Die Softwarearchitektur von Grid Computing

Ron Trautsch
HfT-Stuttgart, Studiengang Informatik, WS 07/08
26. Dezember 2007

Inhaltsverzeichnis

1. Einleitung

Eine allgemein akzeptierte Regel der Informatik sagt: „Je komplexer ein vorhandenes System ist, desto mehr Möglichkeiten gibt es, dieses anzugreifen“.
Auch im Bereich Grid Computing musste man das erkennen.
Nachdem die erste Euphorie, die vor ca. 5 Jahren ihren Höhepunkt erreichte, abgeklungen war, wurde das Thema Sicherheit immer wichtiger. Viele namhafte Experten äußersten sich sehr kritisch und verwiesen auf viele Schwachstellen und potentielle Gefahrenquellen.
Seitdem wurde mit enormem Aufwand an Sicherheit - Konzepten und auch bereits Realisierungen gearbeitet. Da das Interesse der Wissenschaft, Wirtschaft und Politik an Grid Systemen nach wie vor groß ist, stellt sich heute die Frage, inwieweit man Fortschritte gemacht hat und ob die heutigen Grid Systeme sicher vor äußeren Angriffen sind. Da das Grid Computing durch Software umgesetzt wird, ist es wichtig, dass die Softwarearchitektur des Grid Computing einen Stand der Sicherheit aufweist, bei dem es Angreifern nicht möglich ist, dem System zu schaden.

Im Folgenden soll das theoretische Konzept des Grid Computing,
die Gefahren für das System, sowie die Sicherheitsanforderungen – und Mechanismen erläutert werden.

2. Theoretisches Konzept

2.1 Grundlagen

Es geht im Grid Computing darum, in dynamischer Weise die Kapazitäten von Hochleistungsrechnern den Benutzern je nach Bedarf zur Verfügung zu stellen.
Die Kapazitäten eines Hochleistungsrechners sind vor allem die Rechen – oder Speicherkapazität.
Der Benutzer soll nicht mehr lokale Ressourcen nur für sich verwenden, sondern die Gesamtressourcen aller Rechner im Grid soll allen zur Verfügung stehen.
Dieses Konzept hat weit reichende Konsequenzen:
Es führt dazu, dass der Benutzer eines Grid Systems in einem kontrollierten Maß soviel Rechenkapazitäten nutzen kann, dass Aufgaben mit bisher zu großem Rechenaufwand nun bewältigt werden können.
Andererseits führt es aber auch zur effektiveren Ausnutzung der Ressourcen und zu einer Balancierung der Arbeitslasten. Als Kommunikationsmedium dient das Internet.
Da sehr viele Benutzer im Grid tätig sein können, ist eine Allokationsverwaltung nötig, die jedem Benutzer je nach Rechten und Priorität der Anforderung, Ressourcen zur Verfügung stellt. Dabei soll einem Benutzer nicht bekannt sein, wo sein Auftrag bearbeitet oder gespeichert wird oder ob sein Auftrag auf einem Server oder einem ganzen Verbund von Servern parallel läuft.

Diese Transparenz soll dazu führen, dass der Benutzer das Gefühl hat, in unkomplizierter Weise lokal zu agieren und keinen Eindruck von der komplexen Architektur, die sich hinter dem Grid verbirgt, bekommt.
Doch um zu verstehen, wie ein Grid System funktioniert, ist es wichtig, grundsätzliche Komponenten des Systems zu kennen:

Die Benutzerschnittstelle ist eine solche Komponente. Praktisch alle Daten mit denen ein Benutzer arbeitet, werden von einem Server über diese Schnittstelle in den lokalen Arbeitsspeicher geladen, dann dort vom Benutzer manipuliert und wieder auf einem Server gespeichert. Als Server bezeichnet man einen Rechner im Netzwerk, auf dem mehrere Serverdienste laufen, die die Aufträge der Benutzer im Netzwerk bearbeiten. Der dienst - anfragende Rechner des Benutzers, wird als Client bezeichnet.

Eine Rechenressource des Grid wird Computing Element genannt und setzt sich aus einem Gatekeeper und einen oder mehrere Worker Nodes zusammen.
Worker Nodes sind die konkreten Server, Cluster oder auch Supercomputer auf denen die Aufträge ausgeführt werden. Der Gatekeeper ist das Frontend zum Computing Element. Er nimmt Aufträge in einer Warteschlange entgegen, prüft sie und transferiert sie zu freien Worker Nodes.

