MPRA
Munich Personal RePEc Archive

A proposal for Security Architecture for Grid Services

Amroush, Fadi and Bouchi, Amer
University of Aleppo

02. November 2008

Online at http://mpra.ub.uni-muenchen.de/28040/
MPRA Paper No. 28040, posted 10. January 2011 / 14:47

مقترح لبناء منهجية الأمن لخدمات بيئة Grid
A proposal for Security Architecture for Grid Services

Fadi Amroush [1], Amer Bouchi [1]
[1] *Faculty of electrical engineering, Dpt of Computer Engineering, Aleppo University*
{Fadyamr@yahoo.com | Amer.Boushi@caramail.com}

ملخص البحث Abstract

يقدم البحث التالي إقتراحا لاستراتيجية كاملة لبناء منهجيات الأمن ضمن خدمات بيئة OGSA (Open Grid Services Architecture)، حيث يقدم منهجية شاملة لتنفيذ السياسة الأمنية الصحيحة التي تدعم، تتكامل، تعرف النماذج والآليات المتعلقة بالأمن، بالاضافة للبروتوكولات، المنصات، التقنيات اللازمة لتحقيق أنواع مختلفة من السيايات الأمنية بشكل تام.

تهدف هذه الهيكلية المقترحة للتوافق مع النماذج المعتمدة والتي تعمل حاليا ضمن خدمات الويب Web Services المستخدمة بشكل واسع لتحقيق خدمات OGSA، ولتنفيذ هذه التحديات الكبيرة في الأمن، يقترح هذا البحث دليلا عمليا لتحقيق خدمات GRID آمنة ومتكاملة ومتبادلة مع بعضها البعض والمعتمدة على مجموعة من المبادئ التقنية الأمنية، تناقش الفصول التالية التحديات الأمنية الموجودة في بيئة GRID وترجمة هذه التحديات إلى متطلبات حقيقية، بعد ذلك يقدم البحث هيكلية مقترحة لنموذج الأمن في GRID والتي تعرف التحديات والمتطلبات الأمنية اللازمة لبيئة GRID.

1. مقدمة:

لا يغفل على أحد ضرورة الأمن لوائح الأمان وخاصة في مجال الشبكات وهي من الخطوات الهامة في حماية الشبكة أوبشكل أكبر أوأعم (الشركة،مركز،.....)،وتزود هذه اللوائح أوالقواعد المستخدمين بالقوانين والتصرفات للأعمال المسموحة والملائمة ضمن هذه الشبكة (الشركة). وما هي الأشياء والأعمال الغير مسموح بها،هناك أسباب أخرى إضافية تعرفنا أكثر بفائدة قواعد الأمان:

- تحدد التصرف الملائم والإجراءات اللازمة.
- يتم ضبط التوقعات من الإجراءات التي تتم على الشبكة.
- هذه الأهداف تعطي إمكانية العمل الجماعي سواء أكان إدارياً أومهنياً.
- تعرف أدوار ومسؤوليات كل مجموعة من مجموعات العمل في الشركة في حماية الشبكة.
- تقدم المساعدة في متابعة الأعمال القانونية إذا حدث تصرف غير مقبول.
- إعطاء تعاريف واضحة للمفاهيم والأفكار الأساسية لحماية الشبكة.

إن وجود قواعد وأسس أمان واضحة سوف يعطي لجميع سواء كانوا على الشبكة أوالشركة فهم واضح ومعرفة واضحة عن مسؤولياتهم ودور كل واحد منهم في حماية الشبكة (من المسؤول عن ماذا؟)،ويساعد في ضبط القواعد والعمليات في كل قسم من أقسام الشبكة.

1.1 الأمن في بيئة Grid:

مع تطور البرمجة التفرعية وظهور بيئة العمل التفرعية GRID، ظهرت العديد من البرتوكولات والخدمات والأدوات المترافقة مع بيئة GRID، والتي علينا التعامل معها وتعريفها عند الرغبة في بناء مجموعات افتراضية متوازنة أي ما يدعى virtual Organization (VO).

