Evaluation von Security-Mechanismen in Grid-Umgebungen[1]

Christian Grimm, Stefan Piger, Jan Wiebelitz

Regionales Rechenzentrum für Niedersachsen (RRZN)
Leibniz Universität Hannover
Schloßwender Straße 5
30159 Hannover
grimm@rrzn.uni-hannover.de
piger@rrzn.uni-hannover.de
wiebelitz@rrzn.uni-hannover.de

Abstract: In diesem Beitrag werden sowohl Verfahren zur Authentifizierung und Autorisierungen als auch der Einsatz von Firewalls in Grid-Umgebungen dargestellt und kritisch bewertet. Obwohl die Anforderungen an diese Verfahren aufgrund der Komplexität von Grid-Umgebungen hoch sind, wird heute bereits ein grundlegendes Sicherheitsniveau erreicht. Dennoch stellen sich bei der hier durchgeführten näheren Betrachtung konzeptionelle Schwächen dar, die den Einsatz von Grid-Computing in Umgebungen mit hohen Sicherheits-Anforderungen derzeit erheblich erschweren.

1 Einleitung

Die Komplexität und natürliche Verteiltheit von Grid-Umgebungen erfordern ausgeprägte Security-Mechanismen zum Schutz gegenüber möglichen Angriffen. Besondere Ressourcen wie Hoch- und Höchstleistungsrechner oder Archivspeicher sowie die z. T. sensiblen Daten der Nutzer erfordern ein hohes Maß an Absicherung, um geeignet in einem Produktionsbetrieb für Grid Computing eingesetzt werden zu können. Die derzeit in Grid-Umgebungen verwendeten Ansätze für Authentifizierung und Autorisierung liefern zwar – durch den Einsatz etablierter *Public Key Infrastructures* (PKI) – einen grundlegenden Schutz vor nicht autorisierten Zugriffen. Die zugrunde liegenden Konzepte wie Proxy-Zertifikate mit befristeter Gültigkeit, Abbildung von Nutzern auf Poolaccounts oder die verglichen mit Java rudimentären Sandbox-Umgebungen bilden derzeit jedoch Schwachstellen, die von potentiellen Angreifern genutzt werden können.

---

[1] Das diesem Bericht zugrunde liegende Vorhaben wird mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01AK800B gefördert.

Ziel des Beitrags ist die kritische Beurteilung ausgewählter sicherheitsrelevanter Aspekte in Grid-Umgebungen. Hierbei ist insbesondere die Situation aus Sicht der Ressourcen-Betreiber, wie sie z. B. Rechenzentren von Hochschulen oder Forschungseinrichtungen darstellen, von Interesse. Am Beispiel der Grid Middleware gLite wird zunächst ein kurzer Überblick über Authentifizierung und Autorisierung sowie die Verarbeitung von Jobs in Grid-Umgebungen gegeben. Ausgehend hiervon werden ausgewählte Angriffsszenarien erläutert und Ansätze zu deren Behebung aufgezeigt.

2 Grid-Umgebung am RRZN

Das RRZN betreibt zusammen mit Partnern in dem EU-Projekt *Enabling Grids for E-sciencE* (EGEE) ein Grid Testbed auf Basis der Grid Middleware gLite. gLite wird im Rahmen von EGEE entwickelt und bereits jetzt zur Vorbereitung der in 2007 beginnenden Experimente des *Large Hadron Colliders* (LHC) eingesetzt. Das gLite Testbed am RRZN dient vollständigen Systemtests der neuesten Versionen von gLite, bevor sie in den produktiven Einsatz übergeben werden. Es umfasst dafür sämtliche Komponenten eines vollständigen Grids und kann daher unabhängig von anderen Sites auch für Lehr- und Forschungszwecke betrieben werden.

In Abbildung 1 sind die Komponenten des gLite Testbed mit den Kommunikationsbeziehungen dargestellt, die u. a. bei der Ausführung eines Jobs innerhalb dieser Umgebung auftreten.