Eine weitere wichtige Komponente ist das Storage Element.
Das Storage Element bietet einen einheitlichen Zugriff auf Speichermedien aller Art. Auch wenn es dem Benutzer unbekannt ist, auf welches Medium seine Daten real gespeichert werden, so soll doch der Zugriff darauf von unterschiedlichsten Anwendungen aus einheitlich und geregelt sein.

Die zentrale Komponente eines Grid Systems ist der Resource Broker.
Er nimmt die Aufträge der Benutzer entgegen, prüft sie, untersucht die Auftragsbeschreibung und delegiert die Anforderung zu den passenden und erreichbaren Ressourcen.

Damit alle Komponenten eines Grid Systems kommunizieren können, muss es Standard Protokolle geben, die diese Kommunikation steuern.

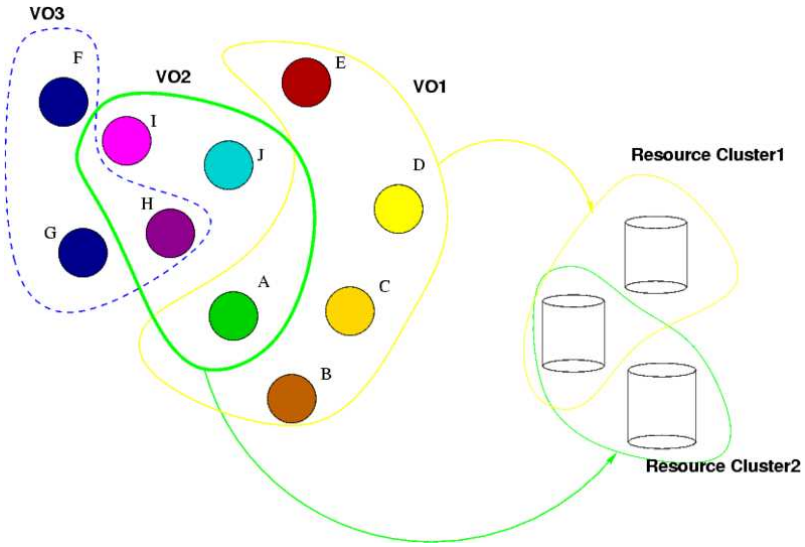
2.2 Dienste

In den letzten Jahren hat ein Siegeszug der Web Services im Internet stattgefunden. Ein Web Service ist zunächst mal ein Internet Dienst wie z.B. Email, der von einem Client angefordert werden kann. Das Besondere ist jedoch, dass ein einheitlicher Zugriff auf entfernte Anwendungen über globale Internet Protokolle möglich gemacht wurde. Das bedeutet, dass Anwendungen, die in unterschiedlichen Programmiersprachen entwickelt wurden, die gleichen Dienste nutzen können.
Als globales Kommunikationsformat zwischen unterschiedlichen Systemen hat sich XML durchgesetzt.

Gerade die Interoperabilität die durch Web Services erzielt wurde, macht auch in Grid Systemen viel Sinn, da es möglich sein soll, Ressourcen aller Art zu nutzen.
Es soll Benutzern auf unterschiedlichen Systemen möglich sein, denselben entfernten Dienst zu nutzen, ohne ihre lokalen Anwendungen anzupassen oder gar umprogrammieren zu müssen. So wurde es nötig, eine Architektur zu entwickeln, die Web Services benutzt um Grid Funktionalität auszuführen.
[1] Eine bekannte Architektur des Grid Computing ist die OGSA(Open Grid Service Architecture). Ihre Hauptaufgaben sind die Unterstützung von heterogenen Ressourcen, das Management verteilter Daten, die Sicherheit und Skalierbarkeit des Systems und die Verfügbarkeit der Systemkomponenten.
Auch wenn es sinnvoll ist, dass Benutzer Ressourcen aller Art nutzen können, so ist es dennoch nicht zweckmäßig, dass alle Benutzer Zugriff auf alle Ressourcen haben.

