SeVEN

Entwicklung eines sicheren Videoübertragungssystems

Softwareentwicklungspraktikum
Sommersemester 2009

Pflichtenheft

Auftraggeber:
Technische Universität Braunschweig
Institut für Betriebssysteme und Rechnerverbund
Prof. Dr.-Ing. Lars Wolf
Mühlenpfordtstraße 23, 1. OG
38106 Braunschweig

Betreuer: Kai Homeier, Timo Veit

Auftragnehmer:

Christoph Gröber	christoph-groeber@gmx.de
Daniel Brüdigam	daniel@planetsserver.com
Gregor Marek	gregor-m@hotmail.de
Hendrik Löbke	hendrik.loebke@gmx.de
Jan Laskowski	j.laskowski@t-online.de
Marek Drogon (Phasenverantwortlicher)	MDrogon@gmx.de

Braunschweig, 15. April 2009

Versionsübersicht

Version	Datum	Autor	Status	Kommentar
v0.2	07.04.09	Gruppe	50%	Ergebnisse 1. Treffen
v0.3	08.04.09	Gruppe	100%	Ergebnisse 2. Treffen
v1.0	15.04.09	Gruppe	100%	Überarbeitete Version

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Zielbestimmung

Datenschutz ist ein wichtiges und immer brisanter werdendes Thema bei der Speicherung von Daten aller Art. In diesem Praktikum geht es dabei speziell um Videodaten. Eine zu Evaluationszwecken angeschaffte Überwachungskamera des IBR speichert, wenn sie eine Bewegung detektiert, Videodaten auf einem Server, auf dem diese vor unerlaubtem Zugriff geschützt sein sollen.

Um den Datenschutz zu gewährleisten, sollen die Videos verschlüsselt zu einer Abspielsoftware übermittelt werden. So können die Daten auch über das Internet an entfernte Rechner sicher übertragen werden. Erst die Abspielsoftware dekodiert und spielt Videos ab.

Ein weiteres Modul ermöglicht das verschlüsselte Hochladen von Videos auf den Server. Eine Benutzerverwaltung ermöglicht es, neue Benutzer anzulegen und individuelle Rechte zu vergeben, sowie diese zu ändern.

1.1 Musskriterien

Es soll auf einen zentralen Server ein Video-Speichersystem realisiert werden, auf den die Benutzer ihre aufgenommenen Videos von überall aus hochladen koennen. Dieses wird durch eine Player-Software realisiert die es beherrscht, vorhandene Videos zu verschlüsseln und hochzuladen, aber auch ein bereits gelagertes Video gestreamt zu kriegen und dieses waehrend der Laufzeit sofort zu dekodieren. Es sollen nur die jeweiligen Benutzer auf ihre Videos Zugriff haben.
Als Erweiterung dazu kann man eine Videokamera anschliessen, die auf die selbe Weise beim Auslösen automatisch Videos auf den Server überträgt.

1.2 Wunschkriterien

Um die Sicherheit untereinander zu bewahren, soll eine Zugriffsberechtigung hinzugefügt werden, die die Benutzer untereinander abschottet. Ein Video-Management-System sol ein Benutzerinterface implementieren und den Nutzern ermöglichen, untereinander Video-Sharing zu betreiben. Administratoren soll eine Benutzerumgebung zur Verfügung gestellt werden, mit der sie den Inhalt der Videos überwachen und Benutzer verwalten können.

1.3 Abgrenzungskriterien

Mit Hilfe der Kamera soll keine Echtzeitüberwachung realisiert werden, sondern nur eventgesteuerte Aktivierung.
Die eventuell einsetzbare Kamera, für eine eventgesteuerte Überwachung, ist schon fertig vorhanden und wird in das fertige System implementiert.
Der Videostream wird durch FMJ realisiert.

1.3.1 Verschlüsselung

Die verwendete Verschlüsselung muss folgende Kriterien erfüllen:

- Die Sicherheit soll auf der Geheimhaltung des Schlüssels beruhen und nicht auf der des verwendeten Verfahrens.
- Auch große Chiffredatenmengen sollen das Berechnen des verwendeten Schlüssels praktisch nicht ermöglichen.
- Die Daten sollen sequenziell entschlüsselt werden können, um das Abspielen der Videos schon vor dem kompletten Download starten zu können.