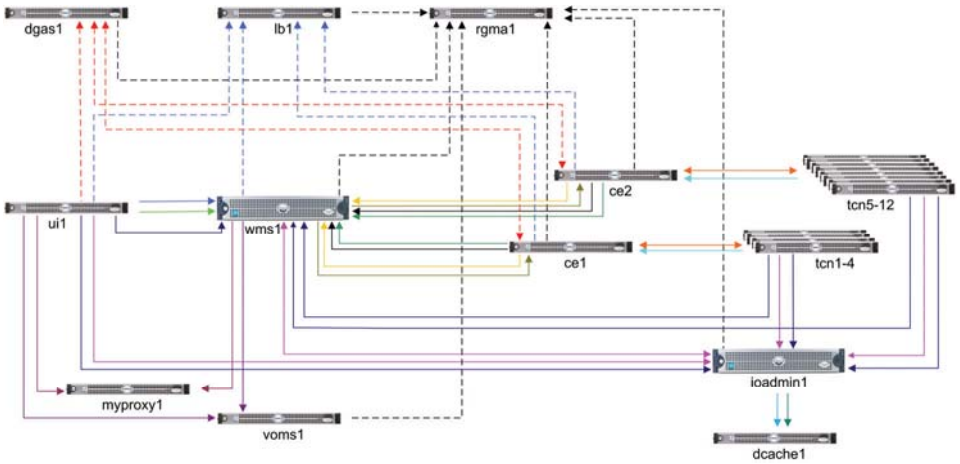

Abbildung 1: gLite Testbed am RRZN

In der über die Partner verteilten Grid-Umgebung treten weitere Kommunikationsflüsse zu Komponenten außerhalb des RRZN auf. Durch Kopplung mit Umgebungen, die auf anderer Grid Middleware wie z. B. LCG2 oder Globus Toolkit 4 basieren, können weitere Komponenten hinzugefügt werden oder veränderte Kommunikationsbeziehungen auftreten. Ausgehend von der dargestellten Umgebung lassen sich verschiedene Angriffsszenarien evaluieren und Ansätze zu deren Behebung erproben.

3 Authentifizierung

Allgemeines Ziel der Authentifizierung in Grid-Umgebungen ist der gegenseitige vertrauenswürdige, d. h. der sichere und zuverlässige Nachweis der Identität von Nutzern, Hosts oder Diensten. Hierfür werden X.509 End-Entity Zertifikate verwendet. Die Zertifikate enthalten unter anderem im Subject den *Distinguished Name* (DN) des Inhabers (Beispiel: „/O=GermanGrid/OU=UniHannover/CN=Stefan Piger“), den DN der ausstellenden *Certification Authority* (CA), den Public Key des Inhabers bzw. des Subject, eine eindeutige Seriennummer sowie die Gültigkeitsdauer des Zertifikats. Die CA tritt als so genannte Third-Party auf, d. h. dieser Instanz müssen Nutzer und Dienste gleichermaßen vertrauen. Die für Grid-Umgebungen erforderlichen internationalen Vertrauensbeziehungen sind über den CA-Verbund der GridPMA (Policy Management Authority) organisiert.

Der dem Zertifikat zugehörige Private Key des Inhabers wird in der Regel mit einem Password verschlüsselt und ist somit vor dem unbefugten Zugriff von Dritten geschützt. Gemeinsam bilden Zertifikat und Private Key die so genannten Credentials.

Zertifikate, die während ihrer regulären Gültigkeitsdauer für ungültig erklärt werden, können über *Certificate Revocation Lists* (CRL) zurückgerufen werden. Diese Listen werden täglich aktualisiert.

3.1 Single Sign-On und Proxy-Zertifikate

End-Entity Zertifikate können aufgrund des geschützten Private Key nicht unmittelbar für das in Grid-Umgebungen unumgängliche Single Sign-On eingesetzt werden. Deshalb verwendet man Proxy-Zertifikate, deren Private Key unverschlüsselt bleibt. Proxy-Zertifikate werden von den eigentlichen End-Entity Zertifikaten abgeleitet. Zu beachten ist, dass zwei Varianten für Proxy-Zertifikate existieren. Zuerst hat sich die als Pre-Standard bezeichnete Erweiterung des Subject DN mit CN=proxy etabliert (Beispiel: „/O=GermanGrid/OU=UniHannover/CN=Stefan Piger/CN=proxy“). Mit dem RFC 3820 [TWE+04] ist inzwischen auch eine standardisierte Erweiterung des ursprünglichen RFC 3280 verfügbar.

Ein Proxy-Credential stellt ein eigenständiges Paar aus abgeleitetem Zertifikat mit Public Key sowie unverschlüsseltem Private Key dar. Die Signierung eines Proxy-Zertifikats erfolgt durch den Private Key des „übergeordneten" End-Entity Zertifikates. Hierdurch ist die vollständige Zertifikatskette bis zur Root-CA jederzeit überprüfbar. Ein Proxy-Zertifikat wird mit einer deutlich eingeschränkten Gültigkeitsdauer versehen, typisch sind je nach Art der Grid-Jobs und der zugrunde liegenden Policies wenige Stunden. Ein so genanntes Proxy-Renewal für langlaufende Grid-Jobs ist möglich (s. Kap. 3.3). Dagegen scheidet der oben dargestellte CRL-Mechanismus für den Widerruf von Zertifikaten aus, da Proxy-Zertifikate nicht bei einer CA registriert sind.

