CRYPTO MAGIC einfach. sicher. verbunden.

Whitepaper

CryptoApp Tunnel

Zusammenfassung

CryptoApp Tunnel bietet die vergleichbare Funktionalität eines VPNs, aber weitgehend ohne dessen Nachteile: Insbesondere durch die Arbeitsweise auf Sitzungsschicht (ISO/OSI Schicht 5), die ein Filtern pro Anwendung ermöglicht, kann hiermit ein einfach zu bedienender und wesentlich sichererer Remotezugang mit besserem Kosten-Nutzenverhältnis bei Betrieb und Konfiguration hergestellt werden.

Markus Schräder

CryptoMagic GmbH
Stettenstr. 36
86150 Augsburg

Telefon 089 / 420 95 59 74
E-Mail info@cryptomatic.eu
Online www.cryptomatic.eu

1 Stand der Forschung/Technik

In den meisten etablierten Betriebssystemen hat sich zur Übertragung der Daten von Anwendungen das Protokoll TCP/IP durchgesetzt. Hierbei werden die zu übertragenen Daten von der jeweiligen Anwendung an das Betriebssystem übergeben und von diesem an das Ziel übertragen. Um Daten in dieser Form über öffentliche Netze sicher zu übertragen, haben sich folgende Alternativen durchgesetzt:

1.1 Virtual Private Network

Ein VPN tunnelt paketorientierte Daten des Betriebssystems (ISO/OSI Schicht 2 oder 3), meist über UDP/IP (ISO/OSI Schicht 4), zu einem entfernten Netzwerk.

Der Vorteil bei VPN ist, dass es auf Betriebssystemebene arbeitet, und somit für alle Anwendung transparent funktioniert. Die Nachteile bestehen insbesondere aus folgenden Punkten:

1.1.1 Dauerhafter Eingriff

Die Datenpakete des Betriebssystems müssen im Kernelmodus, beispielsweise über eine virtuelle Netzwerkkarte, abgegriffen werden. Hierfür ist ein Installationsvorgang notwendig, der dauerhaft ins System des Clients eingreift und nur mit Administrationsberechtigungen möglich ist.

Im Firmenumfeld kann dies folglich nur durch einen Systemadmin und nur auf Firmencomputern durchgeführt werden.

1.1.2 Netzkopplung

Ein VPN bedeutet eine direkte Netzkopplung:

1.1.2.1 IP-Adressen und Routing

Zur Übertragung der Daten muss die Endstelle eindeutig adressierbar sein. Hierzu muss dieser eine IP-Adresse zugeordnet werden, die geroutet werden muss. Zudem eröffnet sich eine Vielzahl an VPN spezifischen Fehlerquellen, die insbesondere in heterogenen Umgebungen nur schwer zu beheben sind. Insbesondere ein IP-Sec VPN ist komplex, fehleranfällig und lässt sich im Fehlerfall nur von Fachpersonal reparieren. In der Regel sind Parallelinstallationen verschiedener Hersteller nicht möglich.

1.1.2.2 Schutz durch Firewalls notwendig

Die übertragenen Pakete müssen zum Schutz des Netzwerks gefiltert und in ihrer abgegriffenen Form als Pakete ressourcenaufwändig analysiert und gefiltert werden. Hierzu sind Firewalls notwendig, die von teurem Fachpersonal installiert, konfiguriert und gewartet werden müssen. Es ist nicht möglich zwischen den Anwendungen der jeweiligen Endstelle zu unterscheiden, was aus Sicherheitsgründen bedauerlich ist.

1.2 SSL/TLS

Als Alternative zum VPN hat sich für Webseiten SSL/TLS mit PKI in allen etablierten Webbrowsern (ISO/OSI Schicht 4) durchgesetzt.

1.3 Proxy

Eine weitere Alternative sind Proxylösungen (ISO/OSI Schicht 4/5), meist auf dem SOCKS-Protokoll basierend. Beispielsweise kann mittels SSH (z.B. Putty) eine sichere Verbindung mit SOCKS Proxy hergestellt werden. Hierfür ist allerdings eine Proxyunterstützung der Anwendungssoftware notwendig, sowie die Installation und Konfiguration von SSH.

