Technischer Hintergrund von JAP

JAP ermöglicht es seinem Benutzer, die eigenen Datenspuren im Internet zu verwischen. Die Software bietet eine Möglichkeit zum Selbstschutz gegen professionelle Datensammler und Firmen, die ihr Geld mit dem Verkaufen von Persönlichkeitsprofilen verdienen. Im Endausbau soll das System auch gegen sehr starke Angreifer schützen, die in der Lage sind, Verkehrsanalysen durchzuführen, d.h. den gesamten Datenverkehr des Netzes über einen langen Zeitraum abzuhören.

Was ist JAP?

Mit dem JAP ist es möglich, Webseiten unbeobachtbar aufzurufen. Das bedeutet, dass weder der angefragte Server noch ein Lauscher auf den Verbindungen mitbekommt, welcher Benutzer welche Webseite aufgerufen hat. Diese Funktion wird dadurch erreicht, dass die Kommunikationsverbindung nicht direkt zum Webserver aufgebaut wird, sondern über eine sogenannte Mix Proxy Kaskade verläuft.

Da viele Benutzer gleichzeitig den Anonymitätsdienst nutzen, werden die Internetverbindungen jedes Benutzers unter denen aller anderer Benutzer versteckt: Jeder Benutzer könnte der Urheber einer Verbindung gewesen sein. Niemand, kein Außenstehender, kein anderer Benutzer, nicht einmal der Betreiber des Anonymitätsdienstes kann herausbekommen, welche Verbindungen ein bestimmter Benutzer hat.

Im Regelfall werden in einer Kaskade mindestens drei Mix Proxies arbeiten, die von unabhängigen Institutionen betrieben werden, die in einer Selbstverpflichtung erklären, dass sie weder Log-Files über die transportierten Verbindungen speichern, noch mit den anderen Mix Proxy Betreibern Daten austauschen, die dazu führen könnten, dass ein Benutzer von JAP enttarnt wird.

Technischer Hintergrund von JAP

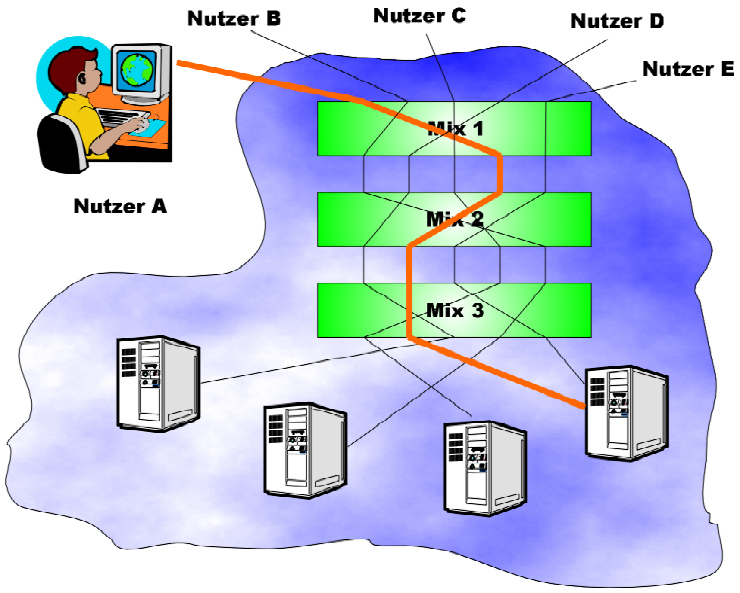
Umsetzung

Das System beinhaltet ein Client-Programm (JAP genannt), das sich jeder Nutzer auf seinem Rechner lokal installiert. Es ist auch möglich, dass mehrere Benutzer gemeinsam **einen** JAP benutzen. Existiert z. B. ein firmeninternes Intranet, so kann der JAP auf einem Rechner installiert werden, der sowohl Zugang zum Intranet als auch zum Internet hat.