2.3 Zugriffsrechte

Je nach Tätigkeit unterscheidet sich die Art der Ressourcen auf die ein Benutzer zugreift und auch die Art der Aufträge an denen er arbeitet.
Im Grid Computing gibt es ein zentrales Konzept, um diese Benutzer in Gruppen einzuteilen und diesen Gruppen definierte Rechte auf Ressourcen zuzuweisen.
Eine solche Gruppe wird virtuelle Organisation genannt.
Eine virtuelle Organisation kann ein Zusammenschluss von Personen, Personengruppen, Unternehmen, Projektteams oder Universitäten sein.
Dabei handelt es sich aber nicht um ein statisches Konzept, sondern es ist möglich dynamisch Veränderungen an einer virtuellen Organisation vorzunehmen.
Für eine volle Ausnutzung der Kapazitäten ist es notwendig, dass eine Ressource wie ein Cluster von mehreren virtuellen Organisationen genutzt wird. Zusätzlich kann eine Person auch in mehren virtuellen Organisationen involviert sein(siehe Abbildung[1]).



Abbildung[1]:
Bei den Teilnehmern einer VO kann es sich um rechtlich unabhängige Unternehmen oder auch Einzelpersonen handeln. (Im Bild mit den Buchstaben A-J gekennzeichnet). Dritten gegenüber treten diese Zusammenschlüsse als ein einheitliches Unternehmen auf(Im Bild mit VO1-VO3 beschrieben).

Schon bei Überlegungen zur grundsätzlichen Funktionsweise eine Grid Systems, sind einige Gefahren, die es Angreifern möglich machen, Schaden anzurichten, offensichtlich. Diese zu erkennen und zu analysieren ist die Grundlage für das Sicherheitskonzept eines Systems und deshalb ist es wichtig die heutigen Grid Systeme auf Unsicherheiten und Gefahren zu untersuchen.

3. Gefahren

3.1 Die Komplexität des Systems

[2] Je komplexer ein System ist, desto höher ist der Aufwand um dieses sicher zu machen. Will man diesen Aufwand reduzieren, muss man das System vereinfachen oder Sicherheitsrisiken eingehen. Die Sicherheit eines Systems ist also abhängig von der Komplexität.
Es gibt mehrere Aspekte, die zur wachsenden Komplexität und damit Angreifbarkeit von Grid Systemen führen. Dabei ist es oft so, dass ein Vorteil des Grid Computing auch einen Nachteil mit sich bringt. Ein wichtiger Faktor ist dabei die hohe Skalierbarkeit des Systems.
Aufgrund der Skalierbarkeit ist es kaum ein Problem neue Rechenressourcen zu integrieren. Dies führt dazu, dass Grid Netze sehr schnell wachsen können.

Die Gefahr ist dabei, dass Ressourcen nicht völlig korrekt zugeteilt werden.
Für jede Ressource im Grid, muss es zu einem Zeitpunkt einen eindeutig definierten Benutzerkreis geben, der sie nutzen darf und dies muss bei Veränderungen am System streng überwacht werden. Im schlechtesten Fall bekommt ein Benutzer Zugang zu Ressourcen, die er eigentlich nicht benutzen darf.
Die Heterogenität der virtuellen Organisationen ist ein weiterer Faktor für die steigende Komplexität. Virtuelle Organisationen können sich in der Art der Architektur, Betriebssysteme und Anwendungen stark unterscheiden.
Gerade der große Vorteil, den die OGSA mit der Interoperabilität möglich macht, hat den Nachteil, dass das System sehr viel komplexer ist, als wenn es eine einheitliche Kommunikation zwischen allen Anwendungen und Diensten gäbe.
Der Preis für die Interoperabilität, ist die steigende Komplexität.
Ein weiterer Faktor ist das verteilte Rechnen.
Die Prozessverwaltung eines Systems, das einen Auftrag auf mehrere parallel rechnende Server verteilt, ist um einiges komplexer als die Begrenzung auf einen Server. Das liegt daran, dass die Server ständig ein hohes Kommunikationsaufkommen zwischen den Threads haben. Threads sind einzelne parallel laufende Ausführungsstränge eines Prozesses, die gemeinsam die Betriebsmittel eines Prozesses nutzen. In einem verteilten System wie dem Grid, können die Threads eines Prozesses auch auf mehrere Server verteilt werden damit ein Prozess schneller bearbeitet werden kann. Damit die Daten, die solch ein Prozess bearbeitet, einen konsistenten Zustand behalten, müssen die Threads ständig miteinander kommunizieren. Bei steigender Anzahl aktiver Benutzer ist die Prozessverwaltung deshalb alles andere als schlank.
Dabei ist noch nicht berücksichtigt, dass ein Resource Broker zuvor erst prüfen muss, ob ein Prozess überhaupt auf einem Server laufen darf.