1.4 Integration in Anwendungen

Eine Integration von Verschlüsselung in Anwendungen durch den Anwendungsentwickler ist mit der Gefahr von Implementationsfehlern verbunden. Der Aufwand bleibt durch regelmäßiges Reagieren bei Sicherheitsproblemen sowie beim Bekanntwerden von neuen Schwachstellen auch nach der Implementation dauerhaft hoch.

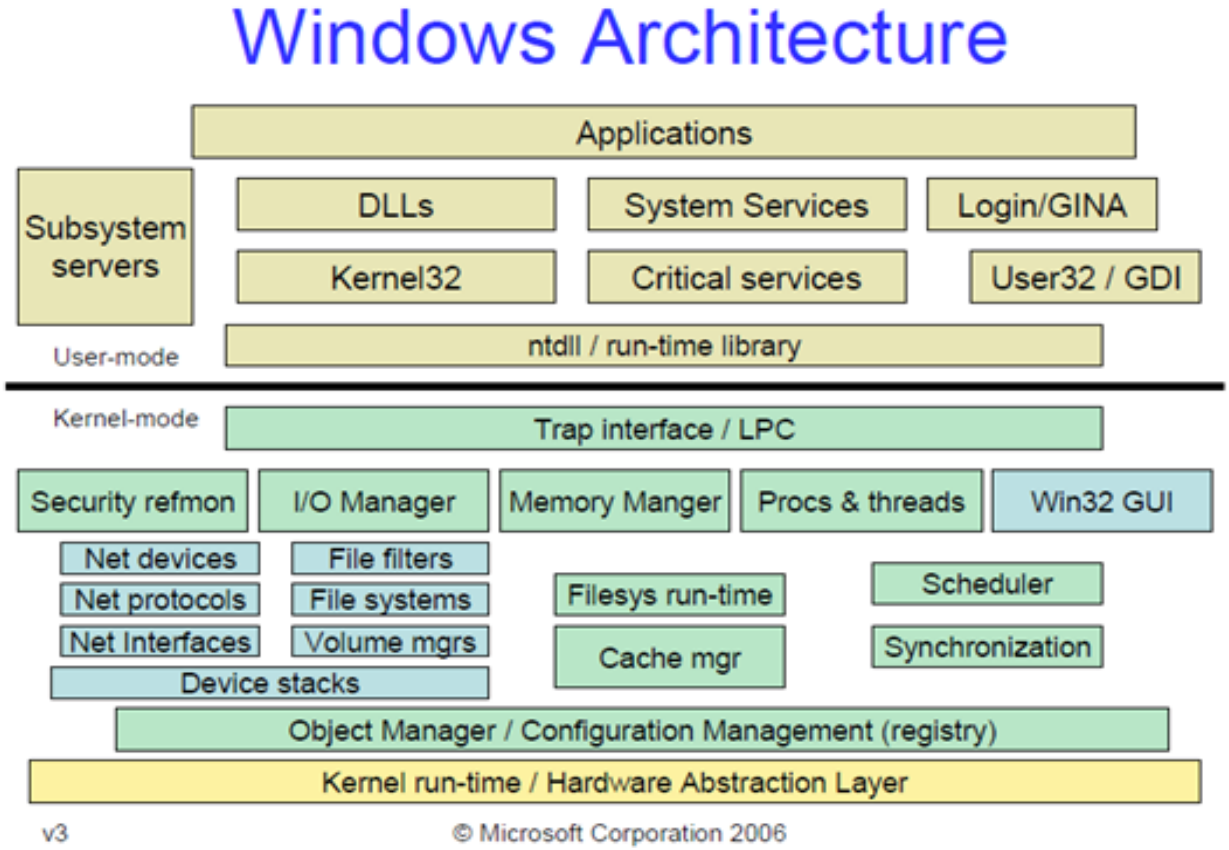
2 Idee

Wie in *1 Stand der Forschung/Technik* beschrieben, basiert in etablierten Betriebssystemen der Remoteaccess für Anwendungen überwiegend auf VPN. Andere Technologien haben sich nur in Kombination mit Anpassungen der jeweiligen Anwendung etablieren können. Dies ist mit Aufwand und Risiken verbunden, nicht generalisierbar sowie nicht für jede Anwendung anwendbar, insbesondere nicht wenn deren Quelltext nicht verfügbar ist.