3.2 Delegation

Neben dem Single Sign-On dienen Proxy-Zertifikate auch der Delegation von Rechten [WFK+04]. Die Weitergabe der vollständigen Proxy-Credentials aus Proxy-Zertifikat und zugehörigem unverschlüsseltem Private Key ermöglichen es beliebigen Grid-Diensten, im Namen des Nutzers, d. h. des ursprünglichen Inhabers, zu agieren. Eine Delegation beschränkter Nutzer-Rechte ist über Zertifikats-Erweiterungen möglich. Die Pre-Standard Proxy-Zertifikate verwenden dazu eine Erweiterung des DN (Beispiel: „/O=GermanGrid/OU=UniHannover/CN=Stefan Piger/CN=proxy/CN=limited proxy"). Proxy-Zertifikate nach RFC 3820 begrenzen die Ableitung weiterer Proxy-Zertifikate über die nicht-kritische Erweitung *ProxyCertInfo* und limitieren die delegierten Rechte über das Feld *ProxyPolicy*.

3.3 MyProxy

Der MyProxy Credential Management Service [Bas05] wurde von NCSA und der University of Illinois entwickelt und ist mittlerweile eine eigenständige Komponent der Grid-Middlewares Globus Toolkit 4 und gLite. MyProxy zeichnet sich durch drei disjunkte Funktionalitäten auf:

1. Online Credential Repository (auch Credential Wallet): dient der sicheren Verwahrung von End-Entity Zertifikaten der Nutzer einschließlich der zugehörigen Private Keys. Durch die Speicherung der vollständigen Credentials auf einem gesondert gesicherten zentralen System sollen die durch unsichere Aufbewahrung bei den Nutzern entstehenden Gefahrenpotentiale gemindert werden [NTW01].

2. Online CA: dient der alternativen Generierung von Proxy-Zertifikaten für Nutzer ohne X.509 End-Entity Zertifikat. Hierfür meldet sich der Nutzer lediglich z. B. über Username und Password an dem MyProxy-Server an und erhält ein reguläres Proxy-Zertifikat.

3. Proxy-Renewal: dient der Erneuerung ablaufender Proxy-Zertifikate zur Vermeidung von Job-Abbrüchen. Der Nutzer platziert hierfür zunächst ein länger gültiges Proxy-Zertifikat (z. B. mit einer Gültigkeitsdauer von mehreren Tagen) auf dem MyProxy-Server. Von diesem Proxy-Zertifikat werden sämtliche zur Bearbeitung des Grid-Jobs erforderlichen Proxy-Zertifikate (z. B. mit einer Gültigkeitsdauer von mehreren Stunden) abgeleitet. Die an der Bearbeitung des jeweiligen Grid-Jobs beteiligten Systeme rufen rechtzeitig vor Ablauf eines Proxy-Zertifikates ein neues von dem MyProxy-Server ab. Zu beachten ist, dass dadurch nicht die Gültigkeit eines bestehenden Proxy-Zertifikates verlängert, sondern ein neues Proxy-Zertifikat erstellt wird.

3.4 Bewertung

Die starke Konzentration auf X.509 Zertifikate in Grid-Umgebungen ist fraglos gut begründet. Die zugrunde liegenden Verfahren sind allgemein etabliert, anerkannt vertrauenswürdig und zudem mit vertretbarem Aufwand zu verwalten, wobei eine PKI generell vorausgesetzt werden muss. Nicht zu vernachlässigen ist jedoch der erforderliche Aufwand für die Nutzer zur sicheren Speicherung und zur regelmäßigen Erneuerung ihrer Zertifikate. Massen-Rollouts von Zertifikaten für neue Nutzergruppen gestalten sich wegen des erheblichen administrativen Aufwands derzeit noch schwierig.

Ergänzend ist eine zunehmende Verbreitung alternativer Verfahren zur Nutzer-Authentifizierung in Grid-Umgebungen zu erkennen. Mit der OnlineCA in MyProxy und durch den Einsatz von Shibboleth [ScCa05] werden derzeit zwei Alternativen entwickelt. Hierbei ist zu bemerken, dass lediglich die initiale Authentifizierung der Nutzer ersetzt wird. Zur Umsetzung von Single Sign-On und Delegation innerhalb der Grid-Umgebungen werden weiterhin ausschließlich Proxy-Zertifikate verwendet.