Ein System wie das Grid, muss aufgrund der Komplexität nicht zwangsläufig unsicher sein, doch die Komplexität ist eine grundsätzliche Gefahr für das System.
Zur wachsenden Komplexität kommt noch eine weitere Gefahr:
Die bedingte Offenheit der Rechner.

3.2 Bedingte Offenheit der Rechner

Das grundsätzliche Sicherheitsproblem bei Grid Computing ist die Tatsache, dass sehr viele Ports von Servern offen sein müssen.
Ein Port ist eine Schnittstelle zwischen Netzwerkkabel und Rechner, wobei nur Datensegmente eines festgelegten Dienstes übertragen werden.
So kann z. B. eine Datei per FTP(*File Transfer Protocol*) nur über den Port 23 übertragen werden.
Die Offenheit hängt also mit der Anzahl der Dienste und deren Nutzung zusammen. Je mehr Dienste verfügbar sein sollen, desto mehr feste oder variable Ports müssen offen sein und je mehr Ports offen sind, desto mehr Möglichkeiten gibt es für einen potentiellen Angreifer, diese zu nutzen.

Da ein Benutzer des Grid über das Internet auf die Ressourcen zugreift, ist der potentielle Angreiferkreis nicht lokal begrenzt, sondern jeder Internetnutzer kann zu einem unerwünschten Eindringling werden.
Natürlich gibt es Möglichkeiten, die Rechner zu schützen, doch die grundsätzliche Herausforderung ist die, ein Mittelmaß zwischen schwerlastigen Sicherheitschecks und einen schnellen und einfachen Zugriff auf Ressourcen zu gewährleisten, was die Grundidee und der große Vorteil des Grid Computing ist.
Die Performance darf nicht zu sehr unter den Schutzmechanismen leiden.
Wenn das Sicherheitsmanagment so sehr „stört“, dass der Zeitaufwand für mehr Rechenkapazität dem einer normalen Netzwerkarchitektur mit starr begrenzten Rechenkapazitäten entspricht, dann ist Grid Computing unnötig, sinnlos und zu teuer.

3.3 Steigender Administrationsaufwand

Mit der steigenden Komplexität und dem steigenden Aufwand für die Bereitstellung von Diensten, steigt auch die Verwaltungsarbeit von Administratoren.
Vor allem bei der Einsetzung von Grid Systemen in Unternehmen, die eine individuelle Personalpolitik betreiben, kann das gefährlich werden.
Falls zu wenige Administratoren eingestellt werden, um Kosten zu sparen, wird auch an der Sicherheit gespart.

Bei all den Vorteilen die das Grid Computing bringt, ist es fatal, den Faktor Sicherheit nicht voll zu berücksichtigen. Aufgrund der Gefahren, die offensichtlich vorhanden sind, ist es wichtig, die Sicherheitsanforderungen klar zu definieren.

4. Sicherheitsanforderungen

4.1 Einbruchsicherheit

Einbruchsicherheit ist die grundlegende Eigenschaft eines sicheren Systems.
Wenn diese nicht gewährleistet ist, dann sind Daten gefährdet.
In erster Linie wird die Einbruchsicherheit dadurch gewährleistet, dass Datensegmente mit einer unbekannten IP Adresse verworfen werden.
Die IP Adresse identifiziert einen Rechner im Internet. Wenn also ein Benutzer, der nicht zum Grid gehört, eine Grid Ressource nutzen will, sollte dies mit seiner tatsächlichen IP Adresse nicht möglich sein.

Dadurch wäre die Sicherheit des Systems jedoch nur teilweise gewährleistet.
Nicht berücksichtigt ist, dass sich ein Angreifer für jemand anders ausgeben könnte, indem er seine Zugangsdaten so manipuliert, dass er als ein tatsächlicher Grid Nutzer in Erscheinung tritt. Dem tatsächlichen Grid Nutzer darf es dagegen nicht möglich sein, auf Ressourcen zuzugreifen, auf die er keine Rechte besitzt.
Um dieser Sicherheitsanforderung gerecht zu werden, wären Zertifikate sehr sinnvoll.