2.1 Voraussetzungen unserer Idee

Unsere Lösung greift die Daten der Anwendungen bereits auf Sitzungsschicht (ISO/OSI Schicht 5) ab, bevor diese vom Betriebssystem in eine paketorientierte Form (ISO/OSI Schicht 3 und 4) umgewandelt worden sind. Die Schnittstellen der Anwendung zum Betriebssystem (Benutzermodus -> Kernel Modus) werden hierzu zur Laufzeit unter der Zuhilfenahme von Einschubmethoden (Hooking) abgegriffen. Unsere Lösung erhält über diesen Weg die Betriebssystemaufrufe der Anwendungen zur Datenübermittlung, und kann diese ableiten oder, wenn keine Ableitung gewünscht oder notwendig ist, transparent an das Betriebssystem durchreichen.

Um dies genauer zu verdeutlichen, hilft es die Windowsarchitektur zu betrachten: Unsere Lösung setzt im Bild beim Block „Applications“ bei den verschiedenen darunter aufgeführten Bibliotheken der Win 32 API im Benutzermodus (User-mode) an.



Microsoft Corporation 2006, http://resources.infosecinstitute.com/windows-architecture-and-userkernel-mode/, abgerufen am 13.01.2016.

Wir haben unseren Ansatz für das Betriebssystem Windows der Microsoft Corporation umgesetzt. Da sich die Betriebssystemschnittstelle der Anwendungen (Win32 API) durch die Hybridkernel Architektur von Windows (NT 3.1 bis 10) im flüchtigen Speicherbereich der jeweiligen Anwendung selbst befindet (Benutzermodus), kann auf diese nicht nur zugriffen werden sondern diese auch verändert werden. Hierzu sind keine Administrationsberechtigungen notwendig, auch stellt dieser Eingriff keine persistente Veränderung des Clientsystems dar.

Diese gesamte Vorgehensweise wird bereits von Software anderer Hersteller verwendet, und ist in der Informatik unter der Bezeichnung von Einschubmethoden (Hooking) bekannt.

2.2 Unsere Leistung

Auf diesem Weg können wir mittels besagten Einschubmethoden (Hooking) zur Laufzeit die Aufrufe der jeweiligen Anwendung an die Betriebssystem API (Win32 API) abfangen und selbst verarbeiten, an das Betriebssystem transparent durchreichen oder an ein entferntes Netzwerk übertragen. Bestehende Lösungen wandeln die Verbindung, analog zum Betriebssystem, bereits am Client in einen paketorientierten Datenstrom (ISO/OSI Schicht 3) um, und übertragen diesen in dieser Form an das entfernte Netzwerk.

Die abgegriffenen Aufrufe, die nicht transparent an das Betriebssystem durchgereicht werden sondern zum entfernten Netzwerk übertragen werden, werden hingegen von uns auf wenige generalisierte Vorgänge vereinheitlicht, die insbesondere den Verbindungsaufbau sowie das Versenden und das Empfangen von Daten darstellen. Zudem erfassen wir hier DNS-Anfragen. Diese Aufrufe übertragen wir, anders als andere Softwarehersteller, über SSL/TLS mit eigener PKI an einen Server im entfernten Netzwerk. Dies ist als RPC ähnlicher Mechanismus vorstellbar. Erst hier, im entfernten Netzwerk, wird aus den abgefangenen Aufrufen wieder eine paketorientierte TCP/IP Verbindung oder eine paketorientierte DNS-Anfrage (UDP/IP).

Da es durch den Integrity Mechanism unter Windows keine Möglichkeit gibt, nicht betriebssystemeigene DLLs zu laden, scheidet dieser Weg aus um in den Speicherbereich eines entsprechend geschützten Prozesses einzugreifen. Darum haben wir hierzu einen innovativen Weg entwickelt, um dies dennoch zu ermöglichen. Auch hierdurch unterscheiden wir uns von anderen Herstellern deutlich.