تعرف المنظمة الافتراضية virtual Organization (VO) بأنها مجموعة من الأماكن الفردية أوالجماعية التي تتشارك معا الموارد والخدمات والخاضعة لمجموعة من القواعد والسياسات الناظمة للمشاركة، وكما ذكر [ANA] فإنها "المشاركة التي تتعلق بها بيئة GRID والتي لا تتعلق بتغيير ملف دائم فحسب وانما تتحكم بالوصول المباشر للحواسيب، البرمجيات، المعطيات، والموارد الأخرى والمطلوبة من مجال واسع من مجالات حل المشاكل بشكل تعاوني collaborative problem-solving واستراتيجيات وساطة الموارد resource-brokering strategies والتي تنتشر بشكل واسع في المجالات الصناعية والعلمية والهندسية."فالمشاركة Sharing تعتبر ضرورية، قابلة للتحكم بواسطة مزودي الموارد والزبائن والتي تعرف بشكل واضح وصريح ودقيق حتى ما هي

المـوارد المتشـاركة، ومـا هوالمسـموح بالمشـاركة وماهي شروط وقيود المشاركة الموجودة.

ضمن هذا السياق نحتاج للتداخل مع النطاقات المختلفة أثناء تنفيذ سياسة أمنية واضحة وأثناء تطبيق الآليات على المنظمات الحقيقية والافتراضية على حد سواء. تشمل التقنيات التي تم تطويرها خلال بيئة GRID حلـولا أمنيـة تـدعم إدارة الاعتماديـة credentials والسياسات عندما يتم تجتاز الحسابات عدة مؤسسات، بالاضافة لبروتوكولات إدارة الموارد والخدمات التي تدعم الوصول البعيد الآمن secure remote access للمـوارد والمعطيـات المطلوبـة للحساب، واعادة تجميع عدة موارد معا، بروتوكولات الاستفسار عن المعلومات information query protocols والخـدمات التـي تقـدم التهيئـة وحالـة المعلومـات الحاليـة حـول المـوارد والمنظمـات والخـدمات .خـدمات ادارة المعطيـات data management services التـي تقوم بنقل ووضع قواعد المعطيات بين أنظمة التخزين والتطبيقات.

يعتمد المفهوم العام عى جعل هذه الخدمات افتراضية أي service virtualization، يركز عمل النموذج الحالي ل OSGA على تطوير لغة وصف خدمات الويب WDSL بالتكامل مع لغات تعريف الواجهة IDLs. [PSY]

لتنفيذ هذه التحديات الكبيرة في الأمن، يقترح هذا البحث دليلا عمليا لتحقيق خدمات GRID آمنة ومتكاملة ومتبادلة مع بعضها البعض والمعتمدة على مجموعة من المبادئ التقنية الأمنية، تناقش الفصول التالية التحديات الأمنية الموجودة في بيئة GRID وترجمة هذه التحديات إلى متطلبات حقيقية، بعد ذلك يقدم البحث هيكلية مقترحة لنموذج الأمن في GRID والتي تعرف التحديات والمتطلبات الأمنية اللازمة لبيئة GRID.

2.1 ما هو أمن المعلومات؟

حددت توصيات أمن أنظمة المعلومات والإتصالات لوكالة الأمن القومي في الولايات المتحدة بما يلي:"المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الإتصالات ولضمان أصالة وصحة هذه الإتصالات".

تضمنت النشاطات المحددة لأمن الإتصالات COMSEC أربعة أجزاء هي: أمن التشفير Crypto security، أمن النقل Transmission Security، أمن الإشعاع Emission Security والأمن الفيزيائي Physical Security. كما تضمّن تعريف أمن الإتصالات خاصيتين تتعلقان بموضوع هذا البحث: السرية والتحقق من الهوية.

2. تحديات الأمن في بيئة GRID:

يمكن أن تقسم التحديات الأمنية التي نواجهها في بيئة GRID إلى ثلاثة مجموعات : الأولى هي التكامل مع الأنظمة الموجودة مسبقا والتقنيات المستخدمة والثانية هي التداخل وتبادل المعطيات بين بيئات الاستضافة المختلفة مثل(J2EE servers،.NET servers، Linux systems) أما المجموعة الثالثة والأخيرة هي علاقات الثقة Trust بين بيئات الاستضافة المتداخلة معا. يوضح الشكل 1 العلاقات بين تلك المجموعات الثلاث للتحديات الأمنية.