Bei der Verwendung von Proxy-Zertifikaten für Single Sign-On und Delegation ist zu bedenken, dass der Diebstahl eines Proxy-Zertifikats im Grid prinzipiell möglich ist (s. Kap. 5) und ein erfolgreicher Angreifer unmittelbar die Identität Dritter mit deren vollständigen Rechten übernimmt. Der insbesondere nach erkannter Kompromittierung erforderliche unmittelbare Rückruf von Proxy-Zertifikaten wie etwa durch CRLs ist nicht möglich. Eine Verbesserung dieser Situation, etwa durch den Einsatz von Verfahren ähnlich dem *Online Certificate Status Protocol* (OCSP) [MAM+99], ist bisher nicht abzusehen. Alternativ wird eine Einschränkung der Gültigkeit von Proxy-Zertifikaten z. B. durch explizite Bindung an die Job-ID eines Grid-Job diskutiert [PGW06][2].

[2] http://www.rrzn.uni-hannover.de/ubp.html

4 Autorisierung

Übergreifendes Ziel der Autorisierung ist die Entscheidung, welche(r) Nutzer, Gruppe oder *Virtuelle Organisation* (VO) welche Ressourcen nutzen darf. Unmittelbare Herausforderungen bei der Umsetzung einer übergreifenden Autorisierung in Grid-Umgebungen sind in der Verhinderung des Missbrauchs von Grid-Ressourcen, der Granularität bei der Definition und Vergabe von Rechten sowie bei der Delegation von Nutzer-Rechten an Grid-Dienste zu sehen.

4.1 Globale und lokale Autorisierung

Die globale Autorisierung in Grid-Umgebungen ist Ressourcen-unabhängig und orientiert sich an der VO, indem die Zugehörigkeit eines Nutzers zur VO sowie dessen Rolle und Attribute innerhalb der VO festgelegt werden. Demgegenüber werden mit der lokalen Autorisierung die Richtlinien für die Zugriffsrechte der Nutzer (oder Dienste) auf den Ressourcen definiert. Anhand dieser Richtlinien erfolgt die Entscheidung zur Freigabe der Ressourcen sowie die Umsetzung zu deren eigentlicher Nutzung. Dies bedeutet schließlich, dass die lokale Ressource die globalen Informationen und die lokalen Richtlinien zur Autorisierung in Einklang bringen muss.

4.2 Identitäts- und rollenbasierte Autorisierung

Die in Grid-Umgebungen verwendeten Modelle zur Autorisierung lassen sich zunächst in identitäts- und rollenbasierte Verfahren unterscheiden. Der identitätsbasierte Ansatz wurde mit dem Globus Toolkit 2 eingeführt und stellt lediglich eine einfache Form der Autorisierung dar. Hierbei wird auf jeder Ressource die Datei *grip-mapfile* gepflegt, welche eine Abbildung der DN der Nutzer auf lokale UNIX-Accounts enthält. Eine Weiterentwicklung in aktuellen Grid-Middlewares stellt die Abbildung des DN auf einen Poolaccount, d. h. auf einen beliebigen Account aus einer Menge von Accounts mit gleichen Rechten, dar. Die Steuerung der Nutzerrechte erfolgt über die entsprechenden UNIX-Berechtigungen des lokalen Accounts mit dem einhergehenden Setzen der effektiven User-ID (UID) und Group-ID (GID) von Prozessen (POSIX in-process enforcement).

Die Nachteile dieses dezentralen Verfahrens sind offenbar, da die Pflege einer Datei, in der sämtliche DN der Nutzer eingetragen werden müssen, nicht skaliert. Eine Synchronisation auf allen Ressourcen im Grid ist zudem aufwändig und fehleranfällig. Darüber hinaus bietet dieser Ansatz keine Differenzierung nach Rollen oder Attributen innerhalb einer VO.

Eine wesentliche Verbesserung wird mit dem zentralen rollenbasierten Ansatz des *Virtual Organisation Membership Service* (VOMS) verfolgt, der im Rahmen verschiedener EU-Projekte (EDG, EGEE und EGEE2) entwickelt wird [FrCi04]. VOMS dient der zentralen Verwaltung von Nutzern und deren Rollen bzw. Attributen (Capabilities) innerhalb einer VO. Da in der Praxis bisher den Nutzern lediglich Rollen zugewiesen und die Attribute nicht genutzt werden, wird mit VOMS de-facto eine so genannte *Role Based Access Control* (RBAC) durchgeführt.

In jeder VO existiert genau ein zentraler VOMS-Service, der somit die eindeutige Attribute Authority darstellt. In einer typischen Abfrage des VOMS-Servers erhält der Nutzer seine ausgewählten Attribut-Zertifikate, die er als nicht-kritische Erweiterungen in ein neues Proxy-Zertifikat übernehmen und dadurch den Grid-Ressourcen vorlegen kann (Push-Modell).

