eMCrypt Client

Unter Eselfängern

Nachdem die Werbung schon einige Zeit lief, ist seit Mitte April mit *eMCrypt Client* von der Firma 3PO Web-Invest Ltd. ein weiterer Client für das eMule und eDonkey Netzwerk erhältlich.[1, 2] Als hervorstechendes Merkmal wird das risikolose Tauschen durch die Online-Verschlüsselung mittels SSL (Secure Socket Layer) und MD5 (Message Digest 5) genannt. Bisher ist der *eMCrypt Client* kostenlos, soll aber in Kürze gegen ein einmaliges Entgelt angeboten werden.

Gegen die genannten Verschlüsselungsalgorithmen ist aus heutiger Sicht nichts einzuwenden, sofern sie richtig implementiert sind. Aber bei allen Tauschbörsen-Netzwerken (Peer-To-Peer, P2P), kommt es auch darauf an, an welcher Stelle eigentlich was verschlüsselt wird. Um das Problem zu verstehen, muß man sich über die Funktionsweise von Tauschbörsen im Klaren sein.

Bei allen (!) Tauschbörsen sollen letztendlich nur Daten von einem Teilnehmer (Anfangspunkt) zu mindestens einem weiteren Teilnehmer fließen (Endpunkt). Ob dies direkt oder über ein oder mehrere Zwischenstationen abläuft ist für das Endergebnis unerheblich. Damit Daten ausgetauscht werden können, müssen die Anfangspunkte in irgendeiner Form eine Liste der angebotenen Daten veröffentlichen, die Endpunkte auf diese Liste zugreifen und eine Auswahl treffen können. Wie immer im Internet ist jeder teilnehmende Computer durch seine IP-Adresse weltweit eindeutig ansprechbar, anderfalls wäre ein Datenaustausch nicht möglich. Verschlüsselung bedeutet nun, daß die Daten nur von dafür Befugten entschlüsselt werden können. Wer ist aber in einer Tauschbörse ein Unbefugter? Da es sich um ad hoc Netzwerke einander unbekannter, aber nicht im Sinne der Definition anonymer, Teilnehmer handelt sind alle Clients gleichberechtigt und somit befugt Daten zu senden und zu empfangen. An welcher Stelle soll nun durch Verschlüsselung die Sicherheit steigen? Eine verschlüsselte Angebotsliste ist zwar extrem sicher, aber das Netzwerk dürfte wohl schnell zum Erliegen kommen. Angebote die niemand verstehen kann sind wertlos.

Das Versenden von lokal verschlüsselten Dateien macht in diesem Zusammenhang auch keinen Sinn. Wozu sollte sich jemand eine solche Datei herunterladen, wenn er sie nicht nutzen kann? Wenn aber andererseits jeder Client den Schlüssel zum Entschlüsseln erhält, hätte man sich die Verschlüsselung gleich sparen können.

Als dritte Möglichkeit kommt die Sicherung der Übertragungswege gegen sogenannte Mann-in-der-Mitte-Angriffe (Man-in-the-middle-attacks), d.h. das Abhören einer Verbindung zwischen zwei Punkten durch einen Dritten, in Betracht. Ist diese Verbindung verschlüsselt kann ein Dritter nur dann Mithören, wenn er selbige mit erheblichem Aufwand knackt. Aber warum in alles in der Welt sollte jemand diesen Aufwand treiben, wenn er sich einfach einen Client installieren kann, um damit als ganz normaler Teilnehmer im Netzwerk mitlesen zu können? In einem offenen Tauschbörsennetzwerk ist es völlig bedeu-

tungslos ob alle Clients untereinander über verschlüsselte Verbindungen kommunizieren oder nicht und welches Verfahren hierfür verwendet wird, denn jeder Endpunkt muß in der Lage sein, die eingehenden Daten zu entschlüsseln.

Bleibt noch die verschlüsselte Speicherung der Daten auf der Festplatte. Prinzipiell keine schlechte Angelegenheit, nur leider für die Sicherheit in einem Tauschbörsennetz beim Dateiaustausch ebenfalls vollkommen bedeutungslos. Eine solche Maßnahme schützt nur vor unbefugten Zugriffen direkt am Rechner, dafür aber gibt es wahrlich bessere Alternativen.[3]

Als Fazit bleibt nur eine Schlußfolgerung: *eMCrypt Client* ist selbst geschenkt noch zu teuer! Wer sich mit diesem Programm in Sicherheit wiegt, wird über kurz oder lang eine böse Überraschung erleben. Mit Verschlüsselung allein ist das Problem der Identifizierbarkeit von Anfangs- und Endpunkt nicht zu lösen.

Die geschaltete Werbung mit dem Hinweis auf die anstehenden Klagen der Musikindustrie gegen Tauschbörsenteilnehmer kann man in diesem Zusammenhang als grob irreführend bezeichnen („Nie wieder Angst **bei** ungebetenem Besuch“, nicht etwa vor !). Von allen Produkten die mit einer derartigen Strategie beworben werden, sollte man besser die Finger lassen.

Damit ist *eMCrypt Client* innerhalb kurzer Zeit schon das zweite Programm welches versucht mit der Angst und Unwissenheit der Anwender Geld zu schinden.[4]

Andreas Beck

1. http://WWW.eMCrypt.com/
2. http://WWW.eMCrypt.info/
3. PGPdisk
   http://WWW.PGPi.org/products/pgpdisk/
4. Secure FileSharing. A. Beck. Attraktor 03/2004