1.2 تحدي التكاملية Integration:

لأسباب تقنية وبراغماتية، لا يمكن أن نتوقع أن سياسة أمنية واحدة يمكن تعريفها وتطبيقها على جميع بيئات Grid بحيث تلبي جميع التحديات الأمنية وبحيث يمكن تطبيقها في كل بيئات الإستضافة، فالبنى التحتية الحالية للأمن لا يمكن تبديلها بين ليلة وضحاها، على سبيل المثال لكل نطاق ضمن بيئات Grid مجموعة من القواعد المتعلقة بالتسجيل وتخزين أسماء المستخدمين مثل فهارس LDAP مثلا، وهذه الفهارس قد تكون غير قابلة للمشاركة مع نطاقات ومنظمات أخرى، وبشكل عام إن آليات التحقق المطبقة في البيئات الحالية والتي هي موثوقة ومحترمة سيبقى استخدامها على الدوام .إذا لكل نطاق Domain بنيتة التحتية الخاصة به لتنفيذ التحقق authorization والتي تديره وتنفذه على أكمل وجه .

يجب على هيكلية الأمن ضمن بيئة GRID أن تحقق التكاملية مع انظمة الأمن الحالية نماذجها المختلفة عبر المنصات المتعددة وبيئات الاستضافة المختلفة وهذا يعني أن الهيكلية يجب أن تحقق بحيث تتوافق مع الأنظمة الأمنية الموجودة مسبقا مثل أليات Kerberos،(PKI); وبحيث تتكامل أيضا مع الخدمات الأمنية الجديدة التي يمكن أن تحدث وهكذا تتكامل أيضا مع الخدمات الأمنية الموجودة مسبقاً.

2.2 تحدي التبادلية Interoperability:

إحدى التحديات الهامة هوأن الخدمات التي ستنتقل وتجتاز عدة نطاقات وبيئات استضافة متعددة تحتاج أن تتفاعل مع بعضها البعض وهكذا علينا تحقيق تحدي التبادلية interoperability على عدة مستويات:

- **مستوى البروتوكول protocol level :** نحتاج لأليات تحقق لنا امكانية التواصل ونقل الرسائل بين النطاقات المختلفة ويمكن أن نحقق ذلك باستخدام SOAP/HTTP مثلا.

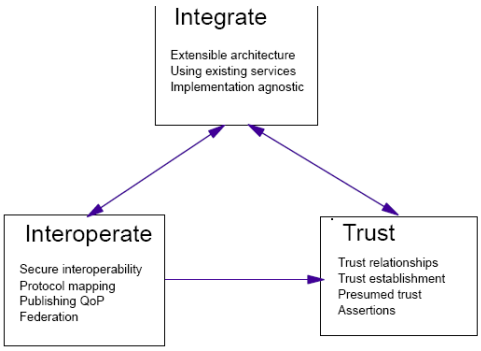
- **مستوى السياسة policy level :** يجب أن تتحق التبادلية بشكل آمن بحيث يعرف كل قسم سياسته الأمنية الخاصة به ومن ثم يتم تعريف السياية الأمنية بكل الأقسام معا ويشمل ذلك الاتصالات الأمنة والتحقق وعلاقات الثقة بين الأقسام المختلفة.
- **مستوى الهوية identity level :** نحتاج لأليات عدة لتعريف مستخدم وتمييزه من نطاق لأخر ويتم ذلك لكي نحقق علاقات الثقة بين النطاقات المختلفة، ويتم تحقق التأكد من الهوية على عدة مستويات فإما يكون معتمدا على المجموعاتgroup-based أوعلى القواعد role-based أوالميزاتattribute-based ، وسيكون من الجيد أن يتم تعريف الهوية مسبقا خلال النطاقات المتشاركة معا .

