DuD
Datenschutz und Datensicherheit

Chaffing und Winnowing

Dirk Fox

Gateway (Tor, Durchgang) ist ein Vermittlungscomputer, der zwei unterschiedliche, aber gleichartige Kommunikationssysteme verbindet. Dazu setzt er die Kommunikationsregeln (Protokolle) des einen in die des anderen um. So ermöglicht er den Teilnehmern beider Systeme, sich zu verständigen. In unserem „Gateway" werden Juristen technische und Technikern juristische Begriffe erläutert.

Ronald Rivest, Kryptologe am MIT und einer der Autoren des RSA-Verfahrens, sorgte mit der Publikation eines neuen Verfahrens, das er „Chaffing and Winnowing"[1] nennt, am 18. März 1998 für Aufregung: Das Verfahren ermöglicht die vertrauliche Übertragung von Daten ohne Verschlüsselung. Damit ist „Chaffing and Winnowing" ein weiteres überzeugendes technisches Argument, das die Umgehbarkeit jeder Kryptoregulierung belegt. Die Funktionsweise des Verfahrens ist einfach. Es setzt sich aus zwei Schritten zusammen:

- Die zu versendende Nachricht wird in Blöcke zerlegt und jeder Block mit einer Folgenummer versehen. An diese numerierten Datenpakete hängt der Sender einen mit einem geheimen, nur ihm und dem Empfänger bekannten Authentifizierungsschlüssel berechneten *message authentication code* (MAC) an.[2]
- Anschließend werden Pakete mit zufälligem Inhalt, bereits vergebenen Folgenummern und einem beliebigen, zufällig gewählten „MAC"-Wert erzeugt, in den Nachrichtenstrom eingemischt („chaffing"[3]) und versendet.

Ein Empfänger des gesamten Datenstroms kann nun mit Kenntnis des geheimen Authentifizierungsschlüssels diejenigen Pakete verwerfen („winnowing"[4]), bei denen der von ihm berechnete MAC nicht mit dem übermittelten übereinstimmt.

Der Nachrichteninhalt wird also nicht verschlüsselt, sondern offen verschickt. Ein Abhörer kann jedoch „Spreu" nicht von „Weizen" unterscheiden: Ohne Kenntnis des Authentifizierungsschlüssels ist es nicht möglich, gültige Pakete zu erkennen.

[1] http://theory.lcs.mit.edu/~rivest/chaffing.txt, überarbeitete Fassung vom 27. März 1998.

[2] So arbeiten übliche Authentifizierungsmechanismen in Kommunikationsprotokollen.

[3] Sinngemäß: „Spreu untermischen".

[4] Sinngemäß: „Ausspelzen" – das Trennen der Spreu vom Weizen.

Sicherheit

Sei n die Anzahl der Blöcke, in die die Nachricht m zerlegt wurde, und k die Anzahl der je Paketfolgenummer hinzugefügten „Chaff"-Pakete, dann muß ein Abhörer eines solchen mit „Chaff" versehenen Datenstroms die gültige Nachricht unter $(k+1)^n$ verschiedenen Nachrichten herausfinden; bei gleicher Auftrittswahrscheinlichkeit sinkt damit die Erfolgswahrscheinlichkeit exponentiell in der Anzahl der Nachrichtenblöcke.

In einer extremen Form des Verfahrens enthält jeder Block nur ein einziges Bit und jedem Paket wird ein „Chaff"-Paket mit dem inversen Bit hinzugefügt. In diesem Fall ist die Erfolgswahrscheinlichkeit eines Abhörers $1:2^{|m|}$ und damit nicht besser als zufälliges Raten: Für ihn ist es informationstheoretisch unentscheidbar, wie die authentische Nachricht lautet.

Voraussetzung ist allerdings, daß der Angreifer das MAC-Verfahren nicht brechen kann. Das gewählte Verfahren muß daher kryptoanalytischen Angriffen wie Strukturanalysen und *brute force*-Attacken widerstehen; die Schlüssel sollten wenigstens 128, besser 160 bit lang sein.[5]

Aufwand

Jedem gesendeten Block, gleichgültig ob „Spreu" oder „Weizen", sind eine Folgenummer und ein MAC hinzuzufügen. Der MAC sollte mindestens 32 bit (= 4 byte) und das Folgenummernfeld so lang sein, daß alle Blöcke einer mehrere Mbyte langen Nachricht mit einer eindeutigen Nummer versehen werden können. Wird eine Blocklänge von einem Bit gewählt, werden für die Folgenummer wenigstens 24 bit (3 byte) benötigt.

Damit fallen je Nachrichtenbit 4 byte MAC, 3 byte Folgenummer und noch einmal dasselbe, nämlich 57 bit „Spreu" an. Werden die Blöcke auf ein Byte aufgefüllt, summiert sich der Overhead auf 127 bit je Nachrichtenbit: Der Bandbreitenbedarf steigt also um mehr als zwei Größenordnungen.

[5] Siehe z.B. Dobbertin, DuD 2/97, S. 82 ff.

Varianten

Rivest schlägt eine Anzahl von Varianten seines Verfahrens vor, durch die sich die Zahl der „Spreu"-Pakete reduzieren läßt:

- Die Pakete eines Senders können mit den Paketen anderer Sender zu einem einzigen Datenstrom „gemischt" werden; die jeweils fremden Pakete sind aus Sicht des Empfängers „Spreu".
- Die Nachricht kann so in Blöcke zerlegt werden, daß erst nach Erhalt des letzten Blocks die Reihenfolge wiederherstellbar ist; dadurch wächst die Zahl der möglichen Kombinationen exponentiell in der Anzahl der Nachrichtenblöcke.
- Wählt der Sender die MAC-Werte der „Spreu"-Pakete nicht zufällig, sondern berechnet einige von ihnen mit einem zweiten Authentifizierungsschlüssel, kann er sogar gegenüber Dritten eine falsche Nachricht als richtige ausgeben.

Bewertung

Wie bei steganographischen Verfahren ist der Bandbreitenbedarf von „Chaffing and Winnowing" im Vergleich zu Verschlüsselungsverfahren erheblich. Wesentlicher Unterschied dieses Verfahrens zu steganographischen Techniken ist, daß für das Hinzufügen der „Spreu" (bei Steganographie das Verstecken der Daten z.B. in einem digitalen Bild- oder Tondokument) Sender und Empfänger kein gemeinsames Geheimnis besitzen müssen. Das Einfügen von „Spreu" in den Datenstrom kann auch von einem unbeteiligten Dritten erfolgen, beispielsweise von einem beliebigen Vermittlungsrechner. Es ist von einer Störung praktisch nicht zu unterscheiden.