Chr. Grimm, M. Pattloch und H. Reiser

Sicherheit in Grids

Dr. *Christian Grimm* ist Juniorprofessor für Rechnernetze an der Universität Hannover und leitet am RRZN den Bereich FuE Rechnernetze und Neue Dienste. Im D-Grid koordiniert er z.T. gemeinsam mit dem DFN-Verein Fachgebiete zu sicherheitsrelevanten Themen (AA-Infrastruktur und Firewalls) sowie zu alternativen Transportprotokollen. Vor seiner Promotion zum Dr.-Ing. im Jahr 2002 war er Oberingenieur am LG RVS der Universität Hannover und technischer Leiter der Internet SkyWay GmbH, Teltow. Forschungsgebiete: Grid-Computing, Sicherheit in Verteilten Systemen, Hochgeschwindigkeits-Datenkommunikation, Verkehrstheorie in IP-Netzen. Mitglied in ACM, GI und IEEE.

Dr. *Marcus Pattloch* betreut den Bereich Sicherheit im Deutschen Forschungsnetz. Als Mitarbeiter der DFN-Geschäftsstelle in Berlin koordiniert er dabei insbesondere die Arbeiten des Computer-Notfallteams im DFN (DFN-CERT) sowie die Erweiterung und den Betrieb der DFN-weiten Public Key Infrastruktur (DFN-PKI). Studium der Informatik an der TU Berlin, Promotion zum Dr. rer. oec. an der Universität des Saarlandes.

Dr. *Helmut Reiser* ist Leiter der Gruppe Netzplanung am Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften; dort u.a. für D-Grid Projekte (VO-Management, Monitoring, Accounting, Aufbau des Kern D-Grid und Globus-Integration) verantwortlich. Studium der Informatik an der Technischen Universität München (Diplom 1997); Promotion über Sicherheit in Managementsystemen auf der Basis Mobiler Agenten an der Ludwig-Maximilians Universität (LMU) 2001. Von 1997 bis 2005 am Lehrstuhl Kommunikationssystem und Systemprogrammierung der LMU beschäftigt. Forschungsinteressen: Sicherheit in föderierten Umgebungen, Grid Technologien und integriertes IT-Management. Mitglied bei GI, IEEE und ACM.

ZUSAMMENFASSUNG

In Deutschland wird durch die vom BMBF geförderte D-Grid Initiative eine Grid-Infrastruktur aufgebaut, in der zur Zeit sechs Community Projekte die verschiedensten Anwenderdisziplinen vertreten. Um die Nachhaltigkeit und Nutzbarkeit von Grids zu gewährleisten, muss ein hohes Sicherheitsniveau erreichbar sein.

In diesem Beitrag werden grundlegende Sicherheitsfragestellungen wie Authentifizierung, Autorisierung, Zugriffskontrolle, Vertraulichkeit und Datenschutz vorgestellt. Außerdem werden der Einsatz von Firewalls und die für Grids gängigen und heute verfügbaren Sicherheitsmechanismen betrachtet. Es werden aber auch offene Fragen und ungelöste Problemstellungen thematisiert, die für einzelne Communities von so grundlegender Bedeutung sind, dass fehlende Lösungen die praktische Einsetzbarkeit von Grid-Technologien in der entsprechenden Anwenderdisziplin gefährden.

1 EINLEITUNG

Das Global Grid Forum (GGF), dessen Ziel eine weltweite Standardisierung für Grid Computing ist, setzt sich aus Nutzern, Entwicklern und Herstellern zusammen. Das grundlegende Dokument für service-orientierte Grids ist die Open Grid Service Architecture (OGSA) [1]. OGSA ist ein allgemeiner architektureller Rahmen zur Beschreibung und Organisation von Grid-Infrastrukturen. Er stellt ein Modell dar, wie Grids entwickelt werden sollen, gibt aber keinerlei Hinweise, die eine konkrete Umsetzung oder Implementierung betreffen.

Im Rahmen der Standardisierungsbemühungen von OGSA wurden innerhalb der OGSA Security Working Group (OGSA-SEC-WG) eine Sicherheitsarchitektur für OGSA [2] sowie die OGSA Security Roadmap [3] entwickelt. Die Sicherheitsarchitektur wurde größtenteils in den OGSA-Standard [1] übernommen, ist aber an manchen Stellen ausführlicher als der Standard selbst. Diese Dokumente können als Grundlage für eine Sicherheitsbetrachtung in Grids dienen, da sie eine sehr umfassende Anforderungsanalyse enthalten.

Nach [2] lassen sich alle Überlegungen zum Thema Grid-Sicherheit im Spannungsfeld zwischen drei Herausforderungen („Security Challenges") einordnen:

1. Integration Challenge: Im Grid ist es nicht möglich, allen beteiligten Organisationen eine einheitliche Sicherheitstechnologie „vorzuschreiben". Damit muss eine Sicherheitsarchitektur unabhängig von konkreten Implementierungen einsetzbar und bestehende Sicherheitsmechanismen müssen

1 Teile dieses Beitrages entstanden im Rahmen des vom Bundesministerium für Bildung und Forschung (BMBF) unter dem Förderkennzeichen 01AK800B geförderten D-Grid Projektes.