Es bieten sich verschiedene Chiffrierverfahren an, zum Beispiel DES, IDEA oder AES. Das SunJCE stellt bereits Implementierungen für diese Verfahren bereit, weshalb wir diese Bibliothek verwenden wollen.

2 Produkteinsatz

Das Videoüberwachungssystem wird folgende Anwendungsbereiche, Zielgruppen und Betriebsbedingungen haben

2.1 Anwendungsbereiche

- Videoüberwachung
- Videosharing
- Gewerbliche und Private Zwecke

2.2 Zielgruppen

- Firmen
- Wohnhäuser
- Überwachungsbedürftige Einrichtungen
- Institute

2.3 Betriebsbedingungen

Bei ausschließlicher Benutzung der Upload-Funktion sind keine besonderen Bedingungen zu beachten. Beim stationären Einsatz einer Kamera sollte diese im Stand-By-Dauerbetriebsmodus laufen. Ausserdem sollte ein sicherer Standort innerhalb bzw. ausserhalb der zu überwachenden Einrichtung gewährleistet sein.

3 Produktübersicht

Folgende Systemfunktionalität wird implementiert:

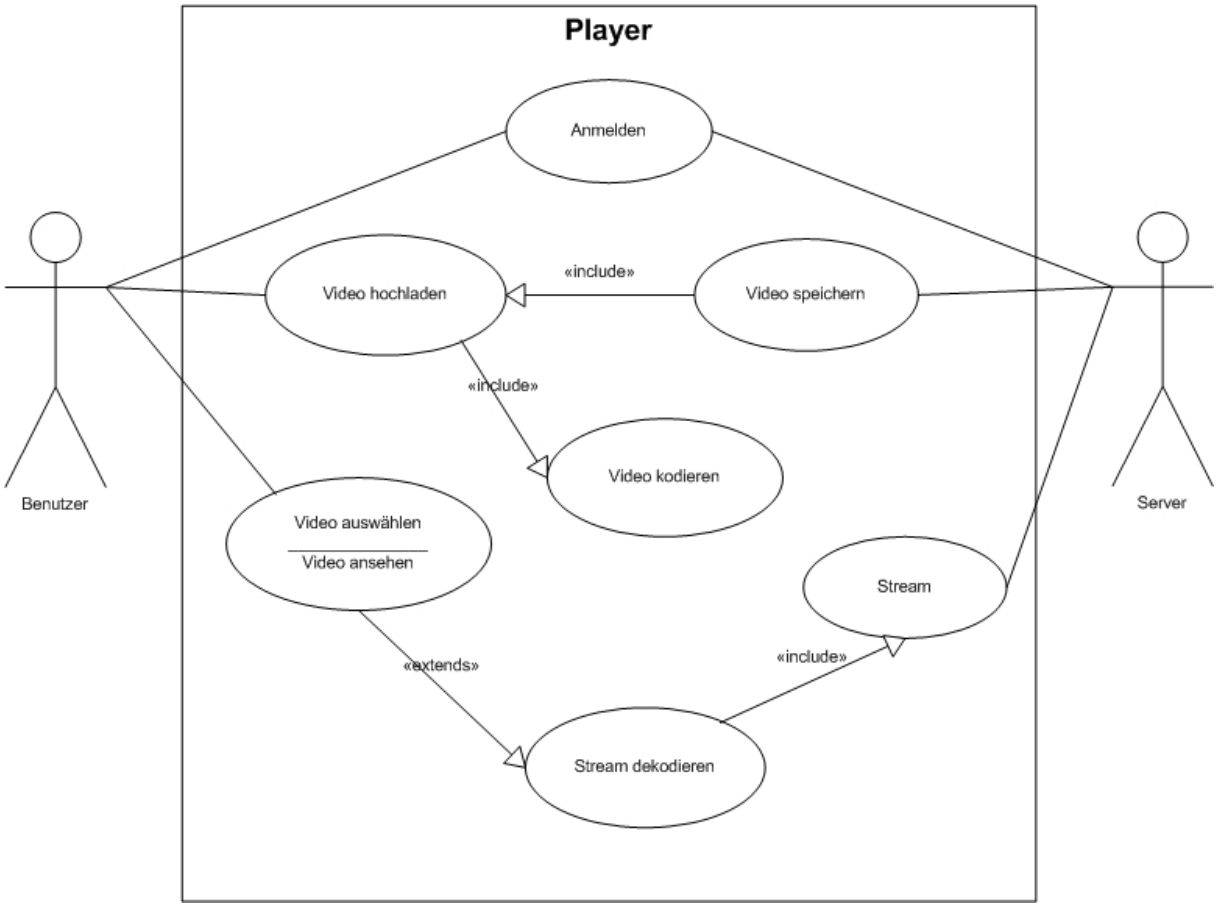

Abbildung 3.1: Anwendungsfall Player

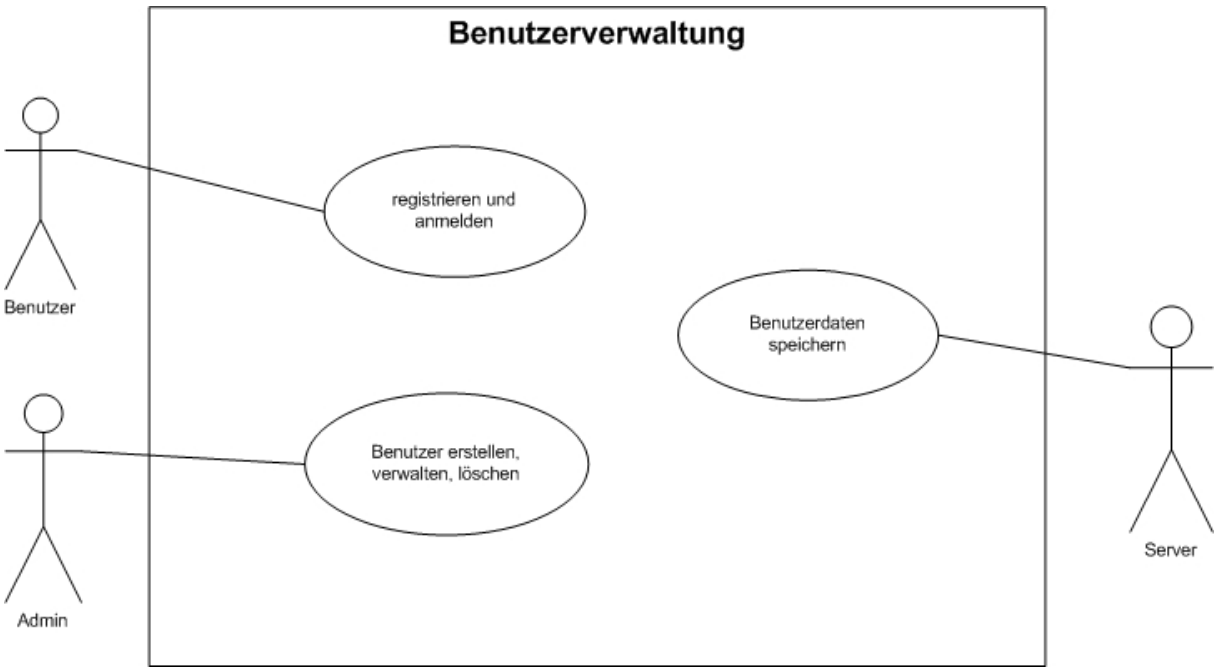

Abbildung 3.2: Anwendungsfall Benutzerverwaltung

4 Produktfunktionen

/F100/ Player

/F110/ Video hochladen

Geschäftsprozeß: Hochladen der Videodateien

Ziel: Video soll verschlüsselt auf dem Server bereitliegen

Vorbedingung: Berechtigung zum Upload und Video muss verschlüsselt vorliegen

Nachbedingung Erfolg: Video wurde erfolgreich übermittelt

Nachbedingung Fehlschlag: Fehler bei der Übertragung oder kein Speicherplatz

Akteure: Berechtigter Benutzer

Auslösendes Ereignis: Benutzer möchte ein Video hochladen

Beschreibung:

1. Anmelden
2. Datei auswählen
3. Datei hochladen
4. Rückmeldung anzeigen

Erweiterung: Mehrere Uploads auf einmal

/F120/ Video ansehen

Geschäftsprozess: Gewünschtes Video ansehen

Ziel: Video soll abgespielt werden

Vorbedingung: Video wird übertragen und entschlüsselt

Nachbedingung Erfolg: Video wird korrekt abgespielt

Nachbedingung Fehlschlag: Video wird nicht oder nur fehlerhaft abgespielt

Akteuere: Berechtigter Benutzer

Auslösendes Ereignis: Benutzer möchte sich ein Video ansehen

Beschreibung:

1. Anmelden
2. Auswählen
3. Stream empfangen
4. Stream dekodieren
5. Video abspielen

Erweiterung: Mögliche Downloadfunktion sowie Zusatzfunktionen

/F130/ Anmeldung

Geschäftsprozess: User meldet sich am System an

Ziel: Auf vorhandene Daten zurückgreifen

Vorbedingung: Registrierung

Nachbedingung Erfolg: Anmeldung erfolgreich

Nachbedingung Fehlschlag: Nicht erfolgreich oder keine Berechtigung

Akteuere: Benutzer, Server

Auslösendes Ereignis: User möchte sich anmelden

Beschreibung:

1. Eingabe des Usernamen und Passwort
2. Überprufung der Daten
3. Rückmeldung

/F140/ Video kodieren

Geschäftsprozess: Ein hochzuladenes Video wird verschlüsselt

Ziel: Video soll verschlüsselt werden

Vorbedingung: Video wird ausgewählt und will hochgeladen werden

Nachbedingung Erfolg: Verschlüsselung erfolgreich

Nachbedingung Fehlschlag: Verschlüsselung nicht erfolgreich

Akteuere: Benutzer, Player

Auslösendes Ereignis: User möchte ein Video hochladen

Beschreibung:

1. Auswahl des Videos
2. Verschlüsseln
3. Hochladen

/F150/ Stream dekodieren

Geschäftsprozess: Ein ankommender Stream wird entschlüsselt

Ziel: Stream soll entschlüsselt werden

Vorbedingung: Ein Video wird übertragen

Nachbedingung Erfolg: Das Video wird ohne Fehler angezeigt

Nachbedingung Fehlschlag: Video wird fehlerhaft oder gar nicht angezeigt

Akteuere: Player, Server

Auslösendes Ereignis: User möchte sich ein Video anschauen

Beschreibung:

1. Stream kommt an
2. Verschlüsselung wird aufgeloest
3. Wiedergabe des unverschlüsselten Videos

/F160/ Stream dekodieren

Geschäftsprozess: Ein Datenstrom wird durchgeführt

Ziel: Der Datenstrom soll sein zugewiesenes Ziel erreichen

Vorbedingung: Server kriegt den Auftrag ein Video zu streamen

Nachbedingung Erfolg: Der Stream kommt am Player an

Nachbedingung Fehlschlag: Der Stream kommt teilweise oder überhaupt nicht am Player an

Akteuere: Player, Server

Auslösendes Ereignis: User möchte sich ein Video anschauen

Beschreibung:

1. Server verschickt Stream
2. Player empfängt Stream

/F200/ Verwaltung

/F210/ Registrierung

Geschäftsprozeß: Accounterstellung

Ziel: Einen Benutzeraccount anlegen

Vorbedingung: Benutzer ist berechtigt, das System zu nutzen

Nachbedingung Erfolg: Registrierung erfolgreich

Nachbedingung Fehlschlag: Registrierung nicht erfolgreich

Akteure: Benutzer, Administrator, Benutzerverwaltung

Auslösendes Ereignis: Benutzer möchte das System nutzen

Beschreibung:

1. Formular ausfüllen und abschicken
2. Daten werden gespeichert
3. Administrator schaltet Benutzer frei
4. Rückmeldung an den Nutzer

/F220/ Benutzerverwaltung

Geschäftsprozeß: Verwaltung eines Benutzers

Ziel: Benutzerrechte ändern oder Benutzer löschen

Vorbedingung: Benutzer ist in der Datenbank vorhanden

Nachbedingung Erfolg: Änderung an Benutzer wurde vorgenommen

Nachbedingung Fehlschlag: Systemfehler

Akteure: Administrator, Benutzerverwaltung

Auslösendes Ereignis: Administrator möchte Änderung vornehmen

Beschreibung:

1. Administrator meldet sich am System an
2. Zu ändernden/löschenden Benutzer auswählen
3. Operation ausführen

4. Änderungen speichern

Erweiterung: Mehrere Operationen auf einmal

5 Produktdaten

Langfristig zu speichernde Daten werden wie folgt realisiert

/D10/ Daten der Videospeicherplätze

- Videoname: Der Names des Videos
- Zugriffsrechte: Wer darf alles auf das Video zugreifen
- Videoattribute: Format, Grösse, Verschlüsselung
- Beschreibung: Wer hat zu welcher Zeit etwas hochgeladen
- Zugriffe Wer hat wann auf ein Video zugegriffen und wann war der letzte Zugriff

/D20/ Daten des Benutzeraccounts

- Vorname
- Nachname
- Strasse
- PLZ
- Wohnort
- Abteilung
- Zugriffsrechte: Welche Rechte hat der bestimmte Benutzer
- Passwort
- Registrier-Datum

6 Produktleistungen

Folgende Leistungsanforderungen müssen implementiert werden

- /L10/
  Die Funktion /F30/ darf nicht länger als 5 Sekunden brauchen um die Daten zu empfangen
- /L20/
  Alle Reaktionen auf Benutzerebene müssen unter 2 Sekunden liegen
- /L30/
  Die Funktion /F20/ soll in angemessener Zeit verschlüsseln und lagern

7 Qualitätsanforderungen

Produktqualität	**sehr gut**	**gut**	**normal**	**nicht relevant**
Funktionalität				
Angemessenheit		x		
Richtigkeit	x			
Interoperabilität	x			
Ordnugsmässigkeit				x
Sicherheit				
Zuverlässigkeit	x			
Reife			x	
Fehlertoleranz		x		
Wiederherstellbarkeit				x
Benutzbarkeit				
Verständlichkeit	x			
Erlernbarkeit	x			
Bedienbarkeit	x			
Effizienz		x		
Zeitverhalten	x			
Verbrauchsverhalten			x	
Änderbarkeit				
Analysierbarkeit			x	
Modifizierbarkeit		x		
Stabilität	x			
Prüfbarkeit			x	
Übertragbarkeit				
Anpassbarkeit		x		
Installierbarkeit		x		
Konformität				x
Austauschbarkeit		x		

8 Benutzeroberfläche

Benutzeroberflächen Intro

- /B10/
  Tabellarische Anzeigeseite der Videoverwaltung soll angelehnt an Windows Benutzeroberfläche sein
- /B20/
  Darstellung des Players in gewohnter Windows Umgebung
- /B30/ Folgende Rollen sind zu unterscheiden

Rolle	**Rechte**	**Benutzeroberfläche**
Normaler Benutzer	/F10/, /F30/	Tabellarische Übersicht
Administrator	/F10/ bis /F40/	Zusätzliche Administrative Methoden

9 Nichtfunktionale Anforderungen

Folgende Anforderungen beziehen sich weder auf Funkionalität, Leistung oder Benutzeroberfläche:

- /NF10/ Das Produkt soll plattformunabhängig sein
- /NF20/ Intuitive Bedienbarkeit ohne grosse Vorkenntnisse
- /NF30/ Leichte Erweiterbarkeit
- /NF40/ Hohe Fehlertoleranz bezüglich Bedien- und Eingabefehlern

10 Technische Produktumgebung

Folgende technische Umgebung wird für das Produkt benötigt

10.1 Software

Server-Betriebssystem: Linux
Client-Betriebssystem: Windows XP oder Vista

10.2 Hardware

Server: Leistungsfähiger PC
Client: PC mit Multimedia-Komponenten

10.3 Orgware

- Verbindung zum Server sollte vorhanden sein
- Verschlüsselung sollte zu jeder Zeit sicher sein
- Keine dauerhafte Verbindung zum Server nötig

10.4 Produktschnittstellen

- Clientzugang realisiert durch TCP/IP-Protokoll
- Erweiterbarkeit für weitere Kameras