Die Nutzung sicherer verteilter Visualisierungsverfahren in der Raumplanung

Anne GRIEPENTROG

(Dipl.-Math. Anne GRIEPENTROG, Gesellschaft zur Förderung angewandter Informatik (GFaI) e.V., Berlin D-12489 Berlin, Rudower Chaussee 5, email: griepen@gfai.de, WWW: www.gfai.de)

EINLEITUNG

Gerade im Bereich der Stadtplanung spielt die Erzeugung von Ansichten zukünftiger Bau- oder Rekonstruktionsvorhaben, die in dieser Form noch nicht existieren, eine wesentliche Rolle. Dazu müssen Planungen der Gebäude in unterschiedlichen Varianten, z.B. in verschiedenen Farben oder Materialien visualisiert und digitalisierte Fotos der städtischen Räume mit den 3D-Modellen verbunden werden. Mit der Entwicklung der Rechentechnik rückt die Möglichkeit einer fotorealistischen Visualisierung von stadtplanerischen Modellen auch für kleine und mittlere Unternehmen in greifbarere Nähe. Erforderlich ist dazu das Vorhandensein leistungsfähiger Rechentechnik, deren Anschaffung jedoch für ein einzelnes Unternehmen meist zu teuer ist. Sie kann jedoch von mehreren Unternehmen gemeinsam genutzt oder von einem Dienstleistungsanbieter zur Verfügung gestellt werden. Die gemeinsame Nutzung setzt das Vorhandensein einer modernen Kommunikationsinfrastruktur zwischen den Unternehmen und einer verteilten, heterogenen Entwicklungsumgebung voraus.

1 PROJEKTZIELE

In diesem Beitrag wird über die Weiterentwicklung des System zur Visualisierung von 3D-Modellen in einer verteilten heterogenen Entwicklungsumgebung, das im Rahmen eines geförderten Projektes[1] entwickelt und in Unternehmen der Architekturbranche getestet wurde, berichtet. Zur Minimierung der für die Visualisierung erforderlichen Rechenzeiten wurde in einer ersten Projektphase eine ISDN-basierte Entwicklungsumgebung aufgebaut, die es mehreren Unternehmen gemeinsam ermöglicht, die bisher verwendeten computergestützten Entwurfssysteme auf PC-Basis weiter einzusetzen und gleichzeitig die in der GFaI vorhandenen Hochleistungsrechner parallel für die Visualisierung zu nutzen.

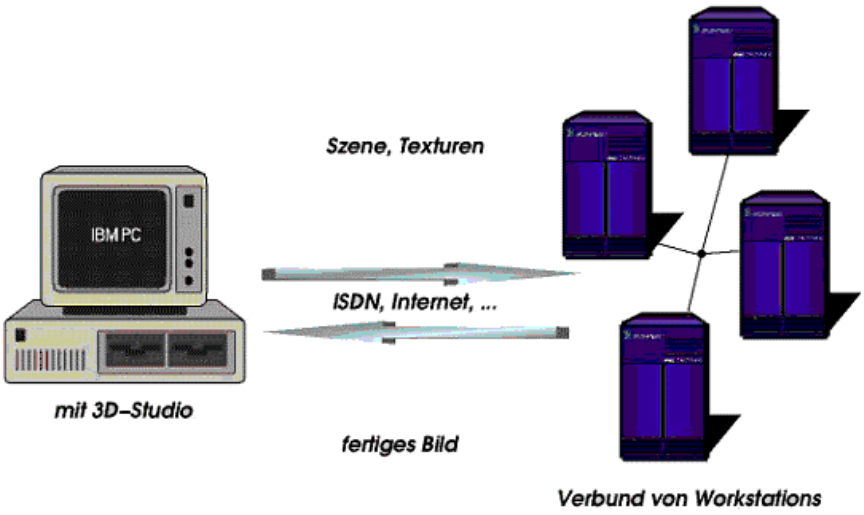

Abbildung 1: Prinzipdarstellung der verteilten Visualisierung

Dadurch konnten die Visualisierungszeiten drastisch verkürzt werden. Wesentlich für die Akzeptanz des Gesamtsystems war die Integration der Komponenten des Systems unter einer bekannten Nutzeroberfläche, die es den Anwendern ermöglicht, ohne zusätzliche Programmierkenntnisse mit dem Planungssystem zu arbeiten. Die benötigten Erweiterungen für die entfernte Visualisierung von 3D-Modellen wurden deshalb vollständig in 3D Studio MAX, als Plugin implementiert.