einfach integrierbar sein. Wegen der hohen Dynamik in der Infrastruktur und u.U. auch bei den beteiligten Partnern sollte die Sicherheitsarchitektur einfach erweiterbar sein.
2. Interoperability Challenge: Die verschiedenen Sicherheitsmechanismen in den einzelnen Domänen müssen zusammenarbeiten, ohne dabei das globale Sicherheitsniveau zu verringern. Kommen unterschiedliche Protokolle zum Einsatz, muss es Abbildungsmechanismen bzw. Gateways zur Übersetzung geben.
3. Trust Relation Challenge: Die Sicherheit basiert an vielen Stellen auf Vertrauensbeziehungen zwischen den beteiligten Domänen. Es sind Mechanismen erforderlich, die diese durch formale Beschreibungsverfahren für Vertrauensbeziehungen und Vertrauensstufen explizit machen. Dazu bedarf es Verfahren, um solche Vertrauensbeziehungen zu etablieren und den Partnern diskrete Vertrauensstufen zuzuweisen.

Die Dokumente beschreiben die für ein Grid notwendigen Sicherheitsanforderungen und Sicherheitsdienste sehr umfassend, ohne sich aber mit deren technischer Umsetzung zu beschäftigen. In diesem Artikel wird die Liste der Anforderungen als Leitfaden verwendet, um den aktuellen Stand der Sicherheit in Grids darzustellen. Im Folgenden wird untersucht, ob und wie sich Anforderungen mittels geeigneter Sicherheitsmechanismen umsetzen lassen und welche speziellen Probleme sich in bestimmten Anwendungsgebieten ergeben können.

Das folgende Kapitel beschäftigt sich mit der Authentifizierung der Nutzer im Grid. Kapitel 3 stellt die Mechanismen zur Delegation von Rechten und den Möglichkeiten des Single Sign-On vor. Daran anschließend wird die Vergabe von Rechten und deren Durchsetzung untersucht. Kapitel 5 befasst sich mit heterogenen (Sicherheits-) Policies und der Lösung möglicher Policy-Konflikte. Die Mechanismen für Vertraulichkeit, Datenschutz, Auditierbarkeit und Nachvollziehbarkeit sind Fokus des Abschnittes 6. Kapitel 7 stellt den aktuellen Stand bei den Firewalls für Grids dar. Im Anschluss daran werden die Notwendigkeit und die Dienste eines Computer Notfallteams (Grid-CERT) motiviert. Die Arbeit schließt mit einer Zusammenfassung und einem Ausblick.

2 AUTHENTIFIZIERUNG

Die Grid Security Infrastructure (GSI) wurde als gemeinsame Sicherheitsschicht aller Komponenten des Globus Toolkit entwickelt [5] und bietet grundlegende Sicherheitsmechanismen auch in den aktuellen Grid Middlewares Globus Toolkit 4 und gLite 3.0. Übergeordnete Ziele der GSI sind

1. vertrauliche Kommunikation zwischen den verteilten Grid-Komponenten,
2. Unterstützung eines einfachen und benutzerfreundlichen Single Sign-On (SSO) für die Nutzer sowie
3. Delegation von persönlichen Credentials an Dienste, die im Namen des Nutzers im Grid agieren.

Grundlage der Authentifizierung von Nutzern und Diensten in der GSI ist die Verwendung von Zertifikaten nach X.509 Version 3 und daraus resultierend die Verwendung einer Public Key Infrastructure mit mehreren unabhängigen Zertifizierungsstellen (Certification Authorities, CAs). Um die internationale Einbindung dieser Zertifikate zu gewährleisten, müssen die CAs von der European Grid Policy Management Authority (EUGridPMA) akzeptiert werden. Bei der EUGridPMA handelt es sich um eine im Jahre 2004 gegründete Organisation, die grundlegende Bedingungen für den Betrieb von Zertifizierungsstellen festlegt und durch ein einheitliches Verfahren Vertrauensbeziehungen zwischen wissenschaftlichen Einrichtungen in europäischen Ländern herstellt. 2005 erfolgte der Zusammenschluss mit The Americas Grid Policy Management Authority (TAGPMA) und der Asia Pacific Grid Policy Management Authority (APGridPMA) zur International Grid Trust Federation (IGTF) wodurch eine weltweite Anerkennung von Grid-Zertifikaten erfolgen kann. Die beiden deutschen EUGridPMA-konformen Zertifizierungsstellen werden vom Forschungszentrum Karlsruhe (GridKA-CA) und dem DFN-Verein (DFN-Grid-CA) betrieben.

Als Alternative zur Authentifizierung von Nutzern über X.509-Zertifikate können Shibboleth-Infrastrukturen [6] verwendet werden, die bereits im Bibliotheks- und eLearning-Bereich eine stark zunehmende Verbreitung finden. Shibboleth ist ein Projekt des Middleware Architecture Committee for Education im Internet2 Konsortium, in dessen Rahmen sowohl Architekturen und Policy-Strukturen als auch Technologien zu deren Umsetzung entwickelt werden. Grundprinzip ist hier die alleinige Authentifizierung durch die lokale Heimatorganisation des Nutzers. Vorteile der Integration von Shibboleth in Grid-Umgebungen werden sowohl im dezentralen Management der Nutzer durch ihre Heimatorganisationen sowie in der Verwendung verschiedenster lokaler Authentifizierungs-Verfahren wie Username/Password, X.509-Zertifikate oder auch Kerberos gesehen.