3.2 تحدي علاقة الثقة Trust Relationship:

يمكن أن تشمل خدمات Grid نطاقات عديدة، ولهذا علينا بناء علاقات الثقة Trust بين هذه النطاقات، ونقصد بعلاقات الثقة أن يكون الوصول آمنا للمعطيات ضمن النطاقات التي نود الوصول لها، ويتعلق بناء علاقات الثقة حسب طبيعة طبولوجيا الشبكة (..VPN)، إن تنفيذ علاقات ثقة متكاملة أمر ليس بالسهل في نتيجة الطبيعة الديناميكية للمنظمات الافتراضية VO والعلاقات بينها، وخاصة أن تلك المنظمات المختلفة يمكن أن تمتلك تقنيات أمنية وتقنيات تشفير مختلفة فيما بينها وهكذا علينا تحقيق التوافقية بين تلك الأنظمة الأمنية المختلفة.

تشكل قضية تحقيق الثقة Trust مشكلة كبيرة حيث تبرز الحاجة إلى الحاجة لخدمات ديناميكية، متحكمة من قبل المستخدم، بالاضافة لادراة الخدمات العابرة transient services حيث يقوم العديد من المستخدمين بتنفيذ خدمات عابرة لتنفيذ مهام محددة مؤقتة، لنأخذ حالة وجود نظام تنقيب عن المعطيات Data Mining على سبيل المثال، يمكن أن يتم إنشاء خدمات عابرة في عدة مواضع وذلك لاستخراج المعلومات من قواعد البيانات البعيدة وتجميع خلاصة المعلومات .تشمل التحديات المرتبطة بخدمات المستخدم العابرة ما يلي:

- **Identity and authorization: يجب** التحكم بالترخيص والتعريف التي سيتم تنفيذ الخدمات العابرة وفقها.
- **Policy enforcement:** يجب تحقيق سياسات دقيقة بحيث يكون لكل مستخدم سيايته الخاصة به فيحدد على سبيل المثال من يستطيع الحصول على المعلومات Access وما هي الأخداث Actionالتي يمكن تنفيذها.
- **Delegation:** يعتبرالتفويض أحد الأمور الهامة في الخدمات العابرة حيث يتطلب الأمر بعض الخدمات أن تعمل طوال الليل على الجهاز عن بعد، وتحتاج الوصول لعدة موارد، فهي تحتاج الحصول على تفويض من المالك الاصلي للوصول لهذه الموارد، ويمكن ملاحظة هذا الأمر في البرامج . يمكن تصنيف التحديات الأمنية الخاصة ببيئة GRID بالشكل التالي:



الشكل 1 – يوضح العلاقة بين حلول التحديات الثلاث

3. متطلبات تحقيق أمن بيئة Grid :

بعد أن استعرضنا التحديات الأمنية الثلاث، سنقوم بمناقشة المتطلبات اللازمة لتحقيق الأمن في بيئة Grid .يجب أن يعرف نموذج الأمن الخاص ب OGSA المبادئ الأمنية التالية:

1.3 التحقق من الهوية Authentication:

تأمين آلية للتحقق من هوية المستخدم المستخدم لخدمات بيئة Grid وتتنوع آليات التحقق من آليات عادية برمجية إلى آليات هاردويرية كتلك التي تعتمد على البصمة أوالحدقة.

2.3 التفويض Delegation :

يجب أن يتضمن النظام على آليات التفويض ومنح الحقوق rights من الطلبات للخدمات، وعندما نتكلم عن التفويض يجب ان يرافقه منح ترخيص authority للمهمة المطلوبة، وعلينا التأكد أن ذلك الترخيص يشمل مهام محددة دون غيرها، بالاضافة لأن تكون محددة بوقت محدد وذات نطاق ومجال محدد.

3.3 دخول مفرد Single Logon :

بعد أن يتم التحقق من الهوية والتفويض، إنه لأمر مهم أن نقوم بتنفيذ دخول مفرد لأي مورد من المعلومات بحيث نكتب سياسة توضخ عدم إمكانية

أكثر من مهمة بآن واحد لمورد ما، أوالسماح لها حسب السياسة التي نريد.