Die Anfragen der Anwendungen an die Betriebssystem API zu verarbeiten ist eine fehleranfällige und aufwändige Herausforderung, deren Lösung wir aus Betriebsgeheimnisgründen in diesem Dokument nicht weiter ausführen. Unsere Leistung besteht insbesondere darin, dass sich unsere über Einschubmethoden (Hooking) eingehängte Softwareschicht für die Anwendungen genauso verhält wie die Betriebssystemschnittstelle selbst. Hierzu müssen auch alle nicht standardkonformen oder in den Dokumentationen unkorrekten oder nicht abgedeckten Verhaltensweisen nachgebildet werden. Dies stellt insbesondere an das Testen sowie das Nachvollziehen von Problemen hohe Anforderungen und bedeutet hohen Aufwand. Uns ist keine andere Implementation bekannt, die sowohl die Windows 32 Bit als auch 64 Bit Plattform unterstützt oder neuere Windows API Calls, die in Windows Vista eingeführt worden sind, stabil behandelt.

2.3 Vorteile

Durch unsere Lösung ergeben sich folgende technische Vorteile:

2.3.1 Erweiterte Routingfunktionalität

Pro Verbindung einer Anwendung kann am Client die Entscheidung getroffen werden, wie diese verarbeitet werden soll. Es ist beispielsweise möglich, dass die Anwendung Firefox für eine IP *a* über den Gateway *A* läuft, die Anwendung Chrome für die IP *a* über das

Gateway *B* läuft und die Anwendung Internet Explorer beim Versuch auf die IP *a* zuzugreifen geblockt wird. Das löst das Problem das sich ergibt, wenn ein IP-Netz mehrfach vergeben wurde.

Es ist beispielsweise auch möglich die Verbindungen ins Internet zu blockieren, solange man Zugriff auf das Firmennetzwerk hat.

2.3.2 Steigerung der Übertragungsgeschwindigkeit

Bei unserer Lösung werden, anders als bei VPN, nicht viele parallele TCP/IP Verbindungen aufgebaut, die jeweils eine eigene Congestion Control unterhalten, sondern nur eine Einzelne. Dies führt dazu, dass nur eine einzige Congestion Control arbeitet und hierbei keine destruktiven Wechselwirkungen auftreten, die sich bei mehreren Verbindungen zwangsweise ergeben. Dies resultiert in einer besseren Ausnutzung der verfügbaren Übertragungsleistung, insbesondere über Mobilfunk.

2.3.3 Überbrückung von Verbindungsabrissen

Da sich die Betriebssystemschnittstelle, die wir abfangen, auch für die Sicherung der Übertragung verantwortlich, ist es möglich auch Verbindungsabrisse intelligent zu überbrücken, oder das Übertragungsmedium zu wechseln. Dies deckt zum Teil Szenarien von Multipath-TCP ab.

3 Nutzen

Unsere Lösung stiftet grundsätzlich einen vergleichbaren Nutzen den ein VPN bietet, allerdings mit zahlreichen Vorteilen. Insbesondere aus Sicht der IT-Sicherheit wird einiges verbessert.

3.1 Filtern von Anwendungsdatenverbindung statt Paketen

Bei einem Fernzugriff per VPN wird eine Netzwerkkopplung geschaffen, die erst auf Paketebene (ISO/OSI Level 3) aufwändig und mit Fachwissen nicht nur geroutet sondern auch gefiltert werden muss. Eine falsche oder nicht ausreichend spezifische Firewall-Regel kann dazu führen, dass über die Netzkopplung unerwünschter Datenverkehr in Richtung des entfernten Netzwerks möglich wird. Kleine Fehler haben hier schnell große Auswirkungen, insbesondere da bei Paketen die dahinterliegende Anwendung sowie das Endgerät nicht unterschieden werden kann. Dies kann zu gravierenden Sicherheitsproblemen führen, die oft erst im Falle eines erfolgreichen Angriffs auffallen.

Ein Vorteil unserer Lösung ist, dass nicht der gesamte Netzwerkverkehr aller Anwendungen eines Endgerätes übermittelt werden muss, sondern der Client konfigurierbar selektiv Verbindungen übertragen kann. Zudem wird bei jeder übertragenen Verbindung die Signatur der Anwendung übermittelt, so dass auch auf der entfernten Seite hiernach gefiltert werden kann. So haben unerwünschte Anwendungen keinen Zugriff, und können unberechtigte Dienste gar nicht erst adressieren, während die erlaubten Anwendungen einfach zugreifen können.