3 DELEGATION UND SINGLE SIGN-ON

Die Ausführung von Grid Jobs vollzieht sich typischerweise auf mehreren, unabhängig voneinander administrierten Systemen, die über das Internet miteinander verbunden sind. Der Zugriff auf einzelne Ressourcen erfordert eine vorherige Authentifizierung und Autorisierung. Hierbei ist zu beachten, dass häufig nur indirekt über bestimmte vorgeschaltete Systeme wie z.B. ein Workload Management auf die Ressourcen zugegriffen werden kann. In jedem Fall müssen Informationen zur Authentifizierung und Autorisierung weitergegeben, d.h. delegiert werden. Ein Single Sign-On lässt sich somit auch als Spezialfall der Delegation auffassen, bei dem beide Parteien unter der Kontrolle des Delegierenden sind.

Da der für die Verwendung von Zertifikaten notwendige private Schlüssel jedoch nicht von dem Nutzer an das Grid übergeben werden darf, sind erweiterte Verfahren zur Authentifizierung und Autorisierung erforderlich. Die mit GSI eingeführte Lösung dieses Problems stellen Proxy-Zertifikate [4], [7] dar. Ein Proxy-Zertifikat übernimmt die Identität eines Nutzer-Zertifikats, erhält jedoch eine wesentlich kürzere Gültigkeit von typisch wenigen Stunden. Abb. 1 stellt die Generierung eines Proxy-Credentials dar. Zu beachten ist, dass mit einem Proxy-Zertifikat ein weiteres, davon abgeleitetes Proxy-Zertifikates signiert werden kann. Das Proxy-Credential enthält neben Nutzer-Zertifikat und privatem Schlüssel alle Proxy-Zertifikate, von denen es abgeleitet ist. Somit können Ressourcen, denen das Proxy-Credential vorgelegt wird, stets die vollständige Zertifikatskette prüfen.

Das Proxy-Zertifikat kann außerdem mit Nutzungsbeschränkungen versehen werden, um die Gefahr des Missbrauchs einzuschränken. Durch diese Form der Delegation wird auch ein Single Sign-On für verteilte Grid-Umgebungen ermöglicht [8].

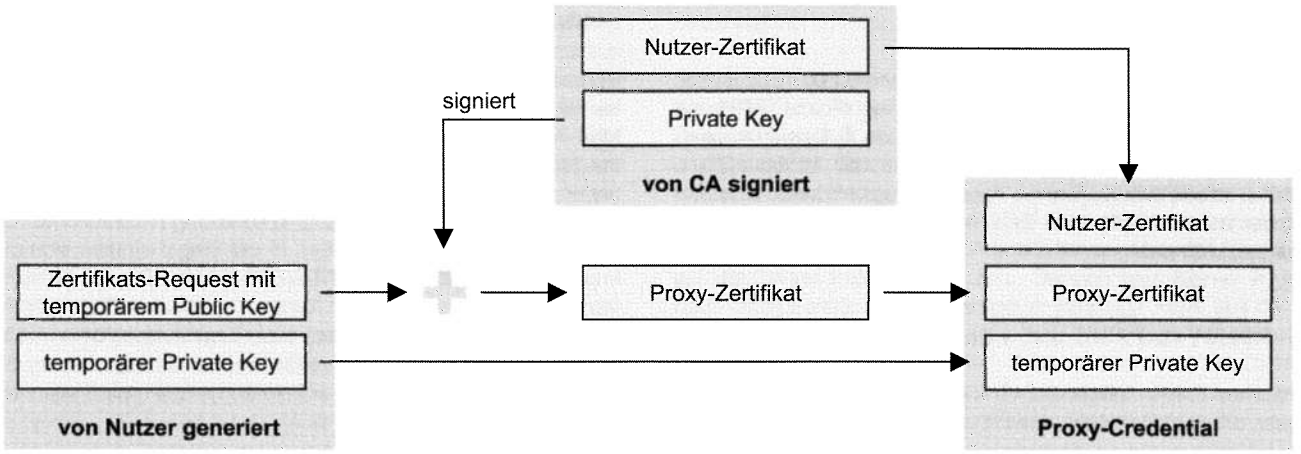

Abb. 1 Erzeugung von Proxy-Zertifikat und Proxy-Credential

Es ist zu beachten, dass Proxy-Credentials einschließlich der zum Proxy-Zertifikat gehörenden privaten Schlüssel lediglich durch die Datei-Zugriffsrechte auf den Systemen im Grid geschützt werden und z.B. von Administratoren eingesehen werden können. Aufgrund der kurzen Gültigkeit und der Möglichkeit, ein Proxy-Zertifikat mit Restriktionen zu verknüpfen, wird das Ausmaß eines potentiellen Schadens deutlich reduziert. Der Einfachheit halber wird daher im Grid kein Sperrmechanismus für Proxy-Zertifikate implementiert, wie er z.B. in PKIs mit den Certificate Revocation Lists oder über das Online Certificate Status Protocol bekannt ist. Proxy-Zertifikate können lediglich indirekt auf den Ressourcen, etwa mittels User Ban Lists, vor dem Ablauf der Gültigkeitsdauer gesperrt werden.

