

Netviewer Admin Sicherheit

Dieses White Paper beschreibt die Sicherheitsmechanismen von Netviewer Admin. Im ersten Teil des Dokuments liegt der Fokus auf der Netzwerktransportschicht. Der zweite Teil beschreibt die Sicherheitsmechanismen auf der Applikationsschicht.

Sicherheit auf der Netzwerktransportschicht

Die Sicherheitsmechanismen der Transportschicht stellen die Grundlage einer sicheren Kommunikation dar. Im Folgenden wird beschrieben, wie Netviewer Admin die verwendeten Kommunikationskanäle durch gegenseitige Authentifizierung und Verschlüsselung schützt.

Aufbau einer Sitzung

Der grundsätzliche Prozess des Sitzungsaufbaus bei Netviewer Admin wird in Abbildung 1 dargestellt und im Folgenden beschrieben.

Voraussetzung für den Sitzungsaufbau ist die Installation des Netviewer Admin Host Programms auf dem Host-Computer. Alternativ kann der Admin Host auch als Applikation betrieben werden. Nachdem der Host sich erfolgreich mit Benutzernamen, Passwort und dem Lizenzschlüssel authentifiziert hat, sendet er in regelmäßigen Abständen einen Ping zum Vermittlungsserver (ConnS) und wartet auf Antwort ①.

Nachdem der Administrator sich am Master-Programm authentifiziert hat, kann er jederzeit mit einem Doppelklick im Master-Programm eine Admin-Sitzung auf dem gewünschten Host-Computer starten. Dazu muss er den Schlüsselsatz des Hosts eingeben. Der Schlüsselsatz ist eine acht- bis 16-stellige Zahl, welche als Zugriffsbeschränkung für einen bestimmten Host dient. Nach der Eingabe des gültigen Schlüsselsatzes kontaktiert das Master-Programm den Vermittlungsserver (ConnS), um eine Sitzung anzufordern ②. Nachdem der Master erfolgreich am Vermittlungsserver authentifiziert wurde (über Benutzername und Passwort oder Active Directory), übermittelt dieser dem Master die Adresse eines Kommunikationsservers ③. Der Master kontaktiert dann den Kommunikationsserver und

wartet darauf, dass der Host in die gestartete Sitzung eintritt ④.

Der Vermittlungsserver gibt die Information, dass der Master eine Sitzung angefordert hat, bei der nächsten Antwort auf einen Ping an den Host weiter ⑤. Der Host sendet eine Anforderung an den Vermittlungsserver ⑥. Dieser sendet die Adresse des Kommunikationsservers, an dem der Master wartet, zurück ⑦. Das Host-Programm kontaktiert den Kommunikationsserver ⑧. Die Verbindung zwischen Master und Host ist damit über den Kommunikationsserver hergestellt ⑨.

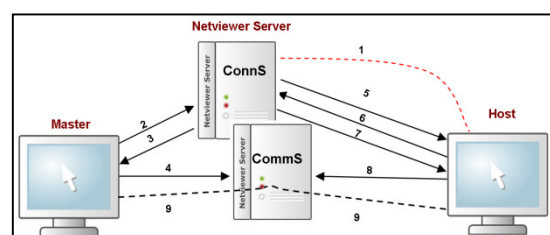


Abbildung 1

Der Vermittlungsserver und der Kommunikationsserver sind unabhängige Entitäten. Der Signalisierungsdatenstrom (z.B. Authentifizierung, Schlüsselaustausch) und der Sitzungsdatenstrom sind logisch voneinander getrennt.

Verschlüsselungsmethoden

Die gegenseitige Authentifizierung zwischen den Netviewer Clients und den Netviewer Servern erfolgt über ein asymmetrisches Verschlüsselungsverfahren. Der öffentliche und der private Schlüssel werden beim Erstellungsprozess der Software einkompiliert. Zusätzlich besitzen Master und Host den acht- bis 16-stelligen Schlüsselsatz, den der Administrator bei der Installation des Hosts individuell gewählt hat.

Das Master-Programm und der Host verwenden den öffentlichen Schlüssel des Servers und ihren eigenen privaten Schlüssel. Der Server verwendet seinen eigenen privaten Schlüssel und den öffentlichen Schlüssel der Clients. Die Geheimhaltung und die Integrität der Daten ist durch zwei Verschlüsselungsmethoden gesichert: ECC (Elliptic Curve Cryptography) und Blowfish. Die asymmetrischen 160-Bit ECC Keys werden zur Authentifizierung und zum Schlüsselaustausch verwendet.

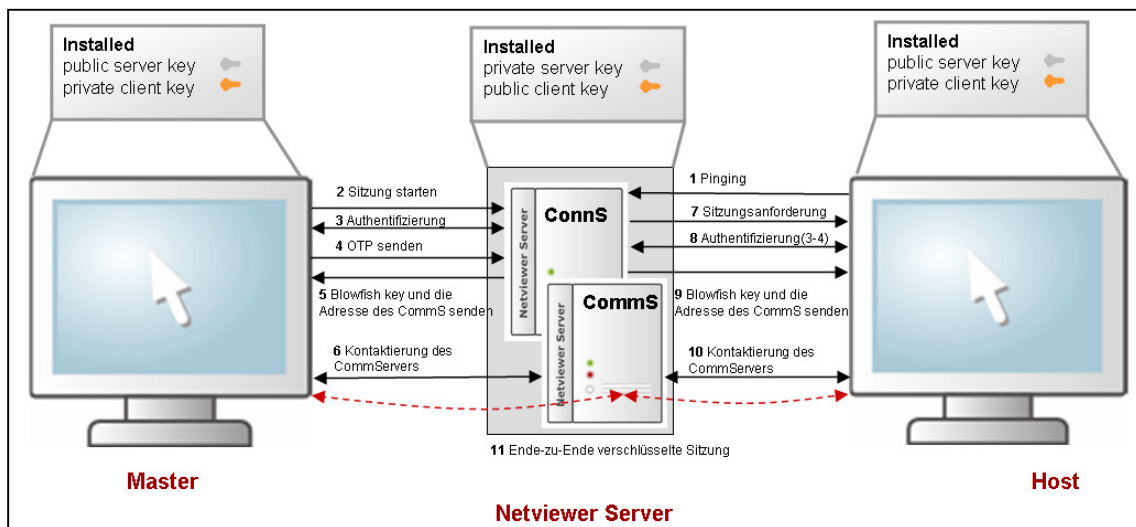


Abbildung 2

Der symmetrische 128-Bit Blowfish Key sichert die integere und vertrauliche Kommunikation zwischen Master und Host.

Der folgende Abschnitt beschreibt den Sitzungsaufbau hinsichtlich der Verschlüsselungsmethoden. Dies ist visualisiert in Abbildung 2.

Der Host sendet in regelmäßigen Abständen einen Ping zum Vermittlungsserver, um seine Anwesenheit zu signalisieren ①. Wenn keine Anforderung seitens des Masters vorliegt, fährt der Client fort, Pings an den Server abzusetzen. Wenn der Master eine Sitzung anfordert ②, authentifizieren sich Master und Vermittlungsserver gegenseitig über die asymmetrischen ECC-Schlüssel und Zufallszahlen ③.

Der Master generiert dann ein OTP (One Time Pad) und sendet es verschlüsselt an den Vermittlungsserver (Conns) ④.

Der Vermittlungsserver entschlüsselt das OTP, generiert einen symmetrischen Blowfish Key und übermittelt ihn zusammen mit der Adresse des CommS über einen sicheren Kanal als XOR-Kombination von OTP und Blowfish Key an den Master ⑤.

Der Master kontaktiert den Kommunikationsserver und wartet dort auf den Host ⑥.

Der Vermittlungsserver informiert den Host über die Anforderung der Sitzung, wenn er den nächsten Ping des Hosts beantwortet ⑦.

Das Host-Programm kontaktiert den Vermittlungsserver zur gegenseitigen Authentifizierung und zum Schlüsselaustausch ⑧.

Der Authentifizierungsprozess entspricht dem des Masters (Schritte ③-④). Der Vermittlungsserver sendet den Blowfish Key und die Adresse des Kommunikationsserver, der für die Sitzung verwendet wird, an den Host ⑨.

Der Host kontaktiert den CommS ⑩ und tritt in Verbindung mit dem Master, der bereits dort wartet.

Nach dem Start der Sitzung zerstören Master und Host den Blowfish Key und erzeugen unter Verwendung des Schlüsselsatzes, der während der Installation definiert wurde, einen neuen. Die sichere Ende-zu-Ende verschlüsselte Sitzung ist damit hergestellt (11).

Sicherheit auf der Applikationsschicht

Auf der Applikationsschicht bietet Netviewer verschiedene technologie- und prozessgestützte Sicherheitsmechanismen, anhand welcher der Sicherheitsgrad der Software an unterschiedliche Anforderungen anpassbar ist. Viele der folgenden Funktionen lassen sich individuell konfigurieren.

Beim Sitzungsaufbau

Die Master- und die Host-Software ist mit einem von der unabhängigen Zertifizierungsstelle VeriSign ausgestellten Zertifikat signiert. Zum Starten des Master-Programms muss sich der Administrator mit einem Benutzernamen und einem Passwort authentifizieren. Nach der erfolgreichen Authentifizierung muss der Administrator den Schlüsselsatz eingeben, um auf einen bestimmten Host zugreifen zu können. Wenn sich der Administrator mit einem Host verbindet, bestehen drei Möglichkeiten. Der Host kann sich in einem der folgenden Status befinden:

a) Ein Benutzer ist am Host-Computer angemeldet.

Wenn der Berater eine Admin-Sitzung startet und ein Benutzer ist auf dem Host-Computer angemeldet, muss der angemeldete Benutzer den Zugriff auf seinen Computer explizit erlauben. Die Bildschirmübertragung und die Fernsteuerung ist für den Master erst verfügbar, wenn der Host zugestimmt hat. Vorher sieht der Administrator nur einen schwarzen Bildschirm. Der Administrator hat die gleichen Berechtigungen und Einschränkungen wie der angemeldete Benutzer. Um weitere Rechte zu erhalten (z.B. um Zugriff auf bestimmte Dateien zu erhalten), kann der Administrator den Benutzer während der Sitzung wechseln. Der am Host angemeldete Benutzer kann die Admin-Sitzung jederzeit beenden.

b) Der Host-Computer ist gesperrt.

Der gesamte Bildschirm ist sichtbar, jedoch muss der Host-Computer zunächst entsperrt werden. Der Administrator kann sich mit seinem Administrator-Account oder dem Account des lokalen Benutzers anmelden. Die Berechtigungen des Administrators hängen vom verwendeten Benutzer-Account ab.

c) Der Host-Computer ist abgemeldet.

Der Windows Login-Dialog ist auf dem Bildschirm sichtbar. Der Administrator kann sich mit seinem Administrator-Account oder dem Account des lokalen Benutzers anmelden. Die Berechtigungen des Administrators hängen vom verwendeten Benutzer-Account ab.

Während einer Sitzung

Der Schutz der Privatsphäre des Benutzers am Host-Computer und seiner persönlicher Daten ist während einer Netviewer Admin-Sitzung durch verschiedene Funktionen und Einstellungen sichergestellt. Ist ein Benutzer auf dem Host-Computer angemeldet, muss dieser Aktionen des Masters auf seinem Computer (z.B. einen Dateitransfer) erlauben.

Es ist möglich einen Wartebildschirm anzuzeigen, während der Master auf dem Host-Computer arbeitet. Dies ist hilfreich, wenn der Master vertrauliche Arbeiten durchführt (z.B. Eingabe von Lizenzschlüsseln).

Der Kommunikationsserver ist zu keiner Zeit imstande, auf die Sitzungsdaten zuzugreifen, da diese Ende-zu-Ende verschlüsselt sind.

Protokollierung und Aufzeichnung

Das Master-Programm erzeugt am Ende der Sitzung eine TXT-Datei, welche unter anderem die Sitzungsdauer und die Anzahl der übertragenen Bytes protokolliert. Die Sitzungsdaten können alternativ als CSV-Datei (z.B. zur weiteren Verwendung zur Abrechnung) auf Master- und/oder Host-Seite protokolliert werden. Zusätzlich werden alle statistischen Sitzungsdaten serverseitig geloggt.

Alle Sitzungsdaten inklusive Video- und Audiodaten können aufgezeichnet und im Netviewer-eigenen Format NVL gespeichert werden. NVL-Dateien können manuell in das Dateiformat ASF konvertiert werden.

Zusammenfassung

Die Sicherheit von Netviewer Admin und die Integrität der übertragenen Daten wird durch die Verwendung verschiedener Sicherheitsmechanismen garantiert:

- Netviewer Admin ist mit dem Netviewer Zertifikat signiert, welches durch eine unabhängige Zertifizierungsstelle (VeriSign) ausgestellt wurde.
- Ein 160-Bit ECC-Schlüssel wird zur gegenseitigen Authentifizierung und zur asymmetrischen Verschlüsselung zwischen Client und Server verwendet.

- Ein 128-Bit Blowfish Key wird zur Verschlüsselung der Sitzungsdaten verwendet.
- Der Master und der Host verwenden den acht- bis 16-stelligen Schlüsselsatz, um den Blowfish Key zu erzeugen, der zur Verschlüsselung der Sitzung verwendet wird. Der Schlüsselsatz wird während der Installation des Hosts individuell definiert.
- Der Vermittlungsserver und der Kommunikationsserver sind unabhängige Entitäten.
- Der Blowfish Key, mit dem die Sitzungsdaten verschlüsselt werden, ist dem Kommunikationsserver nicht bekannt.
- Alle Sitzungen sind Ende-zu-Ende verschlüsselt.
- Alle Sitzungsdaten können zur späteren Revision aufgezeichnet werden.

Version 1.4 - Dezember 2009

Bezug auf Server- und Client Version: G3.1

© 2009 Netviewer AG. Netviewer Support, Meet, Admin, Server, und das Netviewer Logo sind eingetragene Marken der Netviewer AG. Alle Rechte vorbehalten. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.