Der JAP arbeitet als Proxy (z. B. für WWW-Browser) und ist über das Internet mit dem Anonymisierungsdienst verbunden. Dieser besteht aus mehreren hintereinandergeschalteten Zwischenstationen (von ihrem Erfinder David Chaum als Mixe bezeichnet). Jeder Mix sammelt dabei zunächst Nachrichtenpakete von mehreren Nutzern, bevor er sie umkodiert und umsortiert wieder ausgibt. Die Pakete sind mehrfach verschlüsselt und das Umkodieren besteht im Wesentlichen aus einer Entschlüsselung. In der Abbildung ist der prinzipielle Aufbau des Gesamtsystems dargestellt.

Ein Nutzer ist anonym innerhalb der Gruppe aller Nutzer des Anonymisierungsdienstes. Durch die Umkodierung wird erreicht, das ein- und ausgehende Datenpakete ein anderes Erscheinungsbild haben. Damit ist selbst ein Angreifer, der alle Leitungen überwacht, nicht in der Lage zu entscheiden, welche Eingabe- zu welcher Ausgabenachricht gehört. Alle Pakete sind gleich groß, so dass es auch an Hand dieser Eigenschaft nicht möglich ist, eine Verkettung von Ein- und Ausgabe herzustellen. Das gesamte Verfahren ist bereits sicher, wenn mindestens einer der verwendeten Mixe korrekt arbeitet.

Um die Vertrauenswürdigkeit des Dienstes zu erhöhen, sollen mehrere Mixe von unabhängigen Betreibern existieren. Der JAP bietet dem Nutzer die Möglichkeit, aus den vorhandenen Mix-Kaskaden diejenige auszuwählen, die seiner Meinung nach am vertrauenswürdigsten ist.



Mixe als Basis der Anonymisierung durch JAP

Eines der ersten Verfahren für das unbeobachtbare Versenden und Empfangen von Nachrichten sind die Mixe, die auf den amerikanischen Kryptographen David Chaum zurückgehen. Mixe sind eine Art hintereinander geschaltete Anon-Proxies. Viele verschlüsselt ankommende Nachrichten werden im Mix verwürfelt, in ihrem Aussehen verändert und schließlich wieder ausgegeben. Selbst wenn ein Beobachter („Big Brother“) alle Ein- und Ausgänge eines Mix beobachtet, verliert er die Zuordnung, welche ausgehende Nachricht zu welcher eingehen-

den Nachricht gehört. Die Funktionsweise eines Mixes gleicht einem Postamt, das jeden eingehenden Brief öffnet und darin wieder einen verschlossenen Briefumschlag vorfindet, den es an die darauf stehende Adresse, meist wieder ein Postamt, weiterleitet. Das nächste Postamt verfährt ebenso, bis der Brief entsprechend verzögert schließlich beim Empfänger landet. In der Welt des Internet sind die Briefe die Datenpakete und die Postämter die Mixe. Damit diese Weiterleitung klappt, muss der Absender natürlich die Datenpakete entsprechend vorbereiten, d. h. sie verpacken (verschlüsseln), adressieren (mit der Adresse des Empfängers), frankieren, wieder verpacken, adressieren (diesmal mit der Adresse des letzen Postamts), frankieren usw. Dies muss unbedingt auf dem PC des Benutzers geschehen, damit niemand sonst mitbekommt, welche Adressen auf den inneren Datenpaketen stehen