4 AUTORISIERUNG UND ZUGRIFFSKONTROLLE

Das Ziel von Zugriffskontrolle bzw. Autorisierung ist die Beschränkung von Aktionen und Operationen, die sowohl von Nutzern als auch von Diensten in einer Grid-Umgebung ausgeführt werden. Grundlage der Autorisierung bilden die in einer Policy formulierten Richtlinien, die in einer Virtuellen Organisation (VO) gelten (für die Definition des Begriffes VO sei auf den Artikel „Virtuelle Organisationen in Grids“ von J.-M. Milke, M. Schiffers und W. Ziegler in dieser Ausgabe verwiesen). Dazu gehört auch, die von einem Nutzer ausgeführten Programme einzuschränken, sowie einem Nutzer Rechte zu verschiedenen Bereichen eines Systems zu gewähren oder zu verwehren. Die Autorisierung setzt üblicherweise einen Prozess zur Authentifizierung von Nutzern und Diensten voraus, da auf diese Weise deren Identität festgestellt und bestätigt wurde.

Für die Autorisierung in Grid-Umgebungen stellen sich unmittelbar drei übergeordnete Herausforderungen dar:

1. Management der Nutzer und deren Rechte
2. Darstellung und Übertragung der Attribute zur Autorisierung
3. Umsetzung der Autorisierung, d.h. Gewähren oder Verwehren von Zugriffen auf Ressourcen

Für ein einheitliches Management der Informationen zur Autorisierung muss innerhalb jeder VO eine Autorität (einzelne Person oder Gruppe von Personen) definiert werden, die Nutzer zur VO zulassen und sie auch wieder aus der VO entfernen darf. Neben der Zulassung zur VO weist die Autorität den Nutzern Attribute zu, die diese näher beschreiben. Somit wird von der Identität der Nutzer abstrahiert und eine Autorisierung auf den Ressourcen auf die notwendige Betrachtung der Attribute reduziert.

In Grid Middlewares sind bisher weitgehend zentrale Ansätze für VO-Server wie Virtual Organization Membership Service (VOMS) oder Community Authorization Service (CAS) zur Vergabe von Autorisierungs-Informationen implementiert. Die Administration eines VO-Servers, d.h. die Wahrnehmung der VO-Autorität, kann dabei auf mehrere Personen verteilt werden. So können z.B. Administratoren eingeschränkte Rechte erhalten, um nur Nutzer innerhalb einer Rolle der VO zuzulassen und mit Attributen versehen zu dürfen.

Die Attribute zur Autorisierung müssen in einem im Grid-Kontext verwendeten Format (Attribut-Zertifikat oder Security Assertion Markup Language (SAML) Assertion [10]) vorliegen und ausgetauscht werden können. Dabei kontrolliert der Nutzer, welche seiner im VO-Server spezifizierten Attribute in ein Proxy-Zertifikat aufgenommen werden. Um Missbrauch zu verhindern, sind die Attribute nur dann gültig, wenn sie von der jeweiligen VO-Autorität bzw. dem VO-Server signiert sind. Zusätzlich sind die Attribut-Zertifikate oder SAML-Assertions mit einer beschränkten Gültigkeitsdauer versehen, die von dem VO-Server vorgegeben wird.

Die abgerufenen Attribute werden in ein neues Proxy-Zertifikat eingefügt, welches schließlich mit dem Absenden eines Grid Jobs den Ressourcen vorgelegt wird. Anhand der Attribute im Proxy-Zertifikat wird auf den Ressourcen zunächst lokal entschieden, ob der Zugriff gestattet wird. Hierbei ist zu beachten, dass auf diesen dezentral verwalteten Ressourcen und der zentralen VO-Autorität eine gemeinsame Policy über die Formulierung und Zuweisung von Attributen bzw. Nutzungsrechten bestehen muss (s. Kapitel 5).

Zur eigentlichen lokalen Umsetzung der Autorisierungsentscheidung auf den Ressourcen werden die Nutzer auf separate oder gemeinschaftliche, so genannte UNIX-Poolaccounts mit unterschiedlichen Rechten abgebildet. Die Festlegungen zur Abbildung werden typischerweise in den lokalen Grid-Mapfiles niedergelegt. Mit dem herkömmlichen Ansatz des Globus Toolkit erfolgt eine Abbildung lediglich anhand des Distinguished Name aus den Proxy-Zertifikaten. gLite erweitert diesen Ansatz, indem durch die Komponenten Local Center Authorization Service (LCAS) und Local Credential Mapping Service

(LCMAPS) auch die Attribute der Nutzer aus dem VO-Server in das Grid-Mapfile einbezogen werden.

Im Globus Toolkit 4 werden über das Authorization Framework [9] Policy Decision und Policy Enforcement Points (PDP und PEP) eingebunden, die auf den Ressourcen Autorisierungsentscheidungen in Abhängigkeit der übermittelten Attribute fällen. Dabei lassen sich Ketten von Autorisierungsmodulen hintereinander schalten, um eine Entscheidung für die Autorisierung herbeizuführen.

