Mehr Flexibilität für mehr Datenschutz und -sicherheit im Grid

Willy Weisz
Universität Wien
Institut für Scientific Computing, VCPC

Certification Authority

2. D-Grid Security Workshop
Göttingen, 27.-28. März 2007

Widersprüchliche Anforderung

Benutzer fordern:

- vertrauenswürdige Systeme bezüglich Schutz und Sicherheit ihrer Daten

Administratoren fordern

- Sicherheit ihrer Systeme

Grid-Benutzer erwarten

- flexiblen und einfachen Zugriff auf Grid-Betriebsmittel
- einfache Prozeduren für Zgriffsberechtigungen

Identifizierung, Authentisierung und Authentifizierung auf Reisen

Ausweis – Identifikationsdokument

- Personalausweis oder Reisepass

Authentisierung

- Nachweis der Identität durch Ausweisvorlage

Authentifizierung

- Optischer Abgleich von Vorleger und Dokumentenbild
- Zukunft: Computer gestützter Abgleich (RFID)

Autorisierung auf Reisen

Reisepass enthält nur Berechtigung zur Rückkehr ins Ausstellungsland

Berechtigung zur Einreise in anderes Land

- aufgrund bi- oder multilateraler Abkommen
  - ohne Dokumentvorlage (Schengen)
  - nach Vorlage von Pass oder Personalausweis
- Visa – für ganzes Land oder nur Teilregion, über alle oder nur eingeschränkte Grenzübergänge

Identifizierung, Authentifizierung und Autorisierung in Organisationen

Betriebssicherheit von Organisationen

- Identifizierung aller
  - Angestellten und kooperierenden Einheiten („wer“)
  - Betriebsmittel
  - erlaubten Aktivitäten
- Festlegung
  - Wer ist berechtigt,
  - mit welchen Betriebsmitteln
  - was zu tun.
- Funktioniert in kleinen Organisationen
- Skaliert nicht in großen, verteilten Organisationen

Autorisierung in Organisationen

Daher

- Vereinbarung von Attributen für
  - Handelnde (Rollen, Funktionen, Hierarchiestufen etc.)
  - Betriebsmittel
  - Eventuell für Aktionen
- Autorisierungsregeln
  - Welcher Typ von Handelnden
  - darf mit welcher Art Betriebsmitteln
  - welche (Art von) Handlung setzen?

Die Zuordnung von Attributen zu Einzelnen erfolgt „lokal“

Autorisierung bei Zusammenarbeit

Gemeinschaftsprojekte von Organisationen müssen

- Die Autorisierungsmatrix jedes Partners berücksichtigen
- Projektbezogen
  - Vereinbarungen für Attribute aufgrund der Zusammenarbeit treffen,
  - Einzelnen, die zur Zusammenarbeit berechtigt sind, diese Attribute zuordnen,
  - Eine projektspezifische Autorisierungsmatrix definieren

Organisationen im Grid

Organisationen im Grid stellen eine spezielle Art von Zusammenarbeit dar:

- Sie teilen sich Betriebsmittel,
- sind meist geographisch weit auseinander,
- Ihre Teilnehmer treffen sich eher über das Internet als in Gemeinschaftssitzungen
- Sie werden „virtuelle Organisationen“ (VO) genannt.

Identifizierung und Authentifizierung im Grid

Verwendung einer Infrastruktur öffentlicher Schlüssel (Public Key Infrastructure – PKI) mit

- X.509 Zertifikaten und
- X.509 Zertifikatswiderrufslisten

Identifizierung und Authentifizierung im Grid

Identifizierung durch einen vertrauenswürdigen Dritten (Trusted Third Party)

- Die Zertifizierungsstelle (CA),
- die ein Zertifikat, das den öffentlichen Schlüssel enthält, digital signiert und
- damit bestätigt, dass der durch die „Subject“-Eintrag des Zertifikats identifizierte Endeinheit (Mensch oder System/Dienst) im Besitz des zugehörigen privaten Schlüssels ist.

Identifizierung und Authentifizierung im Grid

Authentifizierung

- Die Endeinheit muss den Besitz des privaten Schlüssels, der zum Zertifikat passt, bei jeder Interaktion nachweisen.

Identifizierung und Authentifizierung im Grid

Einheiten mit Zertifikaten:

- Verbraucher (Menschen oder andere Einheiten)
- Betriebsmittel
- Anwendungen
- Dienste

Vertrauen in PKIs

Vertrauende Instanzen (Relying Parties)
vertrauen darauf, dass
die Zertifizierungsstellen Zertifikate ausstellen,
die zumindest Minimalanforderungen an

- die Identitätsprüfung,
- die sichere Verwahrung und Verwendung des privaten Schlüssels der CA,
- die Verarbeitungsprozesse,
- die Verfügbarkeit von Widerrufsinformation
- andere Angaben im Sicherheits- und Zertifizierungskonzept (Certificate Policy / Certification Practice Statement – CP/CPS)

genügen

Vertrauen in PKIs

Vertrauende Instanzen vertrauen darauf, das

- Benutzer ihre privaten Schlüssel vor unerlaubten Zugriff und Benutzung schützen durch
  - Speicherung in einem sicheren „Behältnis“, auf das nur der Eigner zugreifen kann
    - Eine geschützte Datei mit restriktiven Zugriffsrechten in einem sicheren Dateisystem
    - Auf einer sicheren Hardware-Einheit (Secure Token) wie SmartCard, USB Token, HSM, ...) - der einzige wirklich sichere Behälter
  - Verwendung einer „guten“ Verschlüsselung, die nur der Eigner kennt.

CAs und ihre Föderationen

CAs existieren

- innerhalb von Organisationen,
- für Vos (z.B. UNICORE CA),
- für regionale (nationale) Gemeinschaften.

Vertrauende Instanzen verlassen sich darauf, dass bestimmte CAs vertrauenswürdige Zertifikate ausstellen.

CAs können Föderationen bilden, um:

- anzuerkennen, dass ihre Mindestsicherheits-anforderungen kompatibel sind
- Instanzen Vertrauen in CAs, die sie nicht kennen, zu vermitteln.

Autorisierung aufgrund der Identität

Zugriffssteuerung auf *Ermessens*basis

Discretionary Access Control – ADC

Fast immer genutzt in:

- Betriebssystemen,
- Derzeitiger Grid Middleware
  - Globus Tool Kit
  - UNICORE

Autorisierung aufgrund der Identität

Nach Identifikation und Authentifizierung

- wird ein Verbraucher (Benutzer) einer Identität des Betriebssystems zugeordnet
- Erfreut er sich einer „fast ungehinderten Selbstbedienung“

Diese Autorisierung ist

- zu grobkörnig,
- Nicht brauchbar für z.B. Datenbanksysteme

Das Grid ist derzeit eher nicht geeignet für den Einsatz föderierter Datenbanken

- Weder OGSA-DAI noch die GGF DAIS-WG haben bisher Sicherheitsaspekte in Angriff genommen

Hochsicherheitsautorisierung

Einheiten (Verbraucher oder Betriebsmittel) in Sicherheits-/Vertrauenssstufen eingeteilt

- Zugriffssteuerung auf *Ermächtigung*sbasis
- *Mandatory* Access Control – MAC

Lesezugriff auf Objekte mit gleicher niedrigerer Einstufung (Read Down)

Schreibzugriff auf Objekte mit gleicher oder höherer Einstufung (Write Up)

Verbraucher muss sich eventuell temporär niedriger einstufen, um ein Objekt zu schreiben.

Zu restriktiv für die meisten Grid-Anwendungen

Rollenbasierte Zugriffssteuerung

Role-based Access Control – RBAC

RBAC ist die Lösung, wenn

- DAC zu schwach und
- MAC zu restriktiv ist.

Ermöglicht

- Rechte feinkörniger zu vergeben als DAC
- einfache Anpassung an einen Rollenwechsel
- die Vereinbarung hierarchisch gestaffelter Rollen ähnlich einer MAC

Attributbasierte Zugriffssteuerung

Attribute-based Access Control – ABAC

Noch flexibler als RBAC

- Autorisierungen aufgrund von Attributen sind weniger statisch als die Autorisierungen aufgrund von Verbraucher-Betriebsmittel-Verhältnissen in RBAC

Eine Rolle ist eben eines der möglichen Attribute

$\Rightarrow$RBAC ist eine Teilmenge von ABAC

Benutzerdatenbank beim Betriebsmittel

Vollständige Liste aller zugelassenen Einheiten

- UNICORE – UUDB am V-Site
- Globus – gridmap-Datei am ausführenden Rechner

gridmap-Datei

- fernwartbar durch VO-Verwaltungssystem (z.B. VOMS)
- speichert keine X.509 Zertifikate

UUDB

- nur lokal zu verwalten
- speichert Zertifikate – mit begrenzter Lebensdauer
- skaliert nicht

Verwaltung von Autorisierungen in VOs

VOs sollten

- von Identitäten und ihren Zugriffsrechten
- auf Richtlinien (policies), die auf Rollen und Attributen für
  - jeden einzelnen der Teilnehmer intern und
  - das Gemeinschaftsprojekt an sich

  beruhen,

übergehen.

Grundsätze werden in einer VO seltener geändert als die Teilnehmerstruktur.

Attributautoritäten

Ein Verbraucher kann

- In seiner eigenen Organisation
- In der VO

Attribute haben oder Rollen einnehmen.

Informationen über Attribute/Rollen werden von Attributautoritäten (AA)

- der einzelnen Organisationen
- der VO

veröffentlicht und signiert werden.

Gleiches gilt für Attribute der Betriebsmittel.

Datensschutz - Anonymität

Es kann wichtig (oder vom Gesetz gefördert) werden, dass

- die Identität eines Subjekts/Objekts für die Zeit der Verarbeitung anonymisiert wird,
- jedoch später wieder rückverfolgbar (z.B. für eine Abrechnung oder eine Rückmeldung) sein muss

Pseudonymisierung

- z.B. durch Abbildung auf eine „allgemeine Identität“ mit Attributen, die richtige Verarbeitung und später bei Bedarf die Rückverfolgung ermöglichen

Autorisierung durch Richtlinien

Richtlinie (Policy) = Satz von Regeln, die auf Identitäten und Attributen von Verbrauchern und Betriebsmitteln beruhen

Kann die Bewilligung durch Dritten erfordern

- z.B. durch den Patienten zur Freigabe seiner Gesundheitsakte an den Arzt oder die Versicherung
- Der Dritte muss ebenfalls authentifiziert werden,
- seine Attribute berücksichtigt werden.

Anzustrebende Autorisierungsarchitektur

Für jedes Subjekt und Objekt einer Anforderung müssen

- eine vollständige Policy oder ein Satz von Policies durch eine *Source of Authority* (SOA), auch als *Policy Administration Point* (PAP) bezeichnet, definiert werden,
- eine daraus abgeleitete Entscheidung, anzunehmen oder abzulehnen, ableiten.

Anzustrebende Autorisierungsarchitektur

Der Klientenagent sammelt alle ihm zugänglichen Authentisierungsdaten und Attribute

- vom Anforderer
- von *Policy Information Points* (PIP), z.B. ihm zugänglichen AAs

Er sendet diese mit der Anforderung an das Betriebsmittel

Anzustrebende Autorisierungsarchitektur

Dort übernimmt der *Policy Enforcing Point* (PEP) die Anforderung mit allen beigefügten Informationen.

Der PEP übergibt zuerst einmal die Anforderung an einen *Policy Decision Point* (PDP)

- optimal beim Betriebsmittel angesiedelt
- könnte auch übergeordnet angesiedelt sein

Anzustrebende Autorisierungsarchitektur

Der PDP

- wendet die Regeln der Policy an
- unter Berücksichtigung aller Identitäts- und Attributinformationen
- kann eventuell von PIPs, z.B. AAs, weitere Informationen anfordern,
- entscheidet über die Anforderung
- reicht die Entscheidung - *annehmen* oder *ablehnen* – an den PEP zurück.

Anzustrebende Autorisierungsarchitektur

Der PEP schließlich

- setzt die Entscheidung des PDP zwingend um oder
- trifft eine Standardentscheidung, wenn der PDP keine Entscheidung treffen konnte, und setzt diese zwingend um.

Attributsammlung

Attributsammlung durch

- den Agenten des Anforderers
- den PDP

Sammlung durch den Agenten des Anforderers

- skaliert besser
- leichter realisierbar, insbesondere in Bezug auf Attribute, die in der Organisation des Anfordernden vorhanden sind.

Attributsammlung

Attribute oft in unterschiedlichen Datenbanken vorhanden.

Daher Bedarf nach

- Genormten Protokollen zum Transport der Attribute,
- Entwicklung von *Plugins* für Datenbanken, um diese Protokolle zu bedienen.

Vorhandene Protokollnormen

- X.509 Attributzertifikate im ASN.1-Format
- die XML-kodierte Security Assertion Markup Language (SAML)

Was gibt es bereits?

Einige Projekte haben bereits Werkzeuge entwickelt, die einige Teile der anzustrebenden Architektur realisieren.

Meist wurden sie für *Web Services* und das *Globus Toolkit* entwickelt.

UNICORE wurde dabei nie direkt angesprochen, bei der gerade stattfindenden Neukonzeption des Sicherheitskonzepts für UNICORE/GS ist das Tor für eine Totalüberholung offen.

VOMS

Virtual Organisation Management System

- Verwaltet VOs
- Benutzer können Aufnahme in VO anfordern
- Administrator stimmt zu oder lehnt ab
- Am unteren trivialen Ende generiert VOMS eine gridmap-Datei
- Nur PIP-Funktionen – PDP-Funktionen werden dem Globus Gatekeeper überlassen

Shibboleth

- Föderierte Infrastruktur zur Autorisierung, um Web Single Sign-on über Organisationsgrenzen hinweg zu ermöglichen.
- Nutzt SAML v1.1 für den Austausch von Attributen
- Reicht Autorisierungsinformationen in Form von *opaque handles* weiter
  - Schafft Anonymität
  - Ermöglicht jedoch Rückverfolgung zum Anfordernden

GridShib

Integriert Shibboleth mit der von Globus Toolkit version 4 (GTK4) bereit gestellten Grid-Technology

Erfordert effiziente Abbildung der *opaque handle* von Shibboleth auf den Subject DN eines X.509 Zertifikats, wie GTK4 es erfordert.

PERMIS

- Infrastruktur zur Verwaltung von Privilegien
- Autorisierungsdienst, der voll auf einer Policy aufbaut
- Regelwerk in XML kodiert
- Unterstützt RBAC

GridShibPERMIS

Kombiniert

- die Stärke von Shibboleth zur Bereitstellung von Identität und Attributen
  - GridShib stellt den PIP bereit
- Die Grid-Infrastruktur von GTK4
  - stellt die X.509 Authentifizierung bereit
- Autorisierung aufgrund einer Policy von PERMIS bereitgestellt
  - durch seine Schnittstelle *GridShibPERMIS Context* als PDP im *GTK4 Authorisation Framework*

UNICORE/GS +(?)

Explicit Trust Delegation – ETD

Aufgabe: Ermöglicht dynamische Generierung von Sub-Jobs ***nachdem*** der Job vom Anforderer bereits abgesetzt wurde.

- Anforderer erstellt ein Vertrauensattribut für den UNICORE-Agenten,
- damit dieser Aktionen namens des Anforderers autorisieren kann

Erster(?) Einsatz von Attributen in UNICORE – Anforderer ist AA

UNICORE/GS +(?)

Sicherheit modular in UNICORE integrierbar

Anzustrebende PIP-PAP-PDP-PEP-Sicherheits-architektur auf Basis von Identität und Attributen könnte über Plugins realisiert werden.

Wichtig: Einhalten von Normen für Interoperabilität mit anderen Grid Infrastrukturen

Kontakt

Willy Weisz

weisz@vcpc.univie.ac.at

Universität Wien
Institut für Scientific Computing, VCPC

http://www.vcpc.univie.ac.at

AustrianGrid Certification Authority

http://www.austriangridca.at

Austrian Grid ist ein vom österreichischen Bundesministerium für Bildung, Wissenschaft und Kultur (bm:bwk) auf Empfehlung des Rats für Forschungs- und Technologieentwicklung gefördertes Projekt