Sicherheitsaspekte von Web Services

- Diplom -

Mirko Richter
Technische Universität Dresden

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1 Einleitung

2 Hintergrund

2.1 Web Service

2.2 Service oriented Architecture (SOA)

2.3 OSI-Architektur

2.4 Kryptographische Grundlagen

2.4.1 Symmetrische Kryptographie

- Verwendung zweier Schlüssel, die in polynomialer Zeit auseinander bestimmbar sind

2.4.2 Asymmetrische Kryptographie

- Verwendung eines Schlüsselpaares (öffentlich und privat)

2.4.3 Verschlüsselung

- Umwandlung von Klartext in Chiffretext und umgekehrt

2.4.4 Signierung

- Signatur und Verifikation der Authentizität des Senders einer Nachricht durch so genannte "digitale Signaturen"

2.4.5 Hash-Funktionen

- Verwendung von "one-way"Funktionen

3 Web Service - Basistechnologien

3.1 Nachrichtenformat: XML/XSD

3.2 Transport: HTTP/HTTPS/SMTP/...

- Notice that SOAP is in layer 7, together with HTTP and SMTP. However, SOAP travels over HTTP or SMTP. This does not mean that SOAP belongs in a new layer, a layer 8.

3.3 Adressierung: WS-Addressing

3.4 SOAP

3.5 WSDL

3.6 UDDI/WS-MetadataExchange

3.7 BPEL4WS

4 Grundlegende Sicherheitsbetrachtungen

Es ist eine Tatsache, dass jedes Computersystem, welches in irgend einer Art mit anderen (potentiell unsicheren bzw. nicht kontrollierbaren) Systemen verbunden (Intranet, Internet etc) ist, einer permanenten Bedrohung durch Hacker[1], Cracker[2] und so genannte "Script Kiddies[3]" ausgesetzt ist.
Dabei ziehen sich die möglichen Angriffspunkte durch alle Ebenen der OSI-Architektur (Kap. 2.3).
Dieses Kapitel soll einen Überblick darüber geben, welche Aspekte eines Systemes zu schützen sind und mit welchen Bedrohungen in einem vernetzten System zu rechnen ist. Im letzten Teilkapitel wird aufgezeigt, wie sich die Bedrohungen in den letzten Jahren entwickelt haben und wo sie sich hinbewegen werden.

4.1 Schutzziele

Bei der Betrachtung von Sicherheitsaspekten für WebServices ist es wichtig zuerst eine Einteilung in unterschiedliche Schutzziele[4] vorzunehmen. Deren gesamtheitliche Betrachtung soll einen Überblick darüber geben, wie sich ein *sicherer* WebService definieren sollte.
Der Frage, ob Ansätze und eventuell sogar schon Implementationen für entsprechende Sicherheitsmechanismen existieren und wie sie zu bewerten sind, wird in den Kapiteln 6 und **??** nachgegangen.
In der nachfolgenden Unterteilung wird ebenfalls aufgezeigt, an welcher Stelle im Kommunikationsnetz mit Angriffen zu rechnen ist, deren Ziel es ist, das jeweilige Schutzziel auszuhebeln. Auf Bedienungs-, Soft- oder Hardwarefehler bzw. transitive Trojanische Pferde[5] innerhalb der verwendeten Software wird an diesen Stellen allerdings nicht explizit eingegangen, da diese bei allen Schutzzielen zu Einschränkungen in der Nutzung oder zu einer (bösartigen) Unterwanderung führen können.

[1] Versierter Spezialist, der versucht Lücken in Computersystemen aufzufinden mit der Absicht zu warnen (nur selten mit Missbrauchsabsicht).

[2] Versierter Spezialist, der, in der Regel mit Missbrauchsabsicht, versucht in veraltete Systeme oder schlecht geschützte Computersysteme kleiner Unternehmen, Regierungsstellen etc. einzudringen.

[3] Personen mit meist wenigen weiterreichenden Kenntnissen von Computer-Sicherheit, die (häufig unter Missbrauchsabsicht) versuchen mit Hilfe existierender Techniken, Programme oder Skripten, bekannte Schwachstellen in Computersystemen auszunutzen.

[4] Die Anzahl der nötigen Schutzziele variiert in der Literatur, da sich einige aus abstrakter Sicht auch zu einem einzigen zusammenführen lassen(z.B. 3 in [Pf00] und 6 in [Ec02]).

[5] Ein Systemteil ist ein Trojanisches Pferd, wenn er unter Ausnutzung der ihm anvertrauten Daten und Rechte *mehr* als das von ihm Erwartete oder von ihm Erwartetes *falsch* oder *nicht* tut.
Ein *transitives* Trojanisches Pferd ist ein Trojanisches Pferd, welches nicht durch einen unmittelbaren Angriff in das betroffene System eingeschleust wurde, sondern sich in der transitiven Hülle eines oder mehrerer Soft- bzw. Hardware-Entwurfshilfsmittel rekursiv bis in das betroffene System ausbreiten konnte[Pf00].