5 POLICY-MAPPING UND POLICY-KONFLIKTLÖSUNG

Jede am Grid beteiligte Domäne hat eigene administrative Regeln, d.h. legt Domänen-spezifisch fest, wer z.B. in welcher Art und Weise auf die Ressourcen zugreifen darf. Diese lokalen Regeln innerhalb einer Domäne werden im Grid als Local-Site Policies bezeichnet. Auch der Nutzer einer Ressource kann bestimmte Vorgaben machen, beispielsweise wie mit seinen personenbezogenen Daten zu verfahren ist. Diese Regeln bezeichnet man als User Policies. Innerhalb einer Domäne sind diese Regeln festgeschrieben und werden durch technische Mechanismen umgesetzt.

Im Grid kommen zu diesen bestehenden Policies neue hinzu. Auch die Gastdomäne B kann eigene Policies haben und, falls der Task des Grid-Nutzers aus der Domäne A Ressourcen der Domäne B nutzt, muss man sich mit diesen Policies – den Target-Site Policies – in der Domäne B auseinandersetzen.

Gleichzeitig kann sich die VO auf einen Satz gemeinsamer Policies einigen, die innerhalb der VO gelten sollen (VO-Policies). Trotzdem kann man nicht davon ausgehen, dass diese Policies alle einheitlich sind. In der Praxis wird es immer Policies geben, die sich widersprechen, d.h. es kann zu sogenannten Policy-Konflikten kommen. Diese Konflikte sind innerhalb der VO zu lösen. Hierzu gibt es im Wesentlichen die folgenden drei Ansätze:

1. Policy Hierarchie: Es wird eine Ordnung auf den Policies definiert und im Konfliktfall wird die höherwertige Policy wirksam, z.B. könnte die Ordnung VO-, Target-Site-, User-, Local-Site-Policy angenommen werden, d.h. die VO-Policy hätte das höchste Gewicht. Hier zeigt sich deutlich, dass die Ordnungsrelation einen entscheidenden Einfluss auf die Semantik und die Entscheidungsbefugnisse innerhalb der VO hat. Natürlich kann man auch eine partielle Ordnung definieren, bei der es gleichwertige Policies gibt (wenn z.B. Target-Site- und Local-Site Policy gleich sein sollten). In diesem Fall müssen Konflikte durch eine der folgende Strategie gelöst werden.
2. Explizite Konfliktlösung: Konflikte werden a priori oder a posteriori erkannt und dann zwischen den Beteiligten (auf-)gelöst. Diese Vorgehensweise ist aber weder im Hinblick auf die Erkennung noch bezüglich der Konfliktlösung trivial.
3. Zentrale Entscheidungsbefugnis: Dies ist ein Spezialfall von Ansatz 2. In diesem Fall treten alle beteiligten Domänen die Rechte an ihren Ressourcen z.B. an die VO ab, die dann einheitliche Policies für die gesamte VO festlegt.

6 VERTRAULICHKEIT, AUDITIERBARKEIT UND NACHVOLLZIEHBARKEIT

Vertraulichkeit ist dann gewährleistet, wenn kein Unberechtigter Kenntnis über den Inhalt geschützter Daten erlangen kann. Man kann die Vertraulichkeit der Kommunikation von der Vertraulichkeit der Daten unterscheiden. Bei der Kommunikation bieten die gängigsten Middlewares die Möglichkeit der Verschlüsselung der Kommunikationsbeziehung (vertraulicher Kanal) oder einzelner Nachrichten. In der Regel stützen sich die Implementierungen dabei auf SSL, TLS oder SSH ab. Auch die Vertraulichkeit gespeicherter Daten (im lokalen Dateisystem oder mit Hilfe von Grid Daten- bzw. Replikatsdiensten) ließe sich durch Verschlüsselung realisieren. Allerdings bieten die bestehenden Systeme hier noch keine umfassende Unterstützung innerhalb der Middleware.

Zweck des Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird. Datenschutz steht für die Idee, dass jeder Mensch grundsätzlich selbst entscheiden kann, wem er wann welche seiner persönlichen Daten zugänglich und nutzbar machen will. Dem Einzelnen muss die Möglichkeit gegeben werden, dies mit Hilfe so genannter Attribute Release Policies (ARPs) zu bestimmen und festzulegen.

Häufig werden in Grids keine vertraulichen personenbezogenen Daten verarbeitet, so dass die einschlägigen Gesetze hier nicht zur Anwendung kommen. Einen im Hinblick auf den Datenschutz besonders sensiblen Bereich stellen allerdings medizinische Anwendungen oder medizinische Forschung mit Hilfe von Grids dar. Hier kann eine Verletzung des Datenschutzes (ärztliche Schweigepflicht; Patientengeheimnis) einen Straftatbestand darstellen (§203 StGB). In der Medizin können Patientendaten nur dann in Grids verarbeitet werden, wenn sichergestellt werden kann, dass einschlägige Datenschutzbestimmungen auch eingehalten und umgesetzt werden können. Im Moment ist dies, was die Speicherung der Daten angeht, alles andere als trivial zu lösen. Die Middlewares bieten, wie oben bereits angedeutet, keine adäquaten Hilfsmittel für diese Zwecke.

Die Patienten, die an solchen Forschungsprojekten teilnehmen, werden mit erheblichen zusätzlichen Rechten ausgestattet. Sie müssen der Speicherung und Verarbeitung ihrer Daten im Rahmen einer Einwilligungserklärung zustimmen. Diese Einwilligung kann jederzeit und auch teilweise widerrufen werden. Im Fall des Widerrufs müssen die Daten für die keine Einwilligung mehr vorliegt, nachweislich und nachvollziehbar gelöscht werden (Nachvollziehbarkeit). Dazu ist es erforderlich, alle Ressourcen und Domänen, in denen die Daten verarbeitet wurden, zu kennen. Der Weg, den die Daten genommen haben, und die Operationen, die auf den Daten ausgeführt wurden, müssen nachvollziehbar sein (Auditierbarkeit).