[1] Gefördert im Rahmen des IKT-Programms der Senatsverwaltung für Wirtschaft und Betriebe Berlin, Kennzeichen:VB1-7.6-6.07

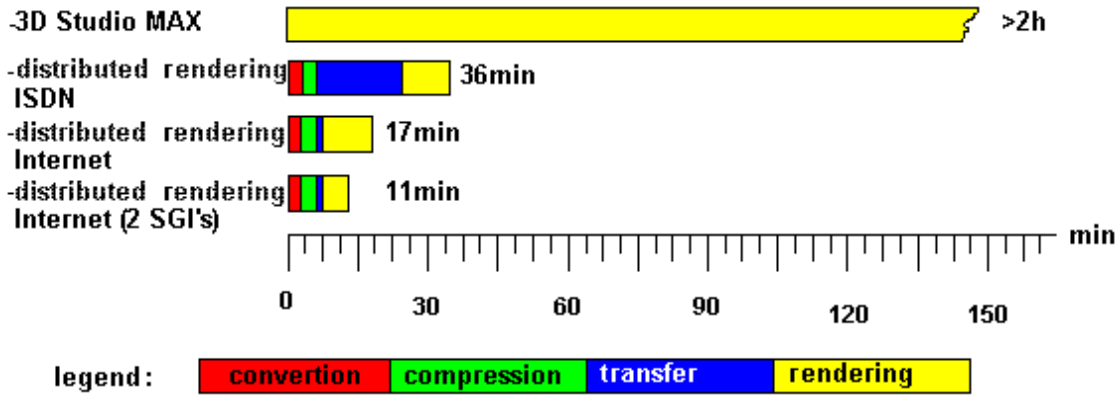

Abbildung 2 : Vergleich der Rechenzeiten beim entfernten Rendering

Um diese Forschungsergebnisse auch als Dienstleistung einem breiten Interessentenkreis zur Verfügung stellen zu können, mußten nun in einer weiteren Ausbauphase des Projekts Verfahren entwickelt werden, um die sicherheitsrelevante Schwachstellen in dem Planungssystem beseitigen. Besonders im Zusammenhang mit Ausschreibungen muß gewährleistet werden, daß die Daten eines jeden Architekten vor unberechtigten Zugriffen anderer Nutzer geschützt sind.

2 REALISIERUNG

Ausgehend von einer Anforderungsanalyse für die Erweiterung des Stadtplanungssystems in Bezug auf die Datensicherheit unter Berücksichtigung der vorhandenen heterogenen Entwicklungsumgebung wurden die folgenden Schwachstellen der Kommunikationsumgebung unter dem Aspekt der Datensicherheit analysiert.

1. Bisher erfolgte eine für den Ausbau des Gesamtsystems zu einer Dienstleistungsumgebung notwendige Authentifizierung der Nutzer nicht, so daß auch Unbefugte den Service des entfernten Renderings nutzen können.
2. Das Versenden und Empfangen der 3D-Modell Dateien erfolgte in der ersten Ausbaustufe der Kommunikationsumgebung unverschlüsselt. Bei einem unbefugtem Abhören der Leitung hat ein „Einbrecher“ keine Probleme, sich die Daten anzueignen und sofort zu nutzen. Da es sich vor allem im Architekturbereich um firmeninterne, oftmals geheimzuhaltende Daten handelt, ist es nicht im Sinne des Nutzers, wenn firmenfremde Personen sich dieser Arbeit bedienen.
3. Das Renderserver-Script muß, damit es ständig für eine Kommunikation zur Verfügung steht, im Hintergrund auf dem Server laufen. Das heißt, daß ein bestimmter Nutzer es einmal gestartet haben muß. Und dieser Nutzer hat damit alle Rechte auf dem Server, z.B. den Zugriff auf alle Systemressourcen. Dieses Verhalten setzt sich für jeden weiteren Nutzer fort, der eine Verbindung mit dem Server aufbaut. Dies ist ein sehr großes Sicherheitsloch, denn so können unbefugt fremde Daten gelöscht werden und eine Kontrolle über des Geschehen ist nicht mehr möglich.
4. Die bearbeiteten Dateien werden auf dem Server in ein und dem selben Verzeichnis abgelegt. Jeder Nutzer sieht also theoretisch die Daten des Anderen. Kommt es auch noch durch Zufall dazu, daß zwei Dateien den gleichen Namen besitzen, so wird die ältere Datei gelöscht und steht damit nicht mehr zur Verfügung.