Die lokale Entscheidung zur rollenbasierten Autorisierung auf den Ressourcen erfolgt durch ein zweistufiges Verfahren. Zunächst entscheidet der *Local Centre Authorization Service* (LCAS) anhand der Identität des Anfragenden sowie den vorliegenden VOMS-Attributen (VO, Gruppe und Rolle), ob ein Zugriff gewährt oder verwehrt wird. Nach positiver Entscheidung erfolgt die lokale Umsetzung der Autorisierung auf den Ressourcen durch den *Local Credential Mapping Service* (LCMAPS). Das Vorgehen ist hierbei ähnlich zu dem identitätsbasierten Ansatz, indem den Nutzern lokale Accounts zugewiesen werden uns somit die herkömmlichen UNIX-Berechtigungen greifen. Hierbei werden jedoch sämtliche Attribute der Nutzer berücksichtigt.

4.3 Bewertung

Im Gegensatz zu den weitgehend homogenen und allgemein etablierten Verfahren zur Authentifizierung stellt sich die Autorisierung in Grid-Umgebungen als heterogenes und bisher nicht zufriedenstellend gelöstes Problem dar. Die verschiedenen Ansätze lassen bisher keine einheitliche Infrastruktur erkennen.

Sogar innerhalb einer Grid Middleware werden verschiedene Ansätze verfolgt, so dass derzeit keine Ressourcen-übergreifende Form der Autorisierung möglich ist. Das Globus Toolkit 4 verwendet mit dem oben nicht näher dargestellten und ausschließlich für Storage-Dienste verfügbaren *Community Authorization Service* (CAS) eine weitgehend unterschiedliche Lösung gegenüber dem – lediglich in Ansätzen implementierten – VOMS/LCAS/LCMAPS für die Compute-Dienste. In gLite werden sogar innerhalb der Compute-Dienste verschiedene Verfahren zur Autorisierung verwendet (vgl. Abbildung 1). Die *Compute Elements* (CE) nutzen zwar VOMS/LCAS/LCMAPS, das vorgeschaltete *Workload Management System* (WMS) setzt jedoch noch auf einen identitätsbasierten Ansatz.

Weiterhin ist bisher keine umfassende Verwaltung der Informationen zur Autorisierung verfügbar. Während für zentrale Entscheidungen eine einheitliche Administration der Nutzer und deren Rechte innerhalb der VO erforderlich ist, benötigen dezentrale Entscheidungen eine einheitliche Administration der Zugriffsrechte auf den Ressourcen. Ein Ressourcen-, Anbieter- oder sogar VO-übergreifendes Management zur Autorisierung muss beide Sichten in Einklang bringen, Ansätze hierfür sind derzeit lediglich in einem frühen Entwicklungsstadium.

5 Missbrauch von Proxy-Credentials

Die Übertragung von Proxy-Credentials in Grid-Umgebungen erfolgt generell über *Transport Layer Security* (TLS). Somit ist eine gegenseitige Authentifizierung der Kommunikationspartner sowie eine Verschlüsselung der übertragenen Daten gewährleistet. Dem gegenüber ist die Handhabung von Proxy-Credentials auf den Grid-Ressourcen bisher nicht ausreichend gesichert. Die zur Verarbeitung erforderliche lokale Speicherung erfolgt im UNIX-Dateisystem unter Verwendung der regulären Dateirechte. Die User-ID dieser Dateien ist somit die des zugehörigen Poolaccounts. Da die gleichzeitige Zuweisung mehrere Nutzer auf denselben Poolaccount vermieden wird, ist ein unmittelbarer Zugriff auf die Proxy-Credentials fremder Nutzer durch die UNIX eigenen Sicherheitsmechanismen unterbunden.

Jedoch erfolgt keine zuverlässige Absicherung der Sandbox bzw. des Job-Kontext auf UNIX-Systemebene. Bisher arbeiten Grid-Jobs in einer generischen UNIX-Umgebung mit den typischen UNIX-Rechten. Dadurch wird der Aufruf regulärer UNIX-Kommandos und Applikationen ohne Beschränkung der Laufzeit möglich.

Ausgangspunkt der im Folgenden beispielhaft dargestellten Angriffe ist der Missbrauch von Poolaccounts. Auf diese Accounts werden die Nutzer-Accounts mit einer durch die Laufzeit der Proxy-Zertifikate eingeschränkten Gültigkeitsdauer abgebildet. Gelingt es einem legitimierten, d. h. authentifizierten und autorisierten Nutzer aus diesem Kontext auszubrechen, kann er seine Befugnisse erweitern. Durch die Installation z. B. eines Cronjobs ist es ihm möglich, Prozesse außerhalb seiner Sandbox-Umgebung bzw. außerhalb des Job-Kontext zu starten. So wird dieser Cronjob unter der User-ID des Poolaccounts ausgeführt, auch nachdem die Laufzeit des ursprünglichen Proxy-Zertifikates beendet ist.

Auf Basis dieser dauerhaft verfügbaren Prozesse ergeben sich unmittelbar verschiedene Angriffsmöglichkeiten:

1. Der Angreifer agiert mit den Rechten des Poolaccounts, die er für lokale Angriffe nutzen kann. So kann er z. B. diese Rechte erweitern, indem er bekannte Schwächen des Betriebssystems oder von installierter Software nutzt. Darüber hinaus kann er von dem kompromittierten Rechner Angriffe in das lokale Netz und weitere Netze, die der Grid-Umgebung unmittelbar angehören, durchführen.

2. Werden neue Nutzer-Accounts auf den ehemaligen Poolaccount des Angreifers abgebildet, können deren Proxy-Zertifikate unmittelbar durch den Cronjob gelesen und somit missbraucht werden. Damit kann der Angreifer neue Jobs unter der Identität eines anderen Nutzers starten. Gleichzeitig erhält er direkten Zugriff auf die Daten des neuen Nutzers.

3. Durch den Cronjob kann der Angreifer auch Netzdienste bzw. Server-Prozesse auf dem kompromittierten Knoten dauerhaft starten. Die Hinweise zur geeigneten Konfiguration dieser Dienste erhält er sogar aus seinen Umgebungsvariablen, in denen unter anderem die Port-Bereiche von GridFTP eingetragen sind. Der Zugriff auf die hier aufgeführten Ports wird explizit von Firewalls gestattet, um die Nutzung von GridFTP zu ermöglichen (s. Kap. 6).

5.1 Lösungen

Wegen der Komplexität von Grid-Umgebungen und der derzeit noch existierenden Vielfalt möglicher Schwachstellen existiert nicht eine alleinige Lösung, mit der die oben genannten Angriffsszenarien verhindert werden können. Abhilfe könnte die bisher nicht vorgesehene zusätzliche Beschränkung der Rechte von Proxy-Zertifikaten z. B. auf eine Job-ID schaffen [PGWG06]. Daneben stellt die Abbildung von Nutzer-Accounts auf Poolaccounts eine offenkundige Schwachstelle dar, die durch die Verwendung temporärer Accounts gemindert werden könnte. Auch in der restriktiveren Handhabung der Sandbox-Umgebung ist eine weitere notwendige Verbesserung zu sehen. So wird derzeit eine wichtige Alternative in der Isolierung der Nutzer durch Virtualisierung diskutiert. Aktuelle verfügbare Ansätze wir der *Workspace Service* (WSS) in gLite sind jedoch bisher nur bedingt für den produktiven Einsatz geeignet.

6 Firewalls in Grid-Umgebungen

Die typischen Kommunikationsbeziehungen in Grid-Umgebungen sind durch zahlreiche beteiligte Hosts sowie heterogene Dienste und Anwendungsprotokolle gekennzeichnet. Aus Sicht eines Ressourcen-Anbieters werden Verbindungsanforderungen von vielen, a priori unbekannten Host aus dem Internet an die Systeme im eigenen Netz gerichtet. Zur Verbesserung der Übertragungsraten werden häufig sogar mehrere parallele Datenströme initiiert, so dass neben der Komplexität der Kommunikationsbeziehungen auch erhebliche Anforderungen an die Performance der Übertragungssysteme gestellt werden.

6.1 Aufhebung des Zonenkonzepts

Der geeignete Schutz von Grid-Umgebungen durch Firewalls wird neben den vielfältigen Kommunikationsbeziehungen dadurch erschwert, dass die Compute- und Storage-Ressourcen häufig nicht in einer ausgewiesenen *Demilitarisierten Zone* (DMZ) für den Zugriff von äußerem und innerem Netz betrieben werden, sondern im inneren Netz angeordnet sind. Das in Abbildung 2 dargestellte klassische Zonenkonzept für Firewalls mit innerem und äußerem Netz sowie DMZ ist in diesen Fällen nicht geeignet umzusetzen.

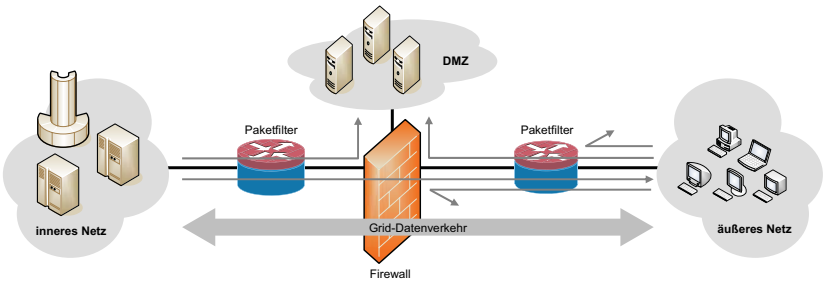

Abbildung 2: Zonenkonzept von Firewalls und Grid-Datenverkehr

6.2 GridFTP

Ein zusätzliches Problem für den Einsatz von Firewalls stellt die Applikation GridFTP dar, die im Globus Toolkit und in gLite für die Übertragung von Dateien verwendet wird. GridFTP initiiert für einen effizienten Datentransfer mehrere parallele TCP-Verbindungen, um den gesamten Durchsatz zu steigern. In der Regel belegt GridFTP für jeden Dateitransfer ca. 20 TCP-Verbindungen. Allgemein anerkannte Abschätzungen fordern die Berücksichtigung von bis zu 250 gleichzeitigen Nutzern in einer Grid-Umgebung, so dass auf den Firewalls die hierfür notwendige dauerhafte Freischaltung von 5.000 Ports empfohlen wird. Die Möglichkeit zur gleichzeitigen Beschränkung der offenen Ports auf die IP-Adressen oder zumindest die IP-Subnetze der beteiligten Quell- und Zielsysteme ist in Grid-Umgebungen häufig nicht gegeben, da selten sämtliche Adressen der Kommunikationspartner bekannt sind. Darüber hinaus skaliert dieser Ansatz aufgrund der hohen Anzahl und Verteiltheit von Hosts in größeren Grid-Umgebungen nicht.

Weiterhin verwendet GridFTP einen verschlüsselten Kontrollkanal, über den die Dateitransfers lediglich initiiert werden. Eine aktive Firewall für GridFTP müsste den Kontrollkanal überwachen und die übertragenen Informationen interpretieren, um die belegten Datenkanäle erkennen und die benötigten Ports dynamisch freischalten zu können. Dieser Ansatz ist durch die Verschlüsselung nicht mehr in derselben Form möglich wie bei herkömmlichem FTP.

Eine Erweiterung der Firewall zur gezielten Entschlüsselung des Kontrollkanals ist nicht praktikabel. Sicherheitsprobleme bei der Verwaltung der Schlüssel zur Entschlüsselung sowie ein hoher Verwaltungsaufwand mit einhergehenden Performanceeinbußen stellen einen derartigen Ansatz grundsätzlich in Frage.

Der in Abbildung 3 dargestellte Third-Party Transfer stellten eine weitere Hürde für eine umfassende Absicherung von Grid-Infrastrukturen durch Firewalls dar. Hierbei baut der GridFTP-Client je einen verschlüsselten Kontrollkanal zu zwei GridFTP-Servern auf und initiiert einen Datentransfer zwischen diesen Server. Die Server tauschen die Datei über einen Datenkanal aus, zwischen den Servern wird kein Kontrollkanal benötigt. Firewalls zwischen den Server erhalten somit unter Umständen keine Kontrollinformationen über den durchzuführenden Dateitransfer, so dass sich hier grundsätzlich keine Möglichkeit zur dynamischen Öffnung von Ports ergibt.

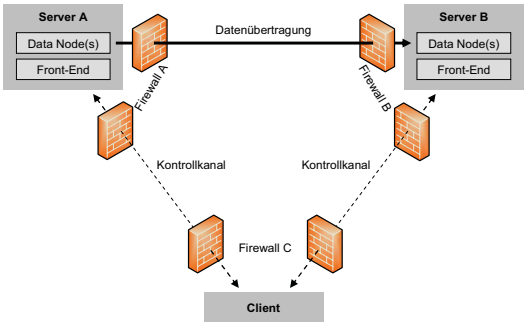

Abbildung 3: Third-Party Transfer in GridFTP

6.3 Bewertung

Dynamische Ansätze von Firewalls, wie sie z. B. für FTP seit langer Zeit etabliert sind, sind für Grid-Umgebungen bisher nicht verfügbar [VoGr06]. Die komplexen Kommunikationsbeziehungen sowie die weitgehend verschlüsselte Übertragung von Kontrollinformationen lassen bisher keine umfassenden Ansätze zu. Da aus Sicht der Firewall-Anbieter Grid-Protokolle bisher als nicht marktrelevant beurteilt werden, erschwert sich die Implementierung und Verbreitung möglicher Ansätze zusätzlich [NAG+06]. Darüber hinaus stellt sich für Third-Party Transfers in GridFTP grundsätzlich keine praktikable Lösung dar.

Die sich daraus ergebende aufwändige Firewall-Administration für Grid-Umgebungen verführt unmittelbar zu kritischen Vereinfachungen der Konfiguration, so dass das allgemeine Sicherheitsniveau der gesamten Grid-Umgebung sinkt.

Zusätzliche Einschränkung ergeben aktuell durch die mangelnde Performance von Firewalls. Die z. T. notwendige Performance von Datentransfers wird von Firewalls gemindert, die aktuelle Grenze ist derzeit bei wenige GBit/Sekunde. Diese Beschränkung führt aktuell sogar zur Umgehung bzw. Vermeidung von Firewalls in großen Grid-Umgebungen.

7 Zusammenfassung und Ausblick

Der hier dargestellten Angriffspunkte und konzeptionellen Schwächen sowie mögliche Ansätze zu deren Ausnutzung zeigen exemplarisch derzeitige sicherheitsrelevante Mängel in Grid-Umgebungen auf. Die skizzierten Ansätze zur Verbesserung dieser Situation erfordern bei der Umsetzung zum Teil erhebliche Änderungen der Grid Middleware, so dass kurzfristig keine wesentliche Verbesserung dieser Situation zu erwarten ist.

Weiterhin wurde eine grundlegende Abschätzung und Bewertung der vorhandenen Sicherheitsmechanismen in Grid-Umgebungen vorgelegt. Diese Betrachtung ist besonders aus Sicht von Rechenzentren wünschenswert, um ihre vorhandenen Ressourcen zumindest mittelfristig angemessen gesichert in Grid-Infrastrukturen einbringen zu können.

Ausgehend von der derzeitigen Situation können Grid Middlewares noch nicht für den Einsatz in sicherheitskritischen Umgebungen empfohlen werden, sofern intensive Kommunikationsbeziehungen mit externen Systemen auftreten und eine hohe Anzahl von Nutzern auf diese Infrastrukturen zugreift. Es ist jedoch zu erkennen, dass in zahlreichen internationalen Projekten insbesondere aus der Medizin und der Bioinformatik Verbesserungen konzipiert und implementiert werden.

Literaturverzeichnis

[ABM04] Ahsant, M., Basney, J., Mulmo, O., Grid Delegation Protocol. Proc. Workshop on Grid Security Experiences, Oxford, 2004

[Bas05] Basney, J., GFD-E.054 – MyProxy Protocol, Global Grid Forum, 2005

[FrCi04] Frohner, Á., Ciaschini, V., VOMS Credential Format, 2004 http://edg-wp2.web.cern.ch/edg-wp2/security/voms/edg-voms-credential.pdf

[MAM+99] Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C., X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, IETF RFC 2560, 1999

[NAG+06] Niederberger, R., Allcock, W., Gommans, L., Grünter, E., Metsch, T., Monga, I., Volpato, G. L., Grimm, C., Firewall Issues overview, Global Grid Forum, 2006

[NTW01] Novotny, J., Tuecke, S., Welch, V., An Online Credential Repository for the Grid: MyProxy. Proc. Tenth International Symposium on High Performance Distributed Computing, San Francisco, 2001

[PGWG06] Piger, S., Grimm, C., Wiebelitz, J., Gröper, R., An Approach to Restricted Delegation of User Rights in Proxy Certificates based on the gLite Middleware. Proc. Cracow Grid Workshop '06, Kraków, 2006 (to appear)

[ScCa05] Scavo, T., Cantor, S., Shibboleth Architecture – Technical Overview. Working Draft Version 2, 8 Jun. 2005. http://shibboleth.internet2.edu/

[TWE+04] Tuecke, S., Welch, V., Engert, D., Pearlman, L., Thompson, M., Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile, IETF RFC 3820, 2004

[VoGr06] Volpato, G. L., Grimm, C., Dynamic Firewalls and Service Deployment Models for Grid Environments. Proc. Cracow Grid Workshop '06, Kraków, 2006 (to appear)

[WFK+04] Welch, V., Foster, I., Kesselmann, C., Mulmo, O., Pearlman, L., Tuecke, S., Gawor, J., Meder, S., Siebenlist, F., X.509 Proxy Certificates for Dynamic Delegation. In: Pro-ceedings of the 3rd Annual PKI R&D Workshop, 2004