

Geo Web Services

Sicherheit und Zugriffskontrolle

Andreas Matheus, 26.4.2004

Inhaltsangabe Sicherheit

- ◆ Geo Web Services und Sicherheit
 - Was sind Geo Web Services
 - Welche Sicherheitsanforderungen ergeben sich aus deren Nutzung?
 - Umsetzung von Sicherheitsanforderungen durch Verschlüsselung
 - ◆ Point-to-Point Sicherheit
 - ◆ End-to-End Sicherheit
 - Zugriffskontrolle ist Bestandteil von Sicherheit

Inhaltsangabe Zugriffskontrolle

◆ Anforderungen an die Zugriffskontrolle

- Verteiltheit
- Informationsbezug
- Raumbezug

◆ Informationsbezug

- Zugriffsrecht kann an Typ gebunden sein
- Zugriffsrecht kann an Instanz gebunden sein

◆ Raumbezug

- Ortsbezug
- Geometrie

Motivation für Web Services

- ◆ Ermöglichen E-Commerce
- ◆ Marktpotential ist vorhanden
 - Umsätze steigen von z.Z. 1,6 Milliarden \$ auf geschätzte 30 Milliarden \$ für 2005
- ◆ Kommunikation über Internettechnologie ermöglicht Internet-weite Erreichbarkeit
 - Protokoll TCP/IP und HTTP
 - SOAP zur Beschreibung der Aufrufe
 - XML zur Beschreibung des Nachrichteninhalts
- ◆ Implementierungstunabhängig

Begriffsdefinitionen

- ◆ Geo Web Services sind Web Services,
 - die den Zugriff auf oder die Verarbeitung von Geodaten ermöglichen, wie z.B. Kartendarstellung, oder
 - raumbezogene Verarbeitung von Informationen (z.B. Geodaten) ermöglichen, wie z.B. Geocoding
- ◆ Geodaten sind Informationen über Objekte mit Raumbezug; die auch Geometrie haben können
- ◆ Raumbezug und Geometrie ist in einem sog. Raumbezugssystem (CRS) angegeben und gültig.

Kommunikation mit dem (Geo) Web Service via SOAP

- ◆ Kommunikation basiert auf SOAP Nachrichten
- ◆ Aufrufender (Client im Auftrag des Benutzers) erstellt **XML strukturierte Nachricht**
- ◆ Nachricht wird in **SOAP** „verpackt“ und an den Service gesendet, z.B. HTTP-Post
- ◆ Nachricht wird ausgepackt, Service wird ausgeführt und **XML strukturierte Antwort** erstellt
- ◆ XML strukturierte Antwort wird als SOAP Nachricht an den Aufrufenden zurück geschickt
- ◆ Für Geodaten kann die Nachricht in GML (einer XML Kodierung für Geodaten) strukturiert sein

Netzwerkbasierende Kommunikation

- ◆ Kommunikation zwischen Client und Service erfolgt über ein Netzwerk; z.B. Intranet, Extranet, Internet
- ◆ Internet ist offen und a priori unsicher
 - Offen: 'Jeder' kann sich Zugang verschaffen
 - Anonym: Authentifizierung der Benutzer erfolgt nicht
- ◆ TCP/IP basierte Kommunikation zwischen zwei Partnern (Client und Service) kann über **sog. Intermediäre** erfolgen
 - Kommunikationspartner haben keinen Einfluss auf das Routing der Nachrichten (welche Intermediäre beteiligt sind)

Ursache für die Definition von Sicherheitsanforderungen

- ◆ SOAP Nachricht ist anonym und liegt im Klartext vor
- ◆ Nachricht kann auf Intermediären gelesen, verfälscht, gelöscht oder dupliziert werden
- ◆ Benutzer können falsche Identitäten verwenden
- ◆ Nicht jeder Service steht für jeden Benutzer zur Verfügung. Nur identifizierte Benutzer erhalten bestimmte Zugriffsrechte.
- ◆ Durchsetzung von Zugriffsrechten erfordert Zugriffskontrolle
 - Authentifizierung
 - Autorisierung

Sicherheitsanforderungen für sichere Kommunikation

- ◆ Vertrauen zwischen Kommunikationsteilnehmern
 - Keine Maskerade: Vortäuschen falscher Identität nicht möglich
 - Nicht Abhören: von Nachrichten
 - Kommunikationssicherheit: Unerlaubtes lesen, Verlust, Modifikation oder Erzeugung von Nachrichten ist nicht möglich
 - Zurechenbarkeit: Erfolgreiches Abstreiten der Nutzung unmöglich
- ◆ Unberechtigte Nutzung ausschließen
 - Zugriff ist nur für autorisierte Nutzer möglich
 - Setzt Authentifizierung voraus

Schutzziele

- ◆ **Vertraulichkeit:** Nachrichten können nur von dem eigentlichen Empfänger gelesen werden
- ◆ **Integrität:** Nachrichten können nicht unbemerkt verfälscht werden
- ◆ **Zurechenbarkeit:** Nachrichten können Identitäten zugeordnet werden
- ◆ **Zugriffskontrolle:** Nur autorisierte Nutzer können den Service nutzen

Lösungsmöglichkeiten

- ◆ Virtuell Private Network (VPN)
- ◆ Nutzung von Kryptographie
 - Kryptographie = „Geheimhaltung von Informationen“
 - Unterscheidung in
 - ◆ Verschlüsselungsverfahren
 - ◆ Digitalen Signaturen und Zertifikate
 - Schlüsselgesteuerte Verschlüsselungsverfahren
 - ◆ Symmetrisch (private key Verfahren)
 - ◆ Asymmetrisch (public key Verfahren)

Schlüsselgesteuerte Verschlüsselungsverfahren

- ◆ Gewährleisten Identität, Integrität und Vertraulichkeit
- ◆ Private Key Verfahren (symmetrisch)
 - Kommunikationspartner nutzen den selben Schlüssel
 - Basiert auf der Geheimhaltung des einen Schlüssels
 - Problem: Sicheres Kommunizieren des Schlüssels
- ◆ Public Key Verfahren (asymmetrisch)
 - Schlüsselpaar (private und public Key)
 - Basiert auf der Geheimhaltung des private Key
 - Public Key kann aus private Key erzeugt werden

Das Zertifikat (X.509)

- ◆ Ein sog. Trust Center bindet einen public Key an die Identität einer juristischen Person
- ◆ Ergebnis ist ein Zertifikat
- ◆ Zurechenbarkeit: Digitale Signatur ermöglicht Zugordnung einer Nachrichten zum Sender
- ◆ Integrität: Digitale Signatur des Hashwerts der Nachricht (erfordert Normierung der Nachricht)
- ◆ Vertraulichkeit: Verschlüsselung mit dem public Key des Empfängers

Anwendung der Verschlüsselung

- ◆ Kommunikation nach dem ISO-OSI Modell
 - Schicht 4 (Transport): TCP/IP
 - Schicht 5 (Anwendung): HTTP, SOAP, etc.
- ◆ Verschlüsselung auf Schicht 4
 - Point-to-Point Verschlüsselung
 - SSL in Verbindung mit HTTP = HTTPS
- ◆ Verschlüsselung auf Schicht 5
 - End-to-End Verschlüsselung
 - XML Encryption, XML Signature, XML Key Management.

Pont-to-Point und End-to-End Verschlüsselung

◆ Point-to-Point Verschlüsselung

- Sicherheit kann **nicht über Intermediäre hinweg** garantiert werden
- Nur **gesamte Nachricht** wird **verschlüsselt**

◆ End-to-End Verschlüsselung

- Sicherheit kann **zwischen Sender und Empfänger** garantiert werden; unabhängig von Intermediären
- **Selektive Verschlüsselung** der XML Nachricht kann gesteuert werden

Realisierung der End-to-End Verschlüsselung

- ◆ Auf der **Senderseite** werden **Händler** genutzt
 - Einfügen von digitaler Signatur (**HS_Sig**)
 - Einfügen von Enryption (**HS_Enc**)
 - Einfügen von Autorisierungsinformation (**HS_Acc**)
- ◆ Auf der Empfängerseite werden (inverse) Händler genutzt
 - Nutzung der Autorisierungsinformation (**HR_Acc**)
 - Validierung der Encryption (**HR_Enc**)
 - Validierung der digitalen Signatur (**HR_Sig**)
- ◆ Auf dem Rückweg der Nachricht zum Sender kein **HS_Sig**

Ende zum Teil Sicherheit

- ◆ Nutzung von Zertifikaten und entsprechender Verschlüsselung ermöglicht die Umsetzung der Schutzziele
 - Integrität
 - Vertraulichkeit
 - Zurechenbarkeit

Zugriffskontrolle

- ◆ Basiert auf eindeutiger Identifizierung von Subjekten (Authentifizierung)
- ◆ Autorisierung entscheidet „Wer darf was“; festgelegt in Zugriffsbeschränkungen (Policies)
- ◆ Zugriffskontrolle setzt die Zugriffsbeschränkungen durch
 - **Subjekt:** Initiator
 - **Operation:** Wird auf dem Objekt ausgeführt
 - **Objekt:** Auf dem wird die Operation ausgeführt
 - **Bedingung:** Es müssen bestimmte Randbedingungen erfüllt sein, damit die Regel durchgesetzt wird

Anforderungen an die Zugriffskontrolle für Geo Web Services

- ◆ Voraussetzung: Nachricht ist XML (bzw. GML) kodiert und gegen XML Schema validierbar
- ◆ Berechtigungen können sich beziehen auf:
 - Geoobjekt = Informationsbezug der Nachricht
 - Typ des Geoobjekts (aus XML Schema)
 - Ein oder mehrere Geoobjekte
 - Raumbezug
 - Relationen zwischen GeoObjekten
- ◆ Zugriff auf Operationen (Write, Read, Create, Delete) soll positiv oder negativ sein

Informationsbezogene Berechtigungen

- ◆ Basis ist ein validierbares XML, bzw. GML Dokument
- ◆ GML bietet vordefinierte (geospatial) Typen und nutzt XML Encoding
- ◆ XML Dokument kann als Baum dargestellt werden
 - Mögliche Baumstrukturen sind durch zugehöriges XML Schema (XSD) vorbestimmt; die Knoten und Kanten des Baumes
 - Element kann explizit Relation zu anderem Element sein
- ◆ Zugriffsrecht auf XSD Typen oder XML Elemente
- ◆ Zugriffsrecht auf ein XSD Typ gilt für alle XML Elemente dieses Typs

Positive und negative Berechtigungen auf Operationen

- ◆ Explizite Deklaration von positiven und negativen Berechtigungen
 - Vorteil: Ausnahmen können einfach dargestellt werden
 - Nachteil: Es kann zu Inkonsistenzen kommen
- ◆ Operationen: Read, Write, Delete und Create
- ◆ Berechtigung ist durch 4-Tupel definiert: $\langle r, w, d, c \rangle$
 $r \in \{+, -, \varepsilon\}$, $w \in \{+, -, \varepsilon\}$, $d \in \{+, -, \varepsilon\}$, $c \in \{+, -, \varepsilon\}$
 - + : Positive Berechtigung
 - - : Negative Berechtigung
 - ε : Berechtigung ist nicht festgelegt

Möglichkeiten von Xpath bei der Informationsobjektadressierung

- ◆ Verwendung von Xpath Ausdrücken ermöglicht
 - Adressierung von XSD Typen und Elementen
 - Adressierung von XML Dokument Elementen und Attributen
 - Adressierung eines Elementes oder eine bestimmte Menge von Elementen
- ◆ Verwendung von Xpath Ausdrücken ermöglicht nicht
 - Adressierung von Vererbung bei XSD Typen
 - Dies muss anders geregelt werden, falls erforderlich

Gültigkeit von Xpath Ausdrücken

- ◆ Adressierung eines XSD Typs ist gültig für alle Instanzen (XML Elemente)
 - XSD globaler Typ
 - ◆ Gültigkeit: Gilt für alle Instanzen des Typs
 - XSD globales Element
 - ◆ Gültigkeit: Gilt für alle Referenzen auf das Element

Deklaration von Zugriffsbeschränkungen: Die Policy

- ◆ Policy enthält ein oder mehrere Regeln
- ◆ Jede Regel liefert ein Ergebnis (Effect)
 - Grant: Besagt, dass Regel fehlerfrei abgearbeitet wurde und dem Zugriff stattgegeben werden soll
 - Deny: Besagt, dass Regel fehlerfrei abgearbeitet wurde und dem Zugriff nicht stattgegeben werden soll
 - N/A: Besagt, dass Regel nicht anwendbar ist
 - Indeterminate: Besagt, dass Regel fehlerhaft abgearbeitet wurde oder dass zur Abarbeitung Informationen fehlen
- ◆ Policy enthält eine übergeordnete Vorschrift die angibt, wie aus den Ergebnissen der einzelnen Regeln letztendlich ein Grant oder Deny entsteht

Raumbezogene Policies

- ◆ Geoinformationen beschreiben **Objekte** mit Raumbezug (= Geoobjekte)
- ◆ 3-D Model enthält geographische **Primitive**: Punkt (0D), Linie (1D), Fläche (2D) und Körper (3D)
- ◆ Objektgeometrie basiert auf primitiven Typen
- ◆ Zugriffsrechte gelten für Fläche (evtl. für Körper)
- ◆ **Zugriffsrechte** wirken **direkt** oder **indirekt**
 - **Direkt**: Raumbezogene Abfrage der Objekte, z.B. BBox
 - **Indirekt**: Bei nicht raumbezogener Abfrage der Objekte anhand der Objektgeometrie

Relationsbezogene Policies

- ◆ Abhängig vom Kontext
- ◆ Wenn Berechtigung für Objekt X existiert, dann gilt die Berechtigung auch auf die Menge der Objekte Y für die gilt $Y \subseteq \text{Relation}(X)$, $Y = \{y_1, y_2, \dots, y_n\}$
- ◆ Erfordert einen „Platzhalter“ in der Policy, dem der Kontext bei der Abfrage zugewiesen wird.
- ◆ Explizite Relationen sind im XML Dokument niedergeschrieben
- ◆ Implizite Relationen zwischen Geoobjekten können anhand des Raumbezugs bestehen

Durchsetzen von Policies

- ◆ Übergeordnete Vorschrift erforderlich
 - Wie muss mit „ \in “ Berechtigungen umgegangen werden?
- ◆ Alle matching Policies müssen durchgesetzt werden
- ◆ Verschiedene Policies matchen direkt für einen bestimmten Request
 - $\text{RequestSubject} \in \text{PolicySubject}$
 - $\text{RequestObject} \subseteq \text{PolicyObject}$
 - Regeln bestimmen, ob Policy anzuwenden ist
- ◆ Verschiedene Policies matchen indirekt über
 - Geometrie von PolicyArea und RequestArea oder
 - Geometrie von PolicyArea und RequestObjects

Wie entstehen Inkonsistenzen?

- ◆ Für einen Request (= Menge von GeoObjekten) matchen eine Menge von Policies
 - Direkt, wenn Element als Objekt in der Policy deklariert ist
 - Indirekt, wenn Raumbezug zutrifft
 - Indirekt über eventuelle Relation(en)
- ◆ Für eine Teilmenge der Policies können die Berechtigungen konträr sein \Rightarrow Inkonsistenzen
 - RequestOperation erlaubt (+), verboten (-) oder keine Aussage (ε)

Auflösen von Inkonsistenzen (1/2)

- ◆ Übergeordnete Vorschrift erforderlich
 - Wie muss mit „ \in “ Berechtigungen umgegangen werden
- ◆ Beheben nach der Regel „most specific overwrites“
 - Informationsbezogene Policy: Lokal deklarierte Berechtigung überschreibt propagiertes Recht
 - Raumbezogene Policy: Nur möglich, wenn Topologie der Zugriffsgebiete vorhanden ist. Nur Geometrie vorhanden, möglichst keine Auflösung.

Auflösen von Inkonsistenzen (2/2)

- ◆ Bei gleich spezifischer Deklaration:
 - Auflösung über „Tie-Braking-Funktion“
- ◆ Tie-Braking-Funktion
 - „Safety first“; d.h. die most restrictive Policy wird durchgesetzt
 - Dazu muss geklärt werden, welcher Zugriff „most restrictive“ ist: $(+, -)$, $(+, \varepsilon)$, $(-, \varepsilon)$

Unzureichende Berechtigung

- ◆ Der Zugriff wird verweigert
 - Welche Information wird zurückgegeben? „Zugriff verweigert“, „Zugriff verweigert weil ...“, ...
- ◆ Der Zugriff wird so modifiziert, dass das Ergebnis die Menge der Berechtigungen widerspiegelt
 - Benutzer muss informiert werden, dass die Anfrage modifiziert wurde!
- ◆ Wo kann dies deklariert werden?
- ◆ Welche Berechtigungen fehlen?
 - Automatismus: Offenlegung der Policystruktur?
 - Ende des Automatismus: Kontaktierung einer verantwortlichen Person um benötigte Berechtigung zu erhalten

Zusammenfassung

- ◆ Verwendung von Web Services erfordert die Garantie von Sicherheitsbelangen
- ◆ Zugriffskontrolle ist Teil der Sicherheitsbelange
- ◆ Vorgestellte Zugriffskontrolle ermöglicht
 - Informationsbezogene Berechtigungen
 - Raumbezogene Berechtigungen
 - Deklaration von positiven und negativen Berechtigungen
 - Deklaration von Berechtigungen auf einzelne GeoObjekte oder eine Menge von diesen
- ◆ Auflösen von Inkonsistenzen

Letzte Folie

Vielen Dank für die Aufmerksamkeit

Fragen?