Sicherheit: Ergebnisse aus D-Grid 1 und Ausblick auf D-Grid 2

DGI-2 FG3 „Sicherheit“

3. Security Workshop Göttingen

1.-2. April 2008

Marcus Pattloch, DFN-Verein

Sicherheit im D-Grid (1)

- Notwendiger Service im D-Grid
  - Bedarf für (IT-)Sicherheit in **allen** Communities
  - Bedarf für Sicherheit bei **allen** Anbietern
- Diverse Arbeiten zum Thema Sicherheit
  - Im DGI-1 FG3 wichtige Querschnittsaufgaben
  - In einigen Communities anwendungsspezifische Arbeitspakte
- Enge Zusammenarbeit mit CGs
  - Aktive Communities stark beteiligt
  - Andere Communities an Ergebnissen interessiert

Sicherheit im D-Grid (2)

- Neue Community-Projekte verfügen z.T. über geringe Vorkenntnisse bzgl. „Sicherheit in Grids“
  - Erfahrung aus D-Grid 1
  - Erkenntnis nach „All-Hands Meeting“ zu D-Grid 2
- Auch neue D-Grid Communities haben großen Bedarf am Thema Sicherheit
- Ein wichtiges Ziel des DGI-2 FG3 „Sicherheit“ ist es, auch die neuen Communities an den erreichten Ergebnissen partizipieren zu lassen und sie in die Arbeiten einzubinden

Themen für DGI-2

- Themen haben sich ergeben durch
  - Ergebnisse der Workshops
  - Anforderungen der Communities
  - Internationale Entwicklungen im Grid-Umfeld
  - IVOM hat als Gap-Projekt Lücken im Bereich AAI/VO geschlossen (Integration Shibboleth)
- Themen des DGI-2 FG3 „Sicherheit“ sind
  - Sicherheitsmanagement (FG 3-1)
  - AAI/VO (FG 3-2)
  - Firewalls (FG 3-3)

Sicherheitsmanagement (1)

- Ausgangslage
  - Erfahrungen aus DGI-1 und beim Aufbau der D-Grid Sonderinvestitionen zeigen
    - nebenläufiges Behandeln sicherheitsrelevanter Frage-stellungen ohne geeignete Koordination führt zu nicht optimalen Ergebnissen
    - es besteht die Gefahr, dass im D-Grid sicherheits-technische Insellösungen entstehen
- Ziele
  - Koordination der Sicherheitsaktivitäten im D-Grid
  - Fokus auf die nachhaltige Sicherung entsprechender Dienste

Sicherheitsmanagement (2)

- Arbeitspunkte
  - Koordination mit den Communities
  - Koordination der Erstellung von Policies im Sicherheitsbereich für einheitliche Abläufe im D-Grid
  - Koordination zum Abgleich mit internationalen Aktivitäten (z.B. EGEE / Open Science Grid)
  - Definition und Umsetzung unterschiedlicher Sicherheitsniveaus auf der D-Grid Infrastruktur
- Teilnehmende Einrichtungen
  - RRZN Hannover, DFN-Verein

AAI/VO (1)

- Ausgangslage
  - Der Bereich AAI/VO hat sich im D-Grid als stark nachgefragter Punkt im Sicherheitsbereich erwiesen
    - Im DGI-1 und im IVOM-Projekt wurden AAI-Lösungen entwickelt, die Basisanforderungen abdecken können und z.B. auf den Sonderinvestitionen eingesetzt werden
- Ziele
  - Aufbauend auf den Ergebnissen aus DGI-1 und IVOM muss die AAI an erweiterte Anforderungen der Communities angepasst werden, z.B.
    - transparente Integration von VO- und Identity Management (VOMS/VOMRS und Shibboleth)
    - Bedarf für attribut-basierte Autorisierung

AAI/VO (2)

- Arbeitspunkte
  - Konzeption
    - Entwicklung generische VO-Struktur
    - Definition von Attributen für die Autorisierung
    - Virtualisierung von Arbeitsumgebungen (Virt. Workspace)
  - Umsetzung
    - Umsetzung der konzipierten Lösungen
    - Betrieb einer Test-Infrastruktur
  - Unterstützung des D-Grid Betriebs
    - Operativer Einsatz der zuvor konzipierten Lösungen
- Teilnehmende Einrichtungen
  - RRZN Hannover, FhG SCAI, LRZ, DFN-Verein

Sicherheit durch die DFN-AAI

- Der DFN-Verein hat die DFN-AAI außerhalb D-Grid aufgebaut und betreibt diese (Basis: Shibboleth)
  - kontrollierter Zugriff auf geschützte Ressourcen
  - Nutzung auch im D-Grid
- Anwendungsgebiete im D-Grid
  - C3-Community, Text-Grid, (INGRID)
  - kurzlebige Grid-Zertifikate (SLCS)
- Authentifizierung und Autorisierung durch DFN-AAI ermöglicht
  - Nutzung des D-Grid ohne Grid-Zertifikate
  - dezentrale Pflege der Basisdaten
  - Unterstützung verschiedener Sicherheitsniveaus

Firewalls (1)

- Ausgangslage
  - Firewalls bei vielen D-Grid Partnern im Einsatz
  - Einige D-Grid Anwendungen erfordern statische Freischaltung vieler Ports (insb. GridFTP)
  - Freischaltung ist aus sicherheitstechnischer Sicht kritisch und kaum akzeptabel
- Ziele
  - (Weiter)Entwicklung D-Grid-weiter Empfehlungen für den sicheren Betrieb von Firewalls
  - Empfehlungen zur Nutzung Höchstleistungsfirewalls
  - Sicherung der Nachhaltigkeit durch Aufbau DFN-Firewalllabor

Firewalls (2)

- Arbeitspunkte
  - Deployment und Support
    - Support der Communities und Ressourcen-Provider
    - Werkzeuge zur Prüfung von Firewall-Konfigurationen
    - Umsetzung unterschiedlicher Sicherheitsniveaus im D-Grid
  - Dynamische Konfiguration
    - aktual. Analyse zur dynamischen Freischaltung von Firewalls
    - prototypische Implementierung für Grid-Applikationen
  - Performance
    - Entwicklung von Messprotokollen zum Benchmarking
    - Messungen in Labor- und Produktivumgebungen
- Teilnehmende Einrichtungen
  - RRZN Hannover, DFN-CERT, FZ Jülich, RWTH Aachen, DFN-Verein

Sicherheit D-Grid Netzplattform

- X-WiN als Netzplattform des D-Grid
- Mechanismen zur Sicherung des X-WiN
  - Beobachtung der Verkehrsflüsse
    - nicht der Inhalte!
  - Verkehrsflussanalyse
  - Optimierungsrechnungen zur Netzstruktur
  - Angriffe auf die Netzplattform erkennen
  - Intrusion Detection / Prevention Systeme

Sicherheit D-Grid Nutzer

- Mechanismen zur Sicherung der Nutzer, Anwender und Anwendungen im X-WiN
- Im „klassischen Netzbetrieb“ seit ca. 15 Jahren durch DFN-CERT etabliert
  - Standard DFN-CERT Dienste werden um Grid-Komponenten ergänzt
  - (DFN-)Grid-CERT unterstützt bei Grid-Vorfällen
- Grid-Anwendungen bringen neue Probleme
  - z.B. verhalten sich viele Grid-Anwendungen wie DDoS-Angriffe oder Bot-Netze
  - wie kann man dies automatisch unterscheiden?
  - **Wichtig**: existierende Sicherheitsinfrastruktur anpassen und nutzen.

Zertifikate im D-Grid (1)

- Die Ausgabe von Grid-Zertifikaten im D-Grid funktioniert!
- Die Dienstleistung wird im D-Grid gemeinsam vom DFN-Verein und vom FZ Karlsruhe erbracht
- Bilanz der ersten 2-3 Jahre
  - mehrere Tausend Grid-Zertifikate ausgegeben
  - mehr als 100 Registrierungsstellen aufgesetzt
  - Zertifikatanfragen werden kurzfristig erledigt

Zertifikate im D-Grid (2)

- Ausstellung von Grid-Zertifikaten im D-Grid
  - Grid-Zertifikate werden ausschließlich im Rahmen der EUGridPMA ausgestellt
  - Grid-Zertifikate werden weltweit anerkannt, durch das von der EUGridPMA bereitgestellte Repository der Root Zertifikate der CAs
  - Technisch grundsätzlich kein Unterschied zu „normalen“ Zertifikaten (X.509), aber
    - eigenes Wurzelzertifikat
    - eigene Policy
    - eigene Infrastruktur, ...

Zertifikate im D-Grid (3)

- Neuer Typ von Grid-Zertifikaten
  - SLCS (Short Lived Credential Service)
  - Verwendung der GridShib Software
  - keine (Grid-)Zertifikate erforderlich
- Pilotimplementierung im DFN ist aufgebaut und in Betrieb
  - Integration als Service Provider in der DFN-AAI
  - Vorstellung auf IVOM-Workshop Hannover (2. 2008)
  - Architekturpapier wird gerade erstellt
  - Akkreditierung des SLCS bei EUGridPMA geplant

Virtualisierung

- s. nächster Beitrag von M. Smith

Zusammenfassung

- Sicherheit bleibt im D-Grid ein wichtiges Thema
- Klare Ausrichtung der Arbeiten im Bereich Sicherheit auf
  - Bedarfe der Communities
  - Betriebsnahe Umsetzung auf der D-Grid Infrastruktur
- Wenn Bedarfe der Communities derzeit unklar oder wenn starke Entwicklungskomponente vorhanden, dann bleibt Möglichkeit eines Gap-Projektes (z.B. Intrusion Detection)
- Die Arbeitspakete decken zentrale Aufgaben ab
  - Sicherheitsmanagement, AAI/VO, Firewalls
  - PKI, Sicherheit Netzplattform / Nutzer, Virtualisierung