Chaum ging bei der Entwicklung der Mixe davon aus, dass der Beobachter das gesamte Netz überwacht und zusätzlich einen Großteil der Mixe kontrolliert. Damit eine Nachricht unbeobachtbar durch das Kommunikationsnetz transportiert wird, muss lediglich ein einziger Mix vertrauenswürdig sein. Schließlich könnte Big Brother ja selbst viele Postämter betreiben. Würde der Benutzer nur einen Mix verwenden bzw. nur Mixe benutzen, die von genau einem Betreiber verwaltet werden, käme das wieder einer „frei Haus“ Lieferung des persönlichen Benutzungsprofils gleich. Als Grundregel für ein praktisches System gilt: Es müssen wenigstens zwei Mixe verwendet werden, damit weder der eine noch der andere Mix alles über die Kommunikationsbeziehung erfährt: Der erste Mix weiß, welcher Benutzer eine Anfrage absendet und dass er sie an einen Mix weiterleiten muss. Der zweite bzw. letzte Mix weiß, wohin eine Anfrage gesendet werden soll, aber nicht, bei welchem Benutzer sie ihren Ursprung hat. Solange die beiden Mixe nicht zusammenarbeiten, bleibt die Kommunikationsbeziehung vor allen Außenstehenden und sogar vor den Betreibern der Mixe verborgen.

In der Praxis wird man natürlich mehr als zwei Mixe verwenden, wobei jeder Mix von einer anderen Institution betrieben wird, die möglichst wenig gemeinsame Interessen mit den anderen Betreibern hat, so dass eine Enttarnung der Benutzer unwahrscheinlich ist. Die Anzahl der Mixe, für die sich ein Benutzer entscheidet, hängt letztendlich von so genannten Vertrauensfaktoren ab. Diese sind aber sozialer Natur und entziehen sich daher einer technischen Beschreibung. Es spielt für die erreichbare Unbeobachtbarkeit aus technischer Sicht keine Rolle, ob in einer Mix-Kette mit 5 Mixen genau 0, 1, 2, 3 oder 4 Mixe korrupt sind, solange wenigstens ein Mix vertrauenswürdig ist. Viel hilft also nicht unbedingt viel; besser ist es, die Betreiber der Mixe sorgfältig auszuwählen, damit diese nicht mit vereinten Kräften an der Enttarnung ihrer Benutzer arbeiten.

Solche Mix-Betreiber könnten z. B. sein: Datenschutzbeauftragte des Bundes und der Länder, Bürgernetzvereine, kirchliche Organisationen und insbesondere Institutionen, deren Geschäftsfeld typischerweise Diskretion erfordert, z. B. Banken, Beratungsstellen oder die Post. Selbstverständlich könnten auch Internet Service Provider (ISPs) oder auf Sicherheit spezialisierte Unternehmen solche Mixe betreiben.

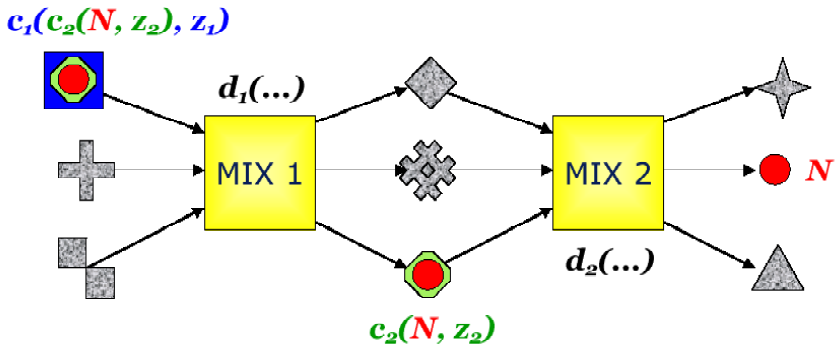
Da sich die Mixe an unterschiedlichen physischen Orten befinden und von unabhängigen Betreibern angeboten werden, ist die Chance, dass doch alle Mixe mit dem Beobachter zusammenarbeiten, sehr gering. In jedem Fall muss aber der Benutzer wesentlich weniger Vertrauen in den einzelnen Betreiber eines Mixes investieren, als dies bei den Anon-Proxies nötig ist. Schließlich kann nicht einmal ein Mix feststellen, welcher Benutzer mit welchem Server kommuniziert.