4.3 مدة حياة الإعتماديةCredential وتجديدها:

عادة ما تستغرق المهمة المطلوب إنجازها وقتا أطول من امدة التفويض التي حصلت عليه، وفي هذه الحالات على المستخدم ان يمتلك القدرة على معرفة ذلك قبل انتهاء المهلة المحددة للمهمة لكي يقوم بتجديد التفويض لها حتى يتم إنهاء المهمة بنجاح.

5.3 التخويل Authorization :

تعني بناء سياسات ترخيص وتخويل Authorization ونعني بها سيسات منح الحقوق للحصول على خدمة ما تحت شروط معينة، ويمكن تحقيق التخويل بعدة طرق بحيث يتم بالخلاصة بالتحكم بالوصول Access control.

6.3 الخصوصية Privacy :

تعني ان نسمح لمزودي الخدمات ولطالبي الخدمات أيضا بناء سياساتهم الخصوصية الخاصة بهم ونعني بالخصوصية هوما هي المعلومات التي يمكن الاطلاع عليها من قبل الآخرين وما هي المعلومات التي يجب الاحتفاظ بها.

7.3 السرية Confidentiality :

نقصد بها تحقيق الخصوصية والسرية على مستوى طبقة النقل وتشمل ذلك آليات نقل المعطيات من نقطة لأخرى.

8.3 تكامل الرسائل Message Integrity :

نعني بتكامل الرسالة أن نحافظ على الرسالة دون أي تعديل أي إذا تم تعديل الرسالة من قبل شخص غير مخول فسيقوم المستقبل بإكتشاف ذلك، تحقق هذه التكاملية ما يدعى QOS جودة الخدمة Quality Of Service .

9.3 تغيير السياسة Policy exchange :

يجب أن يكون نموذج الأمن قادرا على تغيير السياسة الأمنية بشكل ديناميكي عند الحاجة، ونقصد بالسياسة الأمنية تلك المعلومات المتعلقة بالسياسة مثل التحقق والترخيص والقيود والسماحيات والخصوصية...الخ .

10.3 الدخول الآمن Secure Logging :

يجب أن نؤمن دخولا أمنا ومشفرا للمستخدم للنظام والموارد التي يريد استخدامها، ويشمل ذلك بناء آليات المراقبة auditing والتشفير وعدم التكراروالتوثيق notarization .

11.3 التأكد Assurance :

يعني أن نقوم بتحقيق مستوى من التحقق والتأكد على مستوى الاستضافة Hosting ونقصد بذلك تقنيات الحماية من الفيروسات والجدران النارية المستخدمة للانترنت، شبكة VPN ..الخ .

12.3 قابلية الإدارة Manageability :

يجب أن يكون النظام ابلا للادارة، على سبيل المثال: Identity management ، policy management، key management تاتي الحاجة لقابلية الادارة لادارة العمليات عالية المستوى مثل اكتشاف الفيروسات، اكتشاف الاختراقات والحماية.

13.3 الجدار الناري Firewall :

لعل أحد الامور الهامة لبناء أي نموذج أمني هووجود جدار ناري .

4. مبادئ بناء نموذج أمن لبيئة Grid :

من وجهة نظر أمنية، إن جعل تعريف خدمة ما افتراضية يشمل متطلبات أمنية إضافية للولوج للخدمة. يمكن تحديد المبادئ العامة لنموذج نظام أمني خاص ببيئة Grid بالصنفين العاميين التاليين: نموذج أمني عام لجميع خدمات بيئة Grid ,الخدمات الآمنة التي تقدم الوظائف الضرورية.

1.4 الإستدعاء الآمن لخدمات Secure Grid Invocation of Grid Services :

يجب أن تتأكد هيكلية الأمن في بيئة Grid أنه يمكن استدعاء الخدمات من قبل من يطلبها وفق السياسة الأمنية الموجودة، ووفق قيودها الموجودة في بيئة الاستضافة.فسياسة ما قد تشمل نوعا محددا من المتطلبات الخصوصية والسرية والتكاملية وكل ذلك يؤدي لاستدعاء أمن وناجح للخدمات. يجب على خدمة Grid أن تكون قادرة على تعريف أونشر جودة الحماية QOP Quality of Protection .