Im Anschluß an die Schwachstellenanalyse wurde ein Sicherheitskonzept entworfen, die zu entwickelnden Komponenten und die Schnittstellen zwischen den Komponenten analysiert und in Absprache mit den Projektpartnern definiert.

2.1 Sicherheitskonzept

Die Sicherheit Stadtplanungssystems kann mit Hilfe verschiedener Maßnahmen, die dazu dienen, in privaten oder öffentlichen Netzen lediglich autorisierten Benutzern die ihnen zugewiesenen Ressourcen und Dienste zugänglich zu machen, erhöht werden:

1. *Authentifikation*: Überprüfung der Identität des Nutzers (Location)

2. *Autorisierung:* Zuordnung erlaubter Ressourcen u. Dienste auf zugelassene Nutzer (Nutzerkennung, Paßwort)
3. *Encryption:* Verschlüsselung der Daten
4. *Protokollierung:* Wer hat zu welchem Zeitpunkt was gemacht?

Eine *Authentifikation* kann durch eine entsprechende Anmeldung des Nutzers für das entfernte Rendering erreicht werden. Diese Anmeldung erfolgt über eine WWW-Anmeldungsseite, die ein Formular, das vom Nutzer auszufüllen ist, enthält. Die Anmeldungsseite wird an einen WWW-Server (Datenbank) geschickt, dort wird eine neue Eintragung in die Nutzer-Datenbank vorgenommen. Vom WWW-Server aus werden zwei Nachrichten verschickt:

1. Die Daten des neuen Nutzers werden an den Renderserver gesendet
2. Der neue Nutzer wird informiert, wo er sich das für das entfernte Rendering benötigte 3D-StudioMAX-Plugin und die zugehörigen TCL-Skripte abholen kann.

Auf dem Renderserver kann jetzt vom Administrator eine Initialisierungsdatei (Authentifizierung) aus public key, login und password erzeugt werden. Diese schickt er direkt an den Nutzer zurück mit der Aufforderung, diese Datei nicht weiterzugeben und sie im 3D-StudioMAX-Verzeichnis abzulegen. Außerdem werden die Arbeitsbereiche für die neuen Nutzerdaten auf dem Renderserver angelegt.

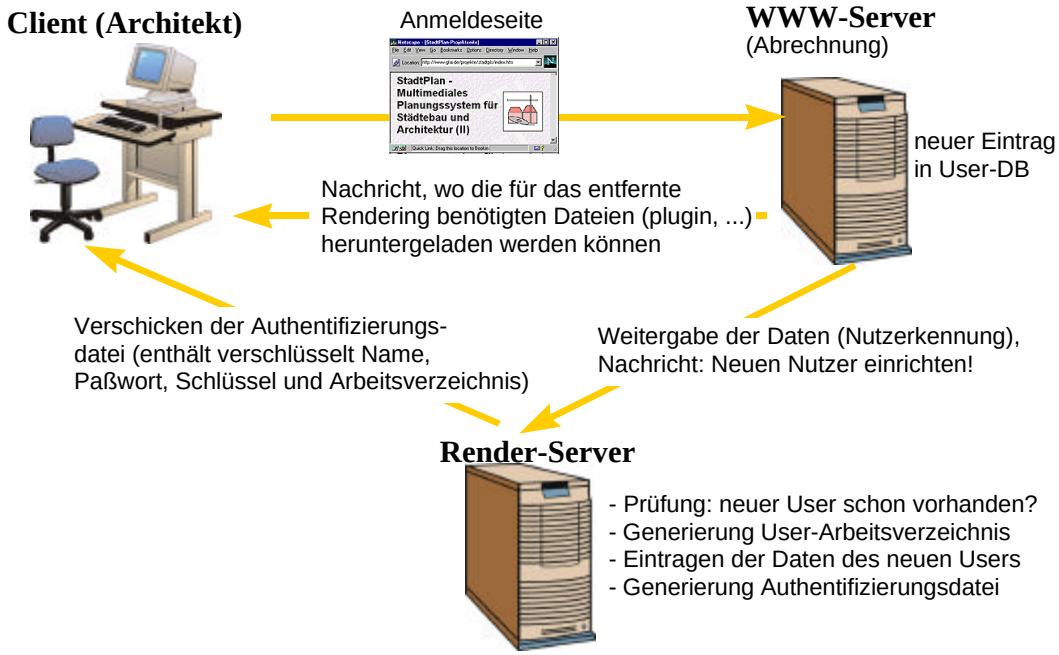

Abbildung 3: Darstellung des Konzepts der Nutzeranmeldung

Um zu vermeiden, daß ein beliebiger Nutzer des entfernten Renderings den Zugriff auf alle Ressourcen des Renderservers hat, wird auf dem Renderserver vom Root aus für jeden aktiven Nutzer ein separates Script, welches nur die Rechte des jeweiligen Benutzers besitzt, gestartet. Es muß daher zuerst eine Identifikation des Nutzers erfolgen, der mit dem Server kommunizieren will. Jeder Nutzer muß ein anderes Verzeichnis zugewiesen bekommen, in dem nur er und der Root alle Rechte besitzen. Sämtliche Dateien tragen hier immer eindeutig identifizierbaren Namen, werden nur dem jeweiligen Nutzer zugeordnet und erhalten auch nur dessen Rechte. Auf diese Art und Weise kann auch ein gleichzeitiges Arbeiten mehrerer Nutzer realisiert werden.

Außerdem sollte eine *Verschlüsselung* der Daten realisiert werden. Dies sollte mit einem Verfahren geschehen, welches zwei Schlüssel erstellt, damit auch nur zwei Benutzer die Daten lesen können. Die Daten können entweder durch einen selbst implementierten Algorithmus verschlüsselt werden, welcher auf bekannten, veröffentlichten Algorithmen basiert. Sinnvoller ist es aber, ein sehr sicheres und auch verbreitetes Verfahren einzusetzen, da der Nutzer dann auch dieses Verfahren nutzen kann um verschlüsselte Daten mit anderen auszutauschen. Im ersten Fall wäre außerdem ein hoher Entwicklungsaufwand für ein nur in diesem Projekt einsetzbares Verfahren die Folge.

Als einzusetzendes Programm bietet sich „PGP - Pretty Good Privacy“ an. Es ist leicht zu konfigurieren, sicher und sehr verbreitet. Außerdem ist es kostenlos zu erhalten und damit für jeden zugänglich. Im multimedialen Planungssystem für Städtebau und Architektur werden die Daten wie folgt verschlüsselt:

1. Auf dem Server wird mittels PGP ein Schlüsselpaar (*private* und *public key*) erstellt.
2. Der Client erhält den *public key* des Servers.
3. Nach dem Aufbau einer Verbindung werden die Daten mit dem *public key* verschlüsselt.
4. Die verschlüsselten Dateien werden an den Server geschickt.
5. Der Server entschlüsselt die empfangenen Dateien mit seinem *private key* und arbeitet mit diesen.

Eine Voraussetzung ist, daß der Nutzer den *public key* des Servers erhält. Dies geschieht beim erstmaligem Anmelden des Nutzers. In der Authentifizierungsdatei, die er in seinem 3D-StudioMAX-Verzeichnis ablegen muß, wird ihm auch der Schlüssel zugesendet.