4.1.1 Vertraulichkeit

- Gewährleistung der Geheimhaltung von Daten

Nachrichten, die zwischen Web Service-Teilnehmern ausgetauscht werden, sollen vor allen anderen Instanzen (Netzbetreiber, mögliche Angreifer, etc.), außer den Kommunikationspartnern selbst, vertraulich bleiben.

Mögliche Angriffe auf Vertraulichkeit:

- Ausspähen der Nachricht auf dem Kommunikationsweg[6].
- Ausspähen der Nachricht durch den Netzbetreiber auf den durch ihn kontrollierten Knoten, falls dort eine protokollkonforme Ent- bzw. Umschlüsselung stattfindet.
- Ausspähen der Nachricht auf Geräten der Teilnehmer (Sender, Empfänger, Geräte des Netzbetreibers) durch einen externen Angreifer.

4.1.2 Integrität

Mit Hilfe dieses Schutzzieles soll jede unbefugte Manipulation gesendeter oder abgespeicherter Daten erkannt werden.
Eine Vielzahl von Autoren (z.B. [Pf00]) rechnet die Schutzziele Authentizität (Kap. 4.1.3) und Verbindlichkeit (Kap. 4.1.4) ebenfalls zu diesem Schutzziel. Aus Gründen der Verständlichkeit wurde in der vorliegenden Arbeit eine separate Betrachtung vorgenommen.

Mögliche Angriffe auf Integrität:

- Veränderung der Nachricht auf dem Kommunikationsweg.
- Veränderung der Nachricht durch den Netzbetreiber auf den durch ihn kontrollierten Knoten, falls dort eine protokollkonforme Ent- bzw. Umschlüsselung stattfindet.

4.1.3 Authentizität

- grundlegender Mechanismus zur Überprüfung der von einem Subjekt vorgegebenen Identität
- Authentifizierung = Verlust der Privatsphäre
- Unterscheidung von Authentifizierung:
  - **Nachricht** ("message authentication"): Empfänger einer Nachricht kann prüfen, ob sie von einem bestimmten Sender generiert und nicht modifiziert worden ist.
  - **Entität** ("entity authentication"): erlaubt Kommunikationspartnern ihre Identität zu prüfen

4.1.4 Verbindlichkeit

- entscheidet Fragen bezüglich Abstreitbarkeit

[6] Als Kommunikationsweg wird der Bereich spezifiziert, in dem sich das Nachrichtensignale außerhalb der beteiligten Sende- und Empfangs-Knoten ausbreitet (Kabel- oder Funkverbindungen, Router etc.).

4.1.5 Verfügbarkeit

4.1.6 Autorisierung

- auf Authorisierung basierender Dienst, der einem Objekt die Rechte, die es besitzt, zuschreibt

4.1.7 Privatheit

Dieses Schutzziel (in der Literatur auch als "Informationelle Selbstbestimmung" bezeichnet) Angriffsziele:

- mit der mobilen Kommunikation wird der Ort eines Gerätes oder Nutzers wichtige Information [Mue04]

4.2 Bedrohungen

Die Liste der möglichen Bedrohungen für ein auf WebServices beruhendes Kommunikationssystem lässt sich in *beabsichtigte* und *unbeabsichtigte* Bedrohungen unterteilen.

4.2.1 Ursachen

Bla

Beabsichtigte Aktive Bedrohungen [Ho03]:

- Trojanische Pferde
- Viren
- Würmer
- Maskerade
- Denial of Service
- Buffer Overrun

Beabsichtigte Passive Besrohungen [Ho03]:

- Elektromagnetische Abstrahlung
- Packet Sniffer
- Social Engineering

Unbeabsichtigte Bedrohungen Die unbeabsichtigten Bedrohungen sollen in dieser Arbeit nur der Vollständigkeit halber am Rande erwähnt werden, da sie für keine weitere Betrachtung vorgesehen sind. In diese Kategorie fallen Fehlverhalten, die zu einer Verletzung aller in Kapitel 4.1 aufgeführten Schutzziele führen können. Diese Bedrohungen abzuwenden obliegt verschiedenen anderen Wissenschaftszweigen. Dazu gehören z.B. [Ho03]:

- höhere Gewalt (z.B. Naturkatastrophen)
- menschliches Fehlverhalten (z.B Fehlbedienung)

- technisches Versagen (z.B. Fehlkonstruktion, Abnutzung)
- Umwelteinflüsse (z.B. Temperatur, Nässe, mechanische Einwirkung)

4.2.2 Folgen

[Mue04]:

- Nachahmung einer fremden Identität ("Spoofing")
- Unbefugte Änderung von Daten ("Tampering")
- Abstreitbarkeit ("Repudiation")
- Informationsenthüllung ("Information Disclosure")
- Dienstverweigerung ("Denial-of-Service")
- Anhebung der Berechtigung ("Elevation of rights")
- Profilbildung eines Nutzers (Aufenthaltsort etc.)

Schutzziele	Nachahmung der Identität	Unbefugte Änderung	Abstreit-barkeit	Ent-hüllung	Dienst-ver-weigerung	Erhöhung der Berechtigung	Profil-bildung
Vertraulichkeit	X	X		X			
Integrität	X	X				X	
Authentizität	X						
Verbindlichkeit	X	X	X	X			
Verfügbarkeit					X		
Autorisierung	X				X	X	
Privatheit							X

Bedrohungen werden meist kombiniert um einen Angriff auszuüben!

4.3 Statistik

Jahr	1995	1996	1997	1998	1999	2000	2001	2002	2003	1.Q - 3.Q 2004
Schwachstellen	171	345	311	262	417	1090	2437	4129	3784	2683
Sicherheitslücken	2412	2573	2134	3734	9859	21756	52658	82094	137529	???

Quelle: http://www.cert.org/stats/cert_stats.html
Schwachstellen = fehlerhaftes Design + "buggy"Implementierung
Gründe:

- zunehmend Abhängigkeit von Netzwerken
- starke Zunahme der Komplexität und der Dynamik von Software

5 Web Service - Sicherheitsbetrachtungen

In der Vergangenheit richteten sich die meisten Angriff gegen die unteren Ebenen dieser Architektur. Doch mit der Verbreitung von Web Services, die eine Verschiebung der Sicherheitsprinzipien in die Applikationsebene nach sich zog, richtet sich nunmehr der Fokus auch auf diese oberste Ebene des OSI-Modells. Dadurch ergibt sich die ganz neue Bedrohung in Enterprise Systeme einzubrechen, ohne dass die zur Zeit weit verbreiteten und ausgereiften Sicherheitsmechanismen der unteren OSI-Ebenen (Firewalls etc.) dagegen Schutz bieten könnten.

5.1 Angreifermodell

Da es bekanntermaßen keinen Schutz vor einem allmächtigen[7] Angreifer geben kann, wird in diesem Kapitel ein für das gewählte Szenario realistisches Angreifermodell erstellt.
Wer greift an:

- Hacker
- Cracker
- Script Kiddie

Wo befindet sich der Angreifer:

- von außen, "Outsiders"oder "Intruders"[Mue04]
- von innen "Insiders"oder "Saboteurs"[Mue04]

Wo findet der Angriff statt:

- zwei Dimensionen [Mue04]:
  - 1. Dimension: an welchem Knoten erfolgt der Angriff
  - 2. Dimension: Auf welcher OSI-Schicht erfolgt der Angriff

6 Web Service - Sicherheitsmechanismen

In diesem Kapitel sollen bereits existierende Sicherheitsmechanismen vorgestellt werden, die unter Aufsicht von Oasis bzw. dem W3C entstanden sind.

- the seven-layer communications stack still applies for each individual communication from a SOAP requester to a Web Service. However, one SOAP-based communication is not the full story. Web Services security presents three challenges:
  - The challenge of security based on the end user of a Web Service
  - The challenge of maintaining security while routing between multiple Web Services
  - The challenge of abstracting security from the underlying network

[7] Ein allmächtiger Angreifer könnte alle für ihn interessanten Daten an der Stelle ihrer Entstehung erfassen, nach Belieben unbefugt verändern und/oder das betroffene IT-System durch physische Zerstörung etc. in seiner Funktionalität beliebig beeinträchtigen [Pf00].

6.1 XACML

XACML (Extensible Access Control Markup Language)

6.2 SAML

6.3 XML-Digital Signature

6.4 XML-Encryption

6.5 WS-Security

6.6 WS-Policy

6.7 WS-SecurityPolicy

6.8 WS-Trust

6.9 WS-SecureConversation

6.10 WS-Federation

6.11 ebXML

6.12 XKMS

6.13 Zusammenspiel

6.13.1 The Liberty Alliance Project

7 Web Service - Angriffsszenarien

7.1 Mann in der Mitte

- [Mue04] einem Angreifer gelingt es, den Kommunikationskanal soweit unter seine Kontrolle zu bringen, das die "Abgehörten"nicht feststellen können, ob sie tatsächlich miteinander oder mit dem Angreifer kommunizieren
  Nutzen: unberechtigter Zugang zu Informationen, Manipulationen oder Übernahme kompletter Datenverbindungen ("connection hijacking")

8 Abkürzungsverzeichnis

9 Referenzen

Literatur

[Ec02] Eckert, Claudia: *Sicherheit*, XML-Workshop FhG-IPSI, Darmstadt, November 2002

[Ho03] Holznagel, Bernd: *Modul X: Grundlagen des Rechts der IT-Sicherheit*, Vorlesungsscript Rundfunkrecht, Universität Münster, WS 2003/2004

[Mue04] Müller, Günter: *Telematik 4 / IT-Sicherheit*, Vorlesungsscript Telematik, Freiburg, WS 2004/2005

[Pf00] Pfitzmann, Andreas: *Sicherheit in Rechnernetzen*, Oktober 2000

Eidesstattliche Erklärung

Ich erkläre hiermit, dass ich die vorliegende Arbeit selbständig und nur unter Verwendung der aufgeführten Literatur erstellt habe.

Dresden, den 22. Dezember 2004