Die Nachvollziehbarkeit steht in einem fundamentalen Widerspruch zum Grundsatz der Virtualisierung. Grids wurden entwickelt, um beispielsweise Speicher-Ressourcen zu virtualisieren, d.h. der Nutzer kennt den physischen Speicherort seiner Daten und die Organisation, welche die Speicher-Ressourcen zur Verfügung stellt, gar nicht mehr. Aus Optimierungsgründen können auch Daten innerhalb des Grids verlagert und repliziert werden. Die Frage, wie eine nachweisbare und verlässliche Löschung aller Daten in den verschiedenen Organisationen durchgeführt werden kann, ist zur Zeit nicht geklärt.

Auch die Auditierbarkeit, die eng mit Fragen des Loggings verbunden ist, ist offen. Hier ist es erforderlich, den Weg, den die Daten genommen haben und alle Operationen die mit und auf den Daten durchgeführt wurden, nachvollziehen zu können. Zum einen bedeutet dies, dass alle entsprechenden Aktionen protokolliert werden müssen. Andererseits muss auch sichergestellt sein, dass die entsprechenden Logs nicht zu einem späteren Zeitpunkt manipuliert wurden.

7 SCHUTZ DER GRID-INFRASTRUKTUREN

Die im Grid gespeicherten und bearbeiteten Daten, der Zugang zu den Ressourcen Virtueller Organisationen sowie der Betrieb zentraler Netzdienste, wie z.B. einer PKI oder Directory- und Accounting-Services, sind sowohl vor unbefugten Zugriffen als auch vor kompromittierenden Angriffen zu schützen. Für den Aufbau und den Betrieb sicherer Netzinfrastrukturen sind dabei Firewalls ein wesentliches Hilfsmittel. Die Anwendungen in einer Grid-Umgebung und die daraus resultierenden Anforderungen an Firewalls unterscheiden sich jedoch erheblich von gewöhnlichen Campus-Netzen oder Server-Umgebungen. Zum einen stellen Grid-Anwendungen extreme Durchsatz- und Latenz-Anforderungen, zum anderen kommen Grid-Protokolle zum Einsatz, die von Firewalls nicht interpretiert werden können und für die daher kein aktiver Schutz geboten werden kann.

Mit dem notwendigen Einsatz von Firewalls gehen typische Einschränkungen einher, die beim Aufbau der Grid-Netzinfrastrukturen unbedingt zu beachten sind. Da nicht mehr über beliebige Protokolle auf die Dienste in den geschützten Netzen zugegriffen werden kann, wird die Flexibilität der Anwendungen eingeschränkt. Eine auf Firewalls heute übliche Lösung besteht in der Analyse von Protokollabläufen und der dynamischen Freigabe von Datenflüssen je nach erkanntem Bedarf. Dieses Verfahren setzt jedoch voraus, dass die den Anwendungen zugrunde liegenden Protokollstacks in den Firewalls implementiert sind. Da diese Voraussetzung für Protokolle Grid-spezifischer Anwendungen nicht erfüllt wird, scheitert dieser Ansatz für das Grid-Computing. Dabei ist auch zu berücksichtigen, dass die weitgehende Verwendung verschlüsselter Datenströme in der GSI eine aktive Interpretation der Protokolle und geeignete Reaktionen durch Firewalls weitgehend verhindert. Als einzige Alternative wird derzeit eine permanente manuelle Freischaltung von Ressourcen, insbesondere großer Bereiche von Ports, praktiziert, welche jedoch hinsichtlich Netzwerk-Sicherheit und Wartbarkeit nicht akzeptabel ist.

Eine weitere Herausforderung stellen neue Kommunikationsparadigmen dar, die in Grid-Umgebungen umgesetzt werden. So kann ein GridFTP-Client einen so genannten Third Party Transfer zwischen zwei Servern initiieren. Die Kontrollkanäle werden ausschließlich zwischen dem Client und den Servern aufgebaut. Zwischen den beteiligten Servern wird lediglich eine Datenverbindung, aber kein Kontrollkanal etabliert, so dass den Firewalls hier auch bei unverschlüsselten Verbindungen keine Möglichkeiten für ein aktives Freischalten geboten wird.

Als weiteres Merkmal verteilt GridFTP Datentransfers auf mehrere parallele TCP-Verbindungen, um den gesamten Durchsatz zu steigern. Dadurch benötigt GridFTP für jeden Transfer ca. 20 offene TCP-Verbindungen. Bekannte Abschätzungen für das Globus Toolkit oder gLite fordern die Berücksichtigung von bis zu 250 gleichzeitigen Nutzern, woraus sich auf den Firewalls die notwendige dauerhafte Freischaltung von 5000 Ports für die beteiligten IP-Adressen oder sogar IP-Subnetze ergibt.