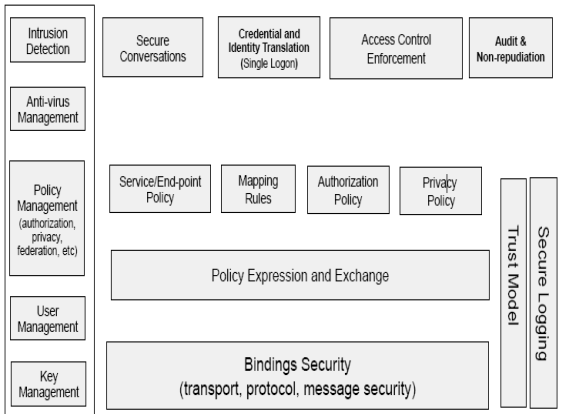
2.4 خدمات بيئة Grid الأمنية Grid Security Services:

يوجد الكثير من الخدمات الأمنية التي يوفرها نموذج خدمات OGSA، وهذه الخدمات الأمنية المتنوعة تتعلق ببيئة الاستضافة Hosting والتي يمكن تغطيتها بسياسة التحقق مثلا وتعتمد الخدمات على بيئة الاستضافة بشكل كبير.

5. النموذج المقترح لتحقيق الأمن لبيئة Grid:

أحدثت خدمات الويب web Services WS ثورة كبيرة في عالم الانترنت حيث قدمت إمكانية نقل الحلول والمعلومات بشكل متكامل ومترابط.ويشكل الأمن في خدمات الويب هاجسا لدى جميع الشركات والزبائن على حد سواء، فعلينا على سبيل المثال تحقيق الارتباط الآمن بين المنظمات الافتراضية، ولحسن الحظ تقدم خدمات ويب حلول أمنية جيدة لذلك فعلى سبيل المثال لدينا نموذج تمرير الرسائل الآمن secure messaging model الذي يقدمه مستند

خارطة الطريق للأمن في خدمات ويب Web Services Security roadmap [WSR] والذي يدعم كلا من بنية تشفير المفتاح public key infrastructure (PKI) وآليات Kerberos . يوضح الشكل التالي الذي يوضح هيكلية نموذج أمن بشكل عام.



الشكل 2 – نموذج أمني عام لشبكة GRID

يمكن التعامل والولوج لخدمات ويب باستخدام الكثير من البرتوكولات وصيغ الرسائل التي تدعمها وهي معرفة ضمن bindings [GRIDSPEC]، وهذه البرتوكولات تؤمن بالطبع جودة الخدمة والاجراءات الأمنية مثل السرية والتكاملية والتحقق من الهوية.

يعرف كل مشارك في نهاية طرفية سياسته الأمنية التي برغب بتطبيقها عند الدخول بمحادثة آمنة مع طرف آخر. نعود لنذكر أن كل سياسة أمنية تتضمن آليات التحقق والترخيص والتكاملية والسرية والثقة.ما إن يرتبط أحد طالبي الخدمة service requestor مع مزود خدمة service provider يقومان بداية كل منهما بتحديد سياسته للآخر،وبعد ذلك يقومان بإنشاء قناة آمنة لاستدعاء التوابع بشكل آمن.

1.5 أمن الارتباط Binding Security:

إن مجموعة الارتباط set of bindings تشمل SOAP (SOAP/HTTP، SOAP over a message queue or SOAP over any other protocol) and IIOP bindings . يعتمد الأمن هنا بشكل عام على الأمن الذي يقدمه البرتوكول بشكل عام، لذلك عند استخدام بروتوكول جديد أوصيفة جديدة لتمرير الرسائل علينا الانتباه للخدمات الأمنية التي يقدمها،والحد الأدنى للخدمات الأمنية الواجب تحقيقها هي التحقق والتكاملية والسرية. يجب علينا الانتباه لبرتوكول Http الذي يعتبر أحد البرتوكولات الهامة المستخدمة ويجب أن ننتبه أنه ليس برتوكولا آمنا لذلك يفضل بشدة استخدام بروتوكول SSL معه بحيث نستخدم "https" على سبيل المثال.

2.5 منهجