Fernwartung mit VNC

Der Dezentralisierung von rechnergestützten Arbeiten bzw. der erforderlichen Mobilität der Mitarbeiter entspricht eine ganze Reihe von Programmen, die einerseits der Fernwartung von Rechnern dienen und andererseits dem Benutzer den Zugriff auf seine gewohnte Arbeitsumgebung von beliebigen Plätzen rund um den Globus gestatten sollen. Dass ein solches Progamm billig, ressourcenfreundlich und in hohem Maße portabel sein kann, beweisen die AT&T Laboratories Cambridge mit ihrer Entwicklung VNC (Virtual Network Computing). Dabei handelt es sich um ein sehr schlankes Open-Source-Tool für den Fernzugriff auf graphische Benutzeroberflächen, dessen Binaries und Quellcode (C++) unter http://www.uk.research.att.com/vnc *zum kostenlosen Download bereitstehen.*

Seit Sommer 2000 ist ein Teil der Rechner im Verwaltungsnetz der HU – die PCs der Beschaffungsstelle in der Hannoverschen Straße – mit einem Programm versehen, das die Fernwartung vom Rechenzentrum aus gestattet.

Sparsames Design

Generell bestehen Fernkonsolen aus zwei Komponenten – einer Client- und einer Serverkomponente. Ein Konzept in der Ausführung dieser Komponenten besteht darin, die Anforderungen an Soft- und Hardware auf der Clientseite möglichst gering zu halten. Man nennt dies *Thin-Client-Architektur*. Darüber hinaus speichern ‚dünne' Clients möglichst wenige oder gar keine Informationen über den gegenwärtigen Zustand des Servers – etwa irgendwelche Desktopeinstellungen oder Informationen über auf dem Server geöffnete Programme. Im Idealfall – wie das für VNC gilt – kann man mit der Thin-Client-Software auf Diskette um die Welt reisen und auf nahezu jeden Rechner, der über Internetzugang verfügt, den Desktop des heimischen bzw. des Arbeits-PC zaubern, um dort alles so vorzufinden, wie man es beim letzten Login auf dem Rechner daheim zurückgelassen hatte: mit allen laufenden Programmen, geöffneten Dokumenten etc. Das Beenden der Sitzung auf dem Client oder ein Crash desselben lässt die Applikationen auf dem Server völlig unberührt. Mit einem solchen Client bewaffnet, kann man beliebige Rechner oder PDAs in ein Terminal verwandeln. Verfügt die Serverkomponente noch dazu über einen integrierten Web-Server – und auch das trifft auf VNC zu –, kann man sich auch die Diskette sparen und mit seinem heimischen Desktop in jedem javafähigen Browser kommunizieren (Abbildung 1).

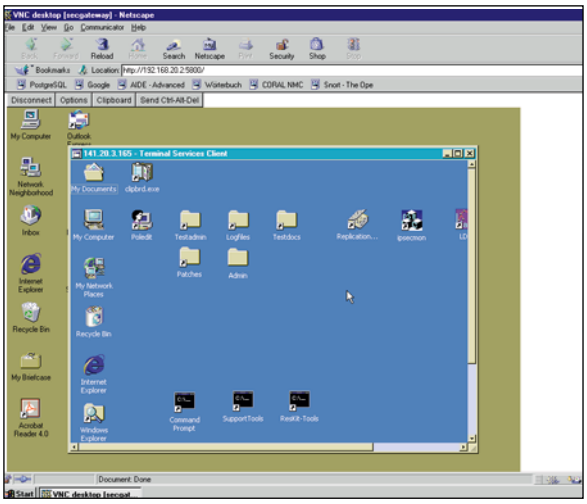

Abb. 1: Windows 2000 Server im Terminal Services Client unter NT – das Ganze per VNC im Browser einer dritten Maschine

Der VNC-Client – der Viewer – besteht aus einer einzigen Datei, welche in der Windows-Version etwa 170 kB umfasst. Daneben gibt es Viewer für X, Windows CE, für Macintosh sowie einen Java-Viewer. Wem dies nicht genügt, der mag sich unter *http://www.uk.research.att.com/vnc/platforms.html* die Viewer seiner Wahl herunterladen. Diese sind dann allerdings nicht von den VNC-Autoren geschrieben, sondern von Anwendern.

VNC-Server gibt es nicht so zahlreich. In den AT&T Laboratories wurden Versionen für X, für Win32 sowie für PowerPC mit MacOS ab Version 7.1 entwickelt. Die Installationsdateien für den Win32-Server (WinVNC) passen bei dem in der Universitätsverwaltung eingesetzten Release mit ca. 1 MB auch auf eine Diskette. Wer unter Windows – von chaotischen DLL-Verhältnissen im Systemverzeichnis genervt – lieber von weiteren Installationen auf seinem gerade mal ordentlich arbeitenden System absieht, wird angenehm überrascht. Der VNC-Viewer benötigt überhaupt keine Installation und läuft sogar von Diskette. Bei der Installation des Servers wird eine einzige DLL in das Systemverzeichnis kopiert, und die Anzahl der Eintragungen in der Systemregistrierung hält sich in Grenzen. Sie sind überdies dokumentiert. Die Windows-Version läuft stabil und kann ohne besondere Anforderungen an die Bibliotheken des Betriebssystems unter NT 3.51 und Windows 95 genauso eingesetzt werden wie unter Windows 2000.

VNC-Server und -Viewer kommunizieren über ein bestimmtes Protokoll unabhängig davon, unter welchem Betriebssystem die eine oder andere Komponente läuft. Wenn Sie also der Meinung sind, unter DOS auf Ihrem Mac arbeiten zu müssen[1], oder wenn Sie unter Linux Ihren NT-Server administrieren wollen,

1 Ich habe das nicht ausprobiert, aber den Viewer für DOS samt TCP/IP- und Graphikbibliothek gibt es unter der angegebenen Adresse.

stellt das für VNC kein Problem dar. VNC läuft über jedes zuverlässige Netzwerkprotokoll. Allerdings sind die Implementationen der AT&T Laboratories sämtlich für TCP/IP ausgelegt.

Das zu Grunde liegende Protokoll, das VNC-Protokoll, auch RFB (Remote Frame Buffer) -Protokoll genannt, arbeitet mit dem Framebuffer, dem Bildwiederholspeicher der Grafikkarte. Die Hauptlast trägt dabei der Server. Er aktualisiert über das Netz den Framebuffer, der auf einem Client angezeigt wird. Diese Daten werden vom Server quasi in einen VNC-Dialekt verpackt (ein Codierungsschema, das zugleich für Kompression sorgt), der vom Client zurückübersetzt und direkt oder über das Betriebssystem in den Framebuffer geschrieben wird. Es gibt verschiedene Arten, wie diese Daten verpackt werden und vor allem wann die Ausgabe auf dem Client zu aktualisieren ist. Dabei sollen Rechenzeit auf dem Server und Bandbreite bei der Übertragung gespart werden.

Codierungsschemata und Updatehandling

Wie bei jeder Client-Server-Interaktion müssen beide Parteien am Beginn und während der Kommunikation die Modalitäten des Datenaustausches vereinbaren. Das erfolgt zwar automatisch, doch hat der Nutzer hier die Möglichkeit einzugreifen.

Die Grundinformation, die der Server bereitstellt, besteht in der Angabe einer X,Y-Koordinate, an der der Client ein Rechteck von n Pixeln zeichnen soll, wobei die Pixeldaten die Farbinformation für jedes einzelne Pixel umfassen. Bei der einfachsten Codierung, dem *raw encoding*, folgen die einzelnen Pixelinformationen in der Reihenfolge von links nach rechts, wie sie auf dem Server liegen. Alle VNC-Server und -Viewer müssen diese Codierung, welche das Netz am meisten belastet, unterstützen.

Nun ist es aber möglich, dass der Client diese Daten schon irgendwo in seinem Speicher hat, etwa wenn nur ein Fenster verschoben oder gescrollt wird. Dann übermittelt der Server nur die Koordinate, von der der Client das zu zeichnende Rechteck aus seinem Framebuffer kopieren soll (*copy rectangle encoding*).

Eine weitere Möglichkeit besteht in der Zerlegung eines Rechteckes in kleinere Rechtecke von Pixeln mit gleichem Wert, wobei dann nur die Anfangskoordinaten, Länge und Breite sowie die Beschreibung eines Pixels für das betreffende Rechteck zu übermitteln sind (*rise and run length encoding*).

Die Autoren des Programmes weisen darauf hin, dass man ebenso gut JPEG encoding oder MPEG implementieren kann, wenn man VNC in speziellen Umgebungen einsetzt. Wesentlich ist nur, dass sowohl der Server als auch der Viewer die Codierungsschemata unterstützen müssen.

Neben der Codierung der Daten wird Rechenleistung und Bandbreite dadurch gespart, dass man dem Server

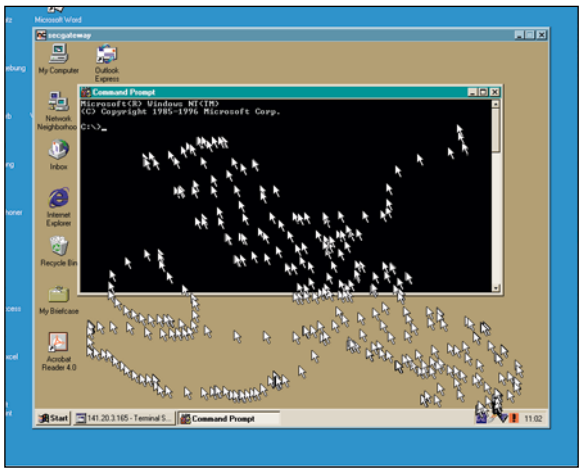

Abb. 2: Der Command Prompt auf dem Remote-PC läuft im Vollbildmodus

mitteilt, für welche Bereiche des Bildschirmes er Updates auf dem Client vornehmen soll, etwa für den ganzen Bildschirm, für das Vordergrundfenster, für das Fenster unter dem Mauszeiger oder ausschließlich für Textkonsolen. Oder es erfolgen Updates nur auf ein bestimmtes Ereignis hin, einen Mausklick oder Tastendruck vom Client. Das Update-Verfahren liegt in der Hand des Servers. Jedoch lösen Tastatur- und Mausereignisse eine Aktualisierungsanforderung seitens der Client-Maschine aus. Diese Einstellmöglichkeit sollte man nutzen, wenn nur wenig Netzwerkbandbreite zur Verfügung steht und der Server seine Updates nicht nach eigenem Gutdünken über das Netz schicken soll, sondern nur auf Anforderung. Auch wenn in Word längere Texte gescrollt werden und die Updates nicht hinterher kommen, sollte man hin und wieder mal per Mausklick „nach dem Rechten sehen“. Das Markieren von Text kann übrigens ebenfalls zur Geduldsprobe werden. Am störrischsten aber verhalten sich Textkonsolen, so z. B. beim FTP über die MS-DOS-Eingabeaufforderung. Hier hilft häufig nur mutiges Drauflosschreiben und Abschicken der Daten ins Blaue hinein, da die Eingaben – etwa ein Benutzername oder ein Verzeichniswechsel – noch nicht angezeigt werden. Das RETURN auf der Tastatur sorgt dann für ein Update. Gerät man mit der DOS-Konsole auf dem Server jedoch zufällig in einen Vollbildmodus, hilft auch das nicht mehr. Das Viewer-Fenster ist eingefroren und in der verwaisten Ansicht des Konsolenfensters auf dem Client zieht der Mauszeiger Spuren (Abbildung 2).

Hier schafft ein kurz entschlossenes ALT+RETURN seitens des Clienten Abhilfe, in dem es den Server aus dem Vollbildmodus zurückholt. Reine Textkonsolen sind inkompatibel zu dem RFB-Protokoll, es gibt also keine VNC-Server dafür (wohl aber Viewer, wie den schon genannten Viewer für DOS).

VNC überwacht auf dem Server die Nachrichten, die eine Anwendung empfängt, wenn sie ihr Fenster

aktualisieren soll. Über ein Finetuning, das man allerdings direkt in die Windows-Registry schreiben muss, kann man je nach Windows-Applikation festlegen, welche Nachrichten von VNC überwacht werden sollen und welche nicht (z. B. WM_PAINT, WM_TIMER, KeyPress bzw. verschiedene Maus-Events). Im Gegensatz zu den oben genannten Codierungsschemata hängt das Updatehandling aber stark vom Betriebssystem ab und ist deshalb von Implementation zu Implementation unterschiedlich.

Die Arbeit mit VNC

Die in der Beschaffungsstelle eingesetzte Installation läuft ohne Rücksicht auf diese Feinheiten mit den Default-Einstellungen. VNC wird dabei als reine Wartungsanwendung genutzt, so dass bestimmte Probleme (wie etwa die genannten Unhandlichkeiten bei der Arbeit mit Word) nicht so ins Gewicht fallen. Der Einsatz von VNC erfolgt auf einen Telefonanruf hin. Dabei hat der Kollege im Rechenzentrum zunächst zu entscheiden, ob VNC überhaupt sinnvoll ist oder ob er sich selbst auf den weiten Weg machen muss (z. B. dann, wenn das Problem mit dem IP-Netz zusammenhängt). Wenn mit VNC gearbeitet werden soll, wird auf dem Rechner in der Beschaffungsstelle das Programm (der Server) gestartet und telefonisch das Passwort vereinbart. Gegebenenfalls informiert sich der Mitarbeiter im RZ über die IP-Nummer des Rechners. Im Anschluss startet er auf einer eigens dafür eingerichteten Wartungsmaschine den Viewer, gibt die IP-Adresse des Servers ein, und wenn alles korrekt ist, sollte sich sofort ein Fenster mit der Passwortabfrage zeigen. Als Authentifizierungsprotokoll ist in WinVNC CHAP implementiert. Nach (hoffentlich) erfolgreicher Beendigung der Arbeit, wird der Remoterechner vom Rechenzentrum aus neu gestartet. Damit soll nicht nur das Programm beendet, sondern auch gleich das Passwort, welches VNC in der Registry verschlüsselt ablegt, gelöscht werden. Mit dem Ergebnis, dass die Anwendung bei jedem erneuten Aufruf ein neues Passwort verlangt. Dazu sind in ein routinemäßig bei jedem Start ablaufendes Skript[2] die entsprechenden Registrykeys aufgenommen worden.