Versendet der Nutzer nun sein Modell von 3D Studio MAX aus an den Renderingserver, so wird das Modell automatisch von dem im PGP-Programm implementierten Komprimierungs-algorithmus, der nahezu mit den Raten von „`gzip`“ vergleichbar ist, komprimiert und sofort verschlüsselt. Nachdem die Datei verschlüsselt ist, wird eine Meldung an den Server geschickt, daß von diesem Zeitpunkt an eine bestimmte Datei mit einer gewissen Länge zu empfangen ist. Der Client startet nun die Prozedur, die für das Versenden der Datei verantwortlich ist. Ist der Transfer beendet, so wird eine Meldung an den Server gesendet. Der Server hat nun geprüft, ob der Client berechtigt ist, den Service in Anspruch zu nehmen. Ist dies nicht der Fall, so erhält der Client eine entsprechende Meldung und die Verbindung wird geschlossen.

Außerdem wurde eine *Protokollierung* aller Arbeitsschritte auf dem Renderserver zum Erkennen unbefugter Eindringlinge und zum Abfangen von Fehlern realisiert. Jeder Client erhält zusätzlich nach jedem ausgeführten Arbeitsprozeß (Rendern, Konvertieren, usw.) eine entsprechende Meldung.

```
29.Jun.1998 11:54:57 (193.158.15.123): 220 Verbindung aufgebaut auf Socket: sock6 und Port: 2210.
29.Jun.1998 11:54:57 (193.158.15.123): 223 Transfer von userInfo.dat 143 Bytes
29.Jun.1998 11:54:57 (193.158.15.123): 224 Transfer von userInfo.dat ist beendet
29.Jun.1998 11:54:58 (193.158.15.123): 230 Zugriff erlaubt! Benutzer ist angemeldet!
29.Jun.1998 11:54:58 (193.158.15.123): 223 Transfer von faces.pgp 290674 Bytes
29.Jun.1998 11:55:01 (193.158.15.123): 224 Transfer von faces.pgp ist beendet
29.Jun.1998 11:55:01 (193.158.15.123): 420 Daten wurden uebertragen!
29.Jun.1998 11:55:01 (193.158.15.123): 420 Verbindung wurde geschlossen!
29.Jun.1998 11:55:02 (193.158.15.123): 240 Rendern wird gestartet.
29.Jun.1998 11:56:34 (193.158.15.123): 240 Rendern ist beendet!
29.Jun.1998 11:56:34 (193.158.15.123): 240 Konvertierung wird gestartet.
29.Jun.1998 11:56:46 (193.158.15.123): 240 Konvertierung ist beendet!
29.Jun.1998 11:56:48 (193.158.15.123): 240 E-Mail wurde versendet.
29.Jun.1998 11:57:21 (193.158.15.123): 220 Verbindung aufgebaut auf Socket: sock7 und Port: 2215.
29.Jun.1998 11:57:21 (193.158.15.123): 223 Transfer von userInfo.dat 143 Bytes
29.Jun.1998 11:57:21 (193.158.15.123): 224 Transfer von userInfo.dat ist beendet
29.Jun.1998 11:57:21 (193.158.15.123): 230 Zugriff erlaubt! Benutzer ist angemeldet!
29.Jun.1998 11:57:21 (193.158.15.123): 250 Bereit zum Empfang der Datei!
29.Jun.1998 11:57:21 (193.158.15.123): 225 Transfer von /usr/people/oelke/tcl/reneoelke/faces.jpg 14755 Bytes
29.Jun.1998 11:57:21 (193.158.15.123): 226 Transfer von /usr/people/oelke/tcl/reneoelke/faces.jpg ist beendet.
29.Jun.1998 11:57:22 (193.158.15.123): 420 Verbindung wurde geschlossen!
```

Abbildung 4: Protokollierung in der Server-Log-Datei

3 AUSBLICK

Der Funktionsumfang des multimedialen Stadtplanungssystem soll im Rahmen der jetzigen zweiten Projektphase, die bis Mitte 1999 geplant ist, so erweitert werden, daß das entfernte Rendering als Dienstleistung angeboten werden kann. Die Erfahrungen bei den kooperierenden Unternehmen zeigen, daß das System für einen Einsatz als tägliches Arbeitswerkzeug, nicht nur im Architekturbereich, sondern auch bei anderen, „visuellen Planungen“ in Unternehmen und Einrichtungen geeignet ist

Aktuelle Informationen zu diesem Projekt sind stets abrufbar unter der Adresse:
http://www.gfai.de/projekte/stadtpls/