3.2 Einfachere Spezifizierbarkeit von Datenverkehr

Um einen Fernzugriff über unsere Lösung sicher betreiben zu können, wird kein Netzwerkspezialist benötigt, der sich mit allen Details von TCP/IP auskennt. Dadurch, dass, im Gegensatz zu VPN Paketen, bei jeder Verbindung die Endstelle und die Anwendungssignatur verfügbar ist, können anwendungsbezogene Zugriffsberechtigungen statt protokollspezifische Filterregeln vorgenommen werden, die effektiv und einfach zu verstehenden sind. Details der darunterliegenden Protokollen wie ICMP oder TCP-Flags sind zur Berechtigung bedeutungslos, da diese nicht von extern beeinflusst werden können.

3.3 Vereinfachtes Handling und robuste Funktion

Durch den Wegfall der Netzwerkkopplung ergeben sich zwei weitere Vorteile: Einerseits muss auf der Endstelle keine Programminstallation mit Administrationsrechten erfolgen. Stattdessen arbeitet unsere Software mit einfachen Benutzerrechten, und kann beispielweise über einen USB-Stick von PC zu PC mitgenommen und verwendet werden. Eine lokale Konfiguration ist ebenfalls nicht notwendig, da alle relevanten Konfigurationsparameter direkt vom Server beim Verbinden bezogen werden. Durch diese OneClick-Technologie ist eine Fehlbedienung durch den Endanwender nahezu ausgeschlossen. Der zweite Vorteil ist die Umgehung von VPN-typischen Problemen wie Routing- und Installationsproblemen auf dem Client: Unsere Software entscheidet vor dem Betriebssystems wie eine Verbindung zu behandeln ist, und dies bevor eine Fehlkonfiguration des Betriebssystems eine Auswirkung entfalten kann.

4 Marktchancen

Das Produkt CryptoApp Tunnel ist seit Anfang 2016 auf dem Markt.

Durch die politische Situation in den Vereinigten Staaten von Amerika (PatriotAct, NSA-Skandal, u.ä.) wird von zahlreichen deutschen und europäischen Unternehmen davon ausgegangen, dass die USA unter anderem Wirtschaftsspionage in Europa betreiben. Vor diesem Hintergrund bestehen große Vorbehalte gegenüber Softwareanbietern aus den USA - speziell im Bereich IT Security. Da unsere Softwareentwicklung komplett in der Bundesrepublik Deutschland stattfindet, können wir für unsere Kunden darstellbar sicherstellen, dass unsere Software frei von Hintertüren jedweder Art ist. Die Tatsache, dass die CryptoMagic GmbH in keiner Weise an US-Amerikanisches Recht gebunden ist, hat sich bereits im Rahmen der derzeitigen Verkaufsverhandlungen als großer Verkaufsvorteil erwiesen.

Besonders durch die verstärkte mediale Berichterstattung über Security-Themen seit den Snowden-Enthüllungen rückt dieses Themenfeld zunehmend in den Fokus von kleinen und mittelständischen Unternehmen. In deren Umfeld existiert oft nicht das Know how um eine komplexe VPN/Firewall-Struktur aufzubauen und zu warten. Durch die sehr simple und intuitive Bedienungsoberfläche von CryptoApp Tunnel können wir diesen Unternehmen eine hochsichere und dennoch einfach zu wartende Lösung anbieten, auf einem Niveau welches derzeit auf dem Markt nicht verfügbar ist. Hierfür kommen Unternehmen mit Mitarbeitern im Home-Office oder im Außendienst in Frage, die einen sicheren Zugang zum Firmennetzwerk benötigen. Eine weitere Zielgruppe sind Unternehmen, die mit sensiblen Kundendaten hantieren (Steuerberater, Rechtsanwälte, Ärzte, etc.). Für diese Kundengruppe wird ein spezielles Lizenzmodell und technische Lösung angeboten, die es ihnen ermöglicht die CryptoApp Tunnel Software und deren kryptografisches Material vor dem Abhören und Veränderung geschützt an ihre Kunden auszuhändigen um eine sichere Verbindung zur Datenübertragung aufzubauen. Auf diesem Weg können beispielsweise ärztliche Befunde auf sicherem Weg zum Patienten übertragen werden oder anwaltliche Dokumente an deren Mandanten sowie umgekehrt.