Es gibt allerdings Fälle, bei denen die Problemlösung einen Neustart des Rechners verlangt. Dazu muss VNC als Dienst laufen, also automatisch mit jedem Windowsstart ausgeführt werden. Wir haben – schon aus Gründen des Datenschutzes – nach Möglichkeit alles getan, dem Benutzer das Ausführen von VNC als Dienst zu erschweren. Allerdings kann jeder von der Kommandozeile über einen speziellen Befehl den Dienst ganz unkontrolliert starten mit dem Ergebnis, eine Hintertür auf seinem Rechner offen zu halten. Es ist geplant, diese Parameter, die man sich aus der VNC-Dokumentation über das Internet besorgen kann, durch abteilungsinterne Aufrufe zu ersetzen. Denn die Grenzen zwischen einem Fernwartungstool und einem Backdoor-Virus sind fließend und mitunter meldet die aktuelle Virenscannerversion das Vorhandensein von VNC auf dem Rechner. Aus diesem Grund löscht das genannte Skript auch entsprechende Aufrufe aus der Registry. Und wegen dieses Skriptes müssen selbst Administratoren ein komplexeres Prozedere ausführen, um den Dienst zum Laufen zu bekommen. Schließlich wurden am Programm selbst Veränderungen vorgenommen. Die Windows-Version ist mit Microsoft Visual Studio 6.0 erstellt worden. Für die Arbeit am Quellcode befindet sich Visual Studio auf dem Wartungs-PC. Neben ins Deutsche übersetzten Menüs und Fehlermeldungen wurden – speziell die Sicherheit betreffend – folgende Änderungen eingearbeitet:

Wenn WinVNC aktiv ist – gleich, ob als Dienst oder als Applikation – meldet es sein Vorhandensein über ein Icon im System-Tray des Servers. Liegt eine Verbindung zum Server vor, verfärbt sich dieses Icon. Dieses zweite Icon wurde verändert zu einem schwarzen Ausrufezeichen auf rotem Grund. Die Praxis hat gezeigt, dass Benutzer dieses Icon bemerken und danach fragen. Damit soll sichergestellt werden, dass aktive VNC-Verbindungen auffallen. Allerdings stellte sich heraus, dass das Icon nur dann erscheint, wenn in der Registry ein Benutzername eingetragen ist, d. h. wenn der Benutzer sich im Netz angemeldet hat. So bestand die Gefahr, dass VNC-Server auf einem Rechner lief, ohne dass der Mitarbeiter am betreffenden Rechner davon Kenntnis hatte. Hier wurde die entsprechende Bedingung für das Erscheinen des Icons im Quellcode auskommentiert, so dass das Icon in unserer Version immer erscheint. Auch an dieser Stelle ist eine Überarbeitung dahingehend geplant, dass – zusätzlich zum Tray-Icon – ein Fenster auf dem Desktop von einer aktiven Verbindung kündet.

Die Sicherheitsstrategie zielt also hauptsächlich darauf, Server nicht unkontrolliert und unbemerkt laufen zu lassen. Dass wir auf Absicherung über SSH oder VPNs bisher verzichtet haben, liegt daran, dass VNC durch die Firewall des Verwaltungsnetzes nicht möglich ist. VNC-Verbindungen sind also auf ein bestimmtes Netzwerksegment beschränkt. Wer VNC aber über öffentliche Netzwerke einsetzt, sollte die Verbindung über ein VPN tunneln, um sicher zu gehen, dass einem bei der Arbeit keiner über die Schulter schaut. Ansonsten kann die grenzenlose Freiheit schnell zum Desaster werden.

Till Hoke
till.hoke@rz.hu-berlin.de

2 Dieses Skript soll verhindern, dass Benutzer Einstellungen in der Systemsteuerung vornehmen. Es wurde für die Installation von VNC erweitert.