Abb. 2 stellt den Ablauf und die Kommunikationsbeziehungen für einen Third Party Transfer dar. Nachdem der Client zu den Servern A und B jeweils einen Kontrollkanal aufgebaut hat, setzt er sie mit den Kommandos SPAS (Striped Passive) und SPOR (Striped Port) in Empfangs- bzw. Sendebereitschaft. Der Kontrollkanal für GridFTP ist mit 2811/tcp allgemein festgelegt und sollte in den Firewalls vor A und B für eingehenden Verkehr auf die Server freigeschaltet sein. Danach baut Server A direkte Datenkanäle zu B auf, wobei er beliebige Ports aus dem oben erläuterten Bereich von typisch 5000 Ports adressiert. Die Firewall vor B erhält aus dem Kontrollkanal zwischen Client und B jedoch keine geeigneten Informationen über diese Datenkanäle. Entsprechend kann sie den Datenkanal nicht dynamisch erkennen und freischalten, wie es bei klassischen FTP-Verbindungen der Fall ist. Der Aufbau der Datenkanäle ist folglich nur dann erfolgreich, wenn der gesamte Port-Bereich auf der Firewall vor B freigegeben ist. Wenn die IP-Adresse von A nicht a priori bekannt ist, erweitert sich die notwendige Freischaltung sogar auf beliebige IP-Adressen. Diese Situation wird zusätzlich erschwert, wenn Frond-End und Data-Nodes eines GridFTP-Servers über unterschiedliche IP-Adressen verfügen.

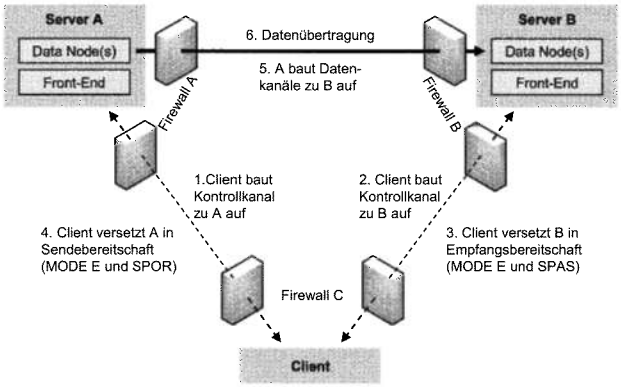

Abb. 2 Third Party Transfer in GridFTP

Als möglicher Ausweg aus dieser Situation wird derzeit die dynamische Konfiguration von Firewalls diskutiert. Hierbei wird einer Firewall in einem separaten Schritt vor der eigentlichen Kommunikation zwischen den Grid-Services ein Verbindungswunsch mit Angabe der entsprechend IP-Adressen und Ports authentifiziert und autorisiert mitgeteilt, wonach die Firewall die erforderlichen Ressourcen temporär freischaltet. Sämtliche Ansätze zur Umsetzung dynamischer Firewalls befinden sich derzeit in einem frühen Entwicklungsstadium. Je nach gewähltem Ansatz sind hierfür Anpassungen an der Firewall oder den Grid-Services erforderlich, so dass kurzfristige Lösungen nicht zu erwarten sind.

8 CERT FÜR GRIDS

Computer Notfallteams (Computer Emergency Response Teams – CERT) leisten durch ihre Dienste seit langem einen wichtigen Beitrag zur Sicherung von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der eingesetzten Ressourcen und Daten. Klassische Aufgaben wie die Bearbeitung von Sicherheitsvorfällen (Incident Response), der Betrieb einer Hot-

line für den direkten Kontakt der Anwender zum CERT, das Bereitstellen sicherheitsrelevanter Informationen wie Advisories oder Informationsschriften oder die Schulung von Anwendern und Administratoren sind klar definiert, etabliert und in der Praxis erprobt.

Diese CERT-Dienstleistungen sind auch in Grid-Infrastrukturen unverzichtbar. Allerdings bringen Grids eine ganze Reihe sicherheitsrelevanter Neuerungen und Herausforderungen mit sich, die mit klassischen CERT-Dienstleistungen nicht abgedeckt sind, obwohl hier natürlich auf die Erfahrungen bei Erbringung dieser Dienste in herkömmlichen Internet-Strukturen zurückgegriffen werden kann.

Mit den Communities und Virtuellen Organisationen nutzen Anwendergruppen die Grid Strukturen, die bisher nicht oder nur wenig mit Sicherheitsproblemen konfrontiert waren, und es kommt Software zum Einsatz, die bisher nicht im Fokus der Arbeit von CERTs stand. Dies betrifft sowohl Betriebssysteme und Anwendungssoftware als auch Middlewarekomponenten (z.B. Globus, UNICORE, gLite). Auch der in einer Grid-Infrastruktur zu erwartende Transport sehr großer Datenmengen über das Netz bedarf einer besonderen Beobachtung und erfordert beispielsweise bei bestehenden Alarmsystemen entsprechende Anpassungen.

Bestehende Sicherheitsrichtlinien sind in der Regel nicht auf diese Besonderheiten einer Grid-Infrastruktur ausgerichtet und bedürfen deshalb einer intensiven Überarbeitung oder Neukonzeption. Es ist deshalb notwendig, die klassischen CERT-Dienste um Grid-spezifische Komponenten zu erweitern, indem z.B. die neuen Softwarekomponenten einem Review auf sicherheitsrelevante Schwachstellen unterzogen und Communities informiert und geschult werden.

