Eurocrypt '89, LNCS 434, Springer-Verlag, Berlin 1990, 373-381.

[7] Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: ISDN-MIXes – Untraceable Communication with Very Small Bandwidth Overhead. Proc. Kommunikation in verteilten Systemen, IFB 267, Springer-Verlag, Berlin 1991, 451-463.

[8] Andreas Pfitzmann: Technischer Datenschutz in öffentlichen Funknetzen. Datenschutz und Datensicherung DuD 17/8 (1993) 451-463.

[9] Lance Cottrel: Mixmaster & Remailer Attacks. http://www.obscura.com/~loki/remailer-essay.html.

[10] Hannes Federrath, Anja Jerichow, Andreas Pfitzmann: Mixes in mobile communication systems: Location management with privacy. Information Hiding, LNCS 1174, Springer-Verlag, Berlin 1996, 121-135.

[11] Andreas Fasbender, Dogan Kesdogan, Olaf Kubitz: Analysis of Security and Privacy in Mobile IP. 4th International Conference on Telecommunication Systems, Modelling and Analysis, Nashville, March 21-24, 1996.

[12] Hannes Federrath: Vertrauenswürdiges Mobilitätsmanagement in Telekommunikationsnetzen. Dissertation, TU Dresden, Fakultät Informatik, Februar 1998.

[13] CERT Advisory CA 96.21: TCP SYN Flooding and IP Spoofing Attacks, CERT Coordination Center, Pittsburgh 1996.

[14] C. Rigney, A. Rubens, W. Simpson, S. Willens: Remote Authentication Dial In User Service (RADIUS). RFC 2138. Obsoletes RFC 2058, Status: proposed standard.

[15] C. Finseth: An Access Control Protocol, Sometimes Called TACACS. RFC 1492. Status: informational.

---

[1] gefördert von der Gottlieb-Daimler- und Karl-Benz-Stiftung Ladenburg und dem Kolleg „Sicherheit in der Kommunikationstechnik“

[2] gefördert von der Deutschen Telekom Berkom GmbH

[3] Einfach ausgedrückt: Sowohl Sender als auch Empfänger besitzen den gleichen Schlüssel zum Ver- und Entschlüsseln.

[4] Sender und Empfänger haben unterschiedliche Schlüssel zum Ver- und Entschlüsseln. Der Verschlüsselungsschlüssel (public key) ist öffentlich bekannt, d.h. jeder kann eine Nachricht für den Empfänger verschlüsseln. Den Entschlüsselungsschlüssel (private key) besitzt nur der Empfänger und nur er kann somit seine empfangenen Nachrichten entschlüsseln.