Technische Beschreibung

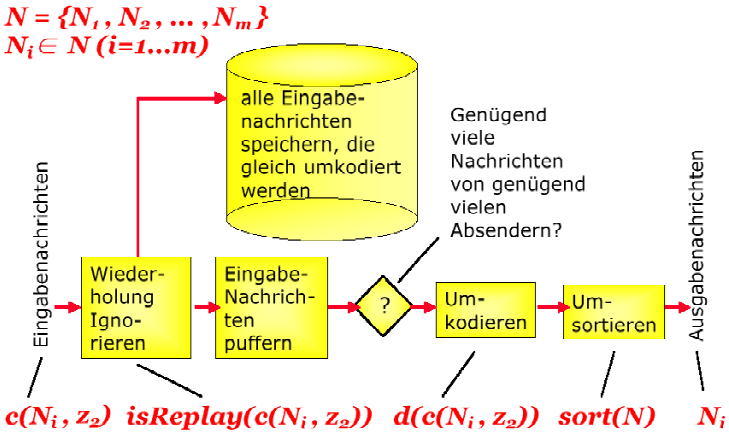
Im folgenden werden der Aufbau und das Funktionsprinzip des Mix-Netzes erklärt. Ein Mix-Netz besteht aus einer Folge von Rechnern, den Mixen, die beispielsweise über das Internet verbunden sind. Die Mixe verarbeiten Nachrichten dabei schubartig, wobei ein Schub aus allen von den Teilnehmern innerhalb einer bestimmten Zeit gesendeten Nachrichten besteht. Die Nutzer des Mix-Netzes senden ihre Nachrichten an den ersten Mix, dieser schickt alle Nachrichten an den zweiten Mix und so fort. Der letzte Mix der Folge sendet die Nachrichten dann jeweils an den eigentlichen Zielrechner. Damit verhindert wird, dass ein Beobachter, der die Datenleitungen abhören kann, den Weg einer Nachricht verfolgt, muss sie mehrfach verschlüsselt werden. Der Sender verschlüsselt jede zu sendende Nachricht so, dass sie nur dann entschlüsselt, und damit der Empfänger ermittelt werden kann, wenn sie von allen zu verwendenden Mixen in der vom Sender vorgesehenen Reihenfolge entschlüsselt wurde.

Dies geschieht nach folgendem Schema (siehe Postamtbeispiel oben): Der Sender verschlüsselt die Nachricht zunächst für den letzten Mix, so dass nur dieser sie lesen kann. Das Ergebnis dieser Verschlüsselung wird nun erneut verschlüsselt, diesmal jedoch für den vorletzten Mix. Nun wird das Ergebnis für den vorvorletzten Mix verschlüsselt und so fort, bis letztendlich eine Verschlüsselung für den ersten Mix durchgeführt wird.

Die so vorbereitete Nachricht wird an den ersten Mix gesendet. Nur er kann sie entschlüsseln und verschickt das Ergebnis dieser Entschlüsselung an den zweiten Mix. Dabei handelt es sich um eine Nachricht, die nur der zweite Mix entschlüsseln kann. Die entschlüsselte Botschaft schickt er weiter an den dritten Mix und so weiter.



Ein Beobachter, der alle Leitungen eines Mixes belauscht, sieht, wie verschlüsselte Nachrichten den Mix erreichen und wieder verlassen. Da der Mix aber eine Umkodierung (Entschlüsselung) durchgeführt hat, ist es dem Beobachter nicht möglich, eine Beziehung zwischen eingehenden und ausgehenden Nachrichten herzustellen. Eine Zuordnung der Nachricht ist insbesondere deshalb nicht möglich, da immer mehrere Nachrichten von unterschiedlichen Teilnehmern schubweise bearbeitet und im Mix *umsortiert* werden. Daher die Bezeichnung „Mix“. Ein Beobachter kann also nicht davon ausgehen, das z. B. die dritte eingehende Nachricht zu der dritten vom Mix gesendeten Nachricht gehört.



Die mehrfache Verschlüsselung und die Umsortierung reichen jedoch noch nicht aus. So müssen alle von den Teilnehmern eines Mix-Netzes gesendeten Nachrichten die *gleiche Länge* haben. Ansonsten wäre es einem Beobachter möglich, den Weg der Nachricht durch das Netz nur aufgrund ihrer Größe zu bestimmen, da er sie anhand dieses Merkmals von allen anderen Nachrichten unterscheiden kann.

Es ist außerdem wichtig, dass die Teilnehmer eines Mix-Netzes auch dann Daten senden, wenn sie eigentlich keine Nachrichten übermitteln wollen. Diese Leernachrichten werden als *Dummy-Traffic* bezeichnet. Ohne ihn wäre es einem Beobachter ebenfalls möglich, die Kommunikationsbeziehung aufzudecken: Da er das Netz überwacht, bemerkt er, wenn ein Teilnehmer aufhört zu senden und gleichzeitig ein vom letzten Mix adressierter Rechner keine Daten mehr empfängt.

Mixe müssen sich auch gegen sogenannte *Replay-Attacken* schützen. Dabei zeichnet der Beobachter eine Nachricht auf und spielt sie später noch einmal ein, so dass dem Mix eine bereits versendete Nachricht zur erneuten Bearbeitung vorgelegt wird. Der Mix führt die Entschlüsselung durch und sendet das Ergebnis weiter. Dabei entsteht eine zur ursprünglichen Verarbeitung identische Nachricht. Vergleicht ein Beobachter nun die Ausgaben des Mixes, kann er die wiederholt gesendete Nachricht entdecken, da nur sie in beiden Ausgaben vorhanden ist. Er hat somit diesen Mix überbrückt. Um solche Replay-Angriffe zu verhindern, besitzt jeder Mix eine Datenbank, in der er bereits bearbeitete Nachrichten speichert. Genau genommen speichert er nicht die Nachricht selbst, sondern nur einen aus der Nachricht berechneten "Fingerabdruck", der diese Nachricht eindeutig identifi-

ziert. Wird dem Mix nun eine Nachricht zur Bearbeitung vorgelegt, überprüft er zunächst, ob sie nicht bereits bearbeitet wurde. In diesem Fall ignoriert er die Nachricht. Um ein unbegrenztes Anwachsen der Datenbank zu verhindern, besitzt jede Nachricht einen Zeitstempel. Der Mix bearbeitet dabei nur Nachrichten, die innerhalb einer vorgegebenen Zeitschranke liegen, z.B. Nachrichten, die nicht älter als eine Minute sind. Somit muss sich der Mix auch nur diese Nachrichten merken. Ältere Nachrichten kann er aus der Datenbank löschen, da sie sowieso nicht mehr bearbeitet würden.

Die sogenannten *"n-1"-Angriffe* stellen eine weitere Gefahr für die Anonymität der Nutzer dar. Die Größe *n* meint dabei die Anzahl der Teilnehmer eines Mix-Netzes (genauer: die Schubgröße). Das Prinzip des Angriffs beruht darauf, dass man von den *n* zu einem Zeitpunkt verarbeiteten Nachrichten *n*-1 kennt und deren Weg bestimmen kann. Als einzige unbekannte bleibt somit die Nachricht des angegriffenen und nun enttarnten Teilnehmers übrig. Durchführbar ist dieser Angriff z.B., indem ein Teilnehmer alleine *n*-1 Nachrichten generiert oder *n*-1 Teilnehmer zusammenarbeiten. Dass mehrere Nachrichten eines Schubes vom selben Teilnehmer stammen, lässt sich mittels kryptographischer Verfahren verhindern. Technisch nicht kontrollierbar ist natürlich, ob Teilnehmer zusammenarbeiten (z. B. weil sie alle mit dem Big Brother zusammenarbeiten), um andere zu enttarnen.

Neben den hier kurz vorgestellten klassischen Angriffen auf das Mix-Netz gibt es eine Reihe weiterer Probleme, die die Anonymität gefährden. Berücksichtigt man diese jedoch, ist es möglich, ein System zu entwickeln, das auch gegen starke Angreifer (Big Brother) einen sicheren Schutz vor Beobachtung gewährleistet.

* * *