Im Rahmen eines D-Grid Projektes wird diese Erweiterung pilotiert. Anhand der vier Bereiche „Koordination und Kooperation", „Prävention", „Früherkennung" und „Reaktion" werden bestehende CERT-Strukturen analysiert und sicherheitsrelevante Grid-Komponenten beschrieben. Dabei befasst sich der Bereich „Früherkennung" auch mit dem Schutz von Grid-Infrastrukturen und ergänzt somit die im vorigen Kapitel beschriebenen Verfahren.

9 AUSBLICK

Mit der zunehmenden Bedeutung von Grids und der steigenden Anzahl von Communities, die diese Grids nutzen, wächst auch der Bedarf, die Sicherheit in Grids zu verbessern. Dass dies nicht als einfache, isolierte Aufgabe zu sehen ist, verdeutlicht der vorliegende Artikel. Sicherheit in Grids umfasst ein sehr breites Spektrum an Funktionalität, Werkzeugen sowie technischen und organisatorischen Maßnahmen. Dies reicht von Fragen der Authentifizierung und Autorisierung über Vertraulichkeit und Datenschutz, die Sicherung der Grid-Infrastrukturen bis hin zur Gestaltung und Umsetzung geeigneter Policies.

Welche dieser „Sicherheits-Bausteine" mit welcher Priorität realisiert werden, hängt wesentlich von den Anforderungen der Nutzergruppen ab. Während z.B. in der Hochenergiephysik der Bedarf an Sicherheitsfunktionalität derzeit nicht so groß erscheint, können andere Communities – z.B. aus der Medizin oder bei Projekten in Zusammenarbeit mit industriellen Partnern – Grids ohne diese Funktionalität gar nicht nutzen. Ziel muss es daher sein, die Sicherheit in Grids unter Berücksichtigung der Anforderungen der Communities so weit zu verbessern und für die zur Zeit noch offenen Fragen angemessene Lösungen zu finden, dass möglichst viele Nutzer von den neuen Arbeitsmöglichkeiten in Grids profitieren können.

Danksagung

Die Autoren danken den Kollegen aus den Fachgebieten 3-4 und 3-5 des D-Grid Integrationsprojekts für hilfreiche Diskussionen sowie dem Münchner Netzmanagement Team (MNM-Team) unter Leitung von Prof. Dr. H.-G. Hegering für wertvolle Kommentare zu früheren Versionen dieses Artikels.

LITERATUR

[1] Foster, I.; H. Kishimoto; A. Savva; D. Berry; A. Dajaoui; A. Grimshaw; B. Horn; F. Maciel; F. Siebenlist; R. Subrammaniam; J. Treadwell; J. von Reich: The Open Grid Services Architecture, Version 1.0. GFD-I.030, Global Grid Forum, Januar 2005, http://www.ggf.org/documents/GFD.30.pdf.

[2] Nagaratnam, N.; P. Janson; J. Dayka; A. Nadalin; F. Siebenlist; V. Welch; I. Foster; S. Tuecke: The Security Architecture for Open-Grid Services. Vers. 1, Open Grid Service Architecture Security Working Group (OGSA-SEC-WG); Global Grid Forum, Juli 2002.

[3] Siebenlist, F.; V. Welch; S. Tuecke; I. Foster; N. Nagaratnam; P. Janson; J. Dayka; A. Nadalin: OGSA Security Roadmap – Global Grid Forum Specification Roadmap towards a Secure OGSA. Open Grid Service Architecture Security Working Group(OGSA-SEC-WG), Juli 2002, http://www.cs.virginia.edu/_humphrey/ogsa-sec-wg/ogsa-sec-roadmap-v13.pdf.

[4] Welch, V.; I. Foster; C. Kesselmann; O. Mulmo; L. Pearlman; S. Tuecke; J. Gawor; S. Meder; F. Siebenlist: X.509 Proxy Certificates for Dynamic Delegation. In: Proceedings of the 3rd Annual PKI R&D Workshop, 2004, http://www.globus.org/Security/papers/pki04-welch-proxy-cert-final.pdf.

[5] Foster, I.; C. Kesselman; G. Tsudik; S. Tuecke: A security architecture for computational grids. Proc. 5th ACM Conference on Computer and Communications Security, San Francisco, November 1998.

[6] Scavo, T.; S. Cantor: Shibboleth Architecture – Technical Overview. Working Draft Version 2, 8 Jun. 2005. http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-tech-overview-latest.pdf.

[7] Tuecke, S.; V. Welche; D. Engert; L. Pearlman; M. Thompson: Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile, IETF RFC 3820, 2004.

[8] Ahsant, M.; J. Basney; O. Mulmo: Grid Delegation Protocol. Workshop on Grid Security Experiences, 2004. http://www.ncsa.uiuc.edu/~jbasney/Grid-Delegation-Protocol.pdf.

[9] Barton, T.; J. Basney; T. Freeman; T. Scavo; F. Siebenlist; V. Welch; R. Ananthakrishnan; B. Baker; K. Keahey: Identity Federation and Attribute-based Authorization through the Globus Toolkit, Shibboleth, Gridshib, and MyProxy. Proc. 5th Annual PKI R&D Workshop, Gaithersburg, April 2006.

[10] Maler E. et al.: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML). OASIS, September 2003. http://www.oasis-open.org/committees/security/