4.2 Digitale Zertifikate

Im Allgemeinen ist ein Zertifikat eine Beglaubigung, dass eine Person eine bestimmte Eigenschaft besitzt. Im Falle eines digitalen Zertifikats im Grid ist das die Eigenschaft, dass ein Benutzer der ist, der er vorzugeben scheint.
Hierzu müssten eine Reihe von Informationen gespeichert werden [3]:

1. Den Namen (oder eine andere eindeutige Bezeichnung) des Ausstellers (engl. Issuer) des Zertifikates.
2. Informationen zu den Regeln und Verfahren, unter denen das Zertifikat ausgegeben wurde.
3. Informationen zu Gültigkeitsdauer des Zertifikates.
4. Den öffentlichen Schlüssel, zu dem das Zertifikat Angaben macht.
5. Den Namen (oder eine andere eindeutige Bezeichnung) des Eigentümers des öffentlichen Schlüssels (engl. Subject).
6. Weitere Informationen zum Eigentümer des öffentlichen Schlüssels.
7. Angaben zum zulässigen Anwendungs- und Geltungsbereich des öffentlichen Schlüssels.
8. Eine digitale Signatur des Ausstellers über alle anderen Informationen.

Als Schlüssel bezeichnet man eine große(meist 1024 Bit) Zufallszahl, die bei erfolgreicher Decodierung einen Kommunikationspartner identifiziert.
Die Verwendung eines öffentlichen Schlüssels verweist bereits auf ein asymmetrisches Verschlüsselungsverfahren. Im Gegensatz zum symmetrischen Verschlüsselungsverfahren, wo jeweils beide Kommunikationspartner denselben geheimen Schlüssel besitzen, gibt es hier für jeden Partner einen geheimen und einen öffentlichen Schlüssel.
Für ein Grid System mit einer meist großen Benutzeranzahl wäre dieses Verfahren geeigneter, weil man beim symmetrischen Verschlüsselungsverfahren die geheimen Schlüssel aller möglichen Kommunikationspartner speichern müsste und zusätzlich noch das Problem der Schlüsselverteilung hätte.

Somit stellen digitale Zertifikate das Mittel dar, um einen Benutzer eindeutig zu authentifizieren, seinen Zugriffsbereich festzulegen und so eine wichtige Sicherheitsanforderung zu erfüllen.

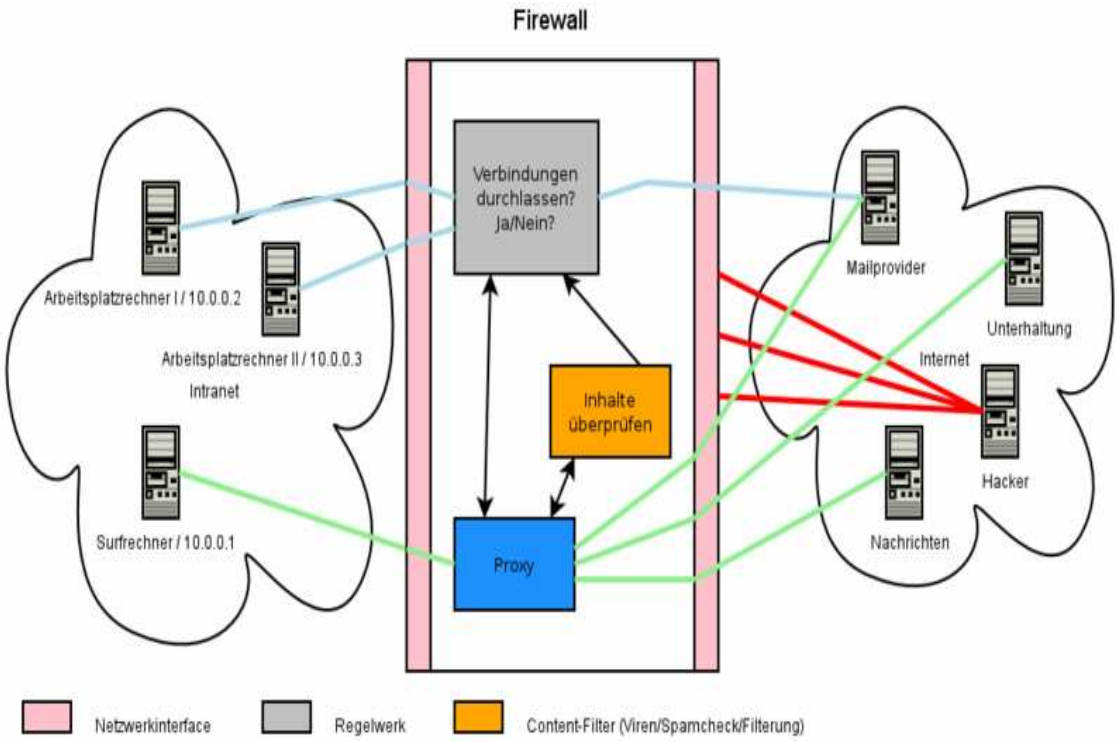
4.3 Verfügbarkeit

Eine allgemeine Anforderung an jedes System, ist eine möglichst hohe Verfügbarkeit. Ein erfolgreicher Angriff auf diese, kann das ganze System lahm legen. Dies könnte von einem potentiellen Angreifer durch einen sog. DoS Angriff erreicht werden. Mit einem „Denial of Service“ Angriff überlastet der Angreifer einen Server durch immer ständig generierten Anfragen solange, bis keine Kommunikation mehr möglich ist. Dies wird meist dadurch erreicht, dass es dem Angreifer gelingt, Fremdsoftware im entsprechenden System zu installieren. Eine unbedingte Anforderung ist es, die Gefahr dieser Art von Angriffen zu minimieren.

5. Sicherheitsmechanismen

5.1 Firewalls

Einbruchsicherheit ist die erste Sicherheitsanforderung des Grid Systems.
Diese wird in erster Linie durch Firewalls erreicht.
Grundsätzlich müssen zwei Arten von Firewalls unterschieden werden.
Die Personal Firewall ist auf dem lokalen Rechner den sie schützen soll als reine Software aktiv. Die Netzwerk Firewall ist dagegen eine Hardware Komponente mit mehreren Netzwerkschnittstellen, die zwei Netze voneinander trennt und den Datenverkehr des einen Netzes in das andere kontrolliert.
Dabei werden die Absender IP - Adresse, Ziel - IP Adresse,
Netzwerk – Protokoll, Port Nummer, Aktion und mehrere Nebenbedingungen geprüft.
Beim Ersteinsatz einer Firewall ist vorerst jede Verbindung verboten. Dann werden die Verbindungsparameter der erlaubten Zugriffe gespeichert und nur Pakete, die diesen Parametern entsprechen, werden durchgelassen.
Konkret auf ein Grid System umgesetzt spielen beide Arten von Firewalls eine Rolle.
Auf jedem Worker Node befindet sich eine konfigurierte Personal Firewall.
Zwischen dem Computing Element und dem Grid befindet sich wiederum eine Netzwerk Firewall. Zwischen dem Grid und dem Internet befinden sich ebenfalls Firewalls, sodass eine Anforderung an eine Ressource durch bis zu 5 Firewalls gelangen muss. Speziell zwischen dem Grid und dem Internet realisiert die Firewall zusätzlich eine Proxy Funktion, wodurch die IP Adressen des internen Netzes verborgen bleiben.



Abbildung[2]: Eine Firewall sorgt dafür, dass nur festgelegte Verbindungen z.B. ins Internet zugelassen werden. So dürfen die Arbeitsplatzrechner nur mit dem Mailserver kommunizieren. Der Surfrechner hat Zugriff auf das Internet, jedoch nur über einen Proxy – Dienst, der dessen IP Adresse verbirgt.

Bei der Integrierung neuer Dienste oder Benutzer müssen die Firewalls von Administratoren so konfiguriert werden, dass die entsprechenden Pakete nicht verworfen werden. Deshalb ist es für einen Angreifer nicht möglich in ein Grid System einzubrechen ohne sich mit einer gestohlenen Authentifizierung Zugang ins Grid zu verschaffen.

Dies führt zu der zweiten Sicherheitsanforderung:
Es soll einem Angreifer nicht möglich sein, sich für einen tatsächlichen Grid Nutzer auszugeben und es soll für einen Grid Nutzer nicht möglich sein, über die eigenen Rechte hinaus zu agieren. Als ein geeignetes Mittel hierfür wurde das digitale Zertifikat in Verbindung mit einem asymmetrischen Verschlüsselungsverfahren vorgeschlagen.

5.2 Authentifizierung und Autorisation

Es ist bereits ersichtlich geworden, warum sich asymmetrische Verfahren für Grid Systeme besser eignen als symmetrische. Das meist verwendete asymmetrische Verschlüsselungsprotokoll in Grid Systemen ist SSLv3.
[4] Das SSL Protokoll besteht aus zwei Schichten:
Das SSL Record Protocol ist die untere Schicht und ist zuständig für eine gesicherte Ende – zu – Ende Verschlüsselung, sowie die Bildung einer Prüfsumme um die Nachrichten – Integrität zu gewährleisten. Die Nachrichten – Integrität bedeutet hierbei die Sicherheit, dass eine Nachricht während der Übertragung nicht manipuliert wurde.
Das SSL Handshake Protocol ist die obere Schicht und ist für die Authentifizierung der Kommunikationspartner, die Zertifizierung der Verbindungsdaten und die Auswahl der verwendeten Schlüssel und Algorithmen zuständig.
Der SSL Handshake läuft dabei in 4 Phasen ab:

1. Phase:

   In der ersten Phase machen sich die beiden Kommunikationspartner durch das so genannte Client_hello und Server_hello bekannt.
   Beim Client_hello sendet der Client folgende Parameter zum Server:
   Die verwendete SSL Version, eine Zufallszahl, eine Session ID und die verwendeten Verschlüsselungs- und Kompressionsmethoden.

   Durch das Server_hello antwortet der Server, indem er sich auf die Session ID und wenn möglich auf die Verschlüsselungs- und Kompressionsmethoden einstellt. Ebenfalls sendet er eine Zufallszahl an den Client.
   Mit Hilfe der Session ID kann später eine Session auch nach einer Unterbrechung fortgesetzt werden, falls der Server dies zulässt.
   Die Zufallszahl, deren Größe je nach Verschlüsselungsverfahren variiert, wird später für den Premaster Schlüssel verwendet.

2. Phase:

   In dieser Phase identifiziert sich der Server gegenüber dem Client, indem er das digitale Zertifikat übermittelt und gleichzeitig ein digitales Zertifikat vom Client anfordert.

3. Phase:

   Der Client überprüft die Gültigkeit des digitalen Zertifikats durch die digitale Signatur des Ausstellers und bricht ab, falls diese ungültig ist. Andernfalls sendet der Client nun das eigene digitale Zertifikat und wartet entsprechend auf die Bestätigung des Zertifikats durch den Server.

4. Phase:

   Nachdem die Identität der beiden Kommunikationspartner gesichert ist, wird nun durch die Codierung der zu Anfangs gesendeten Zufallszahlen mit den öffentlichen Schlüsseln der Premaster Schlüssel generiert. Durch eine Hash Funktion wie SHA-1 oder MD5, die jedem möglichen Text einen definierten Hash Wert zuordnen, wird aus dem PreMaster ein Master Schlüssel generiert. Dieser ist auf beiden Seiten äquivalent, obwohl jede Seite unterschiedliche Zufallszahlen zur Erzeugung des Premaster Schlüssels verwendet haben. Dieser wird nun einmalig zur Verschlüsselung der Daten verwendet.

SSL ist ohne eine zertifikatsbasierte Authentisierung unsicher, weil ein zwischengeschalteter Kommunikationspartner, der sich für den Client als Server und für den Server als Client ausgibt, den gesamten Datenverkehr kontrollieren könnte. Diese Art von Angriff nennt man Man – in – the – Middle - Angriff.
Deshalb wird in Grid Systemen SSLv3 nur in Verbindung mit digitalen Zertifikaten verwendet. Einem Angreifer ist so nicht möglich, sich für jemand anders auszugeben. [5] Das am häufigsten verwendete Grid Computing Sicherheitssystem GSI(Global Security Infastructure) liegt diesem Prinzip zugrunde.

Neben der Authentifizierung war die korrekte Autorisation tatsächlicher Grid Nutzer eine weitere Sicherheitsanforderung.

Dass ein Benutzer auch nur Aufträge an die Ressourcen anfordern kann, die ihm frei stehen, ist eine der zentralen Aufgaben des Resource Brokers. Ein Resource Broker hat Zugang zu sämtliche Informationen über Zugriffsrechte der Benutzer, die er vermitteln muss. Er ist so konfiguriert, dass er einem Benutzer nur Ressourcen zuweist, die für den Benutzer den Status „verfügbar“ besitzen.
Hier wird die zentrale Funktion des Resource Brokers deutlich und da nur die Systemadministratoren auf ihm Konfigurationen vornehmen dürfen, gibt es für einen Benutzer keine Möglichkeit, über die eigenen Rechte heraus zu agieren.

Es gibt noch einen anderen Grund, warum eine Ressource nicht verfügbar ist:
Ein Server könnte aufgrund von technischen Problemen ausfallen.

5.3 Ausfallsicherheiten

Ein Serverausfall ist in einem Grid System deshalb ein ernst zu nehmendes Problem, weil Grid Systeme auf der Benutzerseite sehr oft mit Thin Clients ausgestattet sind. Ein Thin Client hat nur die Aufgabe der Ein – und Ausgabe von Daten, während die gesamte Verarbeitung und Speicherung der Daten auf einem Server stattfinden.
Der Vorteil einer solchen Architektur ist die hohe Skalierbarkeit, da man nur Änderungen auf dem Server vornehmen muss und sich dies automatisch auf alle Clients auswirkt.

Ein Nachteil ist, dass bei einem Serverausfall nicht die geringste Aktivität eines Benutzers an seinem Rechner mehr möglich ist. Nicht gespeicherte Daten gehen verloren. Aufgrund dessen müssen replizierte Server eingesetzt werden.
Inwieweit replizierte Server eingesetzt werden, ist weitgehend eine Kostenfrage. Man unterscheidet zwischen replizierten Servern, die bei einem Ausfall erst hochgefahren werden müssen und solchen die automatisch die ausgefallene Komponente ersetzten. Für ein Grid System sind replizierte Server unabdingbar, um eine hohe Verfügbarkeit zu garantieren.

6. Schluss

Es ist durch diese Betrachtung ersichtlich geworden, wie Grid Systeme funktionieren, wie Dienste umgesetzt werden, was virtuelle Organisationen sind,
welche Herausforderungen und Gefahren es gibt und mit welchen Mitteln Schäden von außen wie von innen, durch zuverlässige Sicherheitsmechanismen vermieden werden.
Besonders in diesem abschließenden Teil, hat sich gezeigt, dass die heutige Softwarearchitektur des Grid Computing alles andere als unsicher ist.
Natürlich wird man im Sicherheitsmanagement nie zu einem Ende kommen, da es immer neue „Einbruchstechniken“ geben wird, aber das Konzept Grid Computing ist in seinem anfänglichen Höheflug daran nicht gescheitert, weil man sich rechtzeitig mit realistischen Überlegungen zur Sicherheit beschäftigt hat.
Die Softwarearchitektur des Grid Computing hat derzeit genügend Sicherheitsmechanismen um sowohl im wissenschaftlichen, als auch im kommerziellen Bereich als sicher zu gelten und hat damit Zukunft.

7. Quellenverzeichnis

Inhalte:

[1] Dienste und Standards für das Grid Computing, 16.10.2007,
http://www.zib.de/CSR/Publications/2004-reinefeld-lni.pdf

[2] Leitfaden IT Sicherheit - Bundesamt für Sicherheit in der Informationstechnik, Referat 114
IT-Sicherheitsmanagement und IT-Grundschutz, 16.10.2007,
http://www.web-creative.org/leitfaden-itsicherheit.html

[3] Wikipedia Artikel – Digitale Zertifikate, 08.12.2007,
http://de.wikipedia.org/wiki/Digitales_Zertifikat

[4] Wikipedia Artikel – Transport Layer Security, 08.12.2007,
http://de.wikipedia.org/wiki/Transport_Layer_Security

[5] Seminar Grid-Computing –
Eberhard-Karls-Universität Tübingen, 26.12.2007,
http://www-ti.informatik.uni- tuebingen.de/~behrend
/lehre/06/ausarbeitung/GridSicherheit_Ausarbeitung.pdf

Bilder:

Abbildung[1]: Virtuelle Organisation
http://de.wikipedia.org/wiki/Bild:VirtOrg.png

Abbildung[2]: Aufbau einer Firewall
http://de.wikipedia.org/wiki/Bild:Konzeptioneller_Aufbau_einer_Firewall.png

Bücher:

Grid Computing – Making the Global Infastructure a Reality,
von Fran Berman, Geoffrey C. Fox und Anthony J. G. Hey, 2003

The Grid: Blueprint for a New Computing Infrastructure,
Von Ian Foster und Carl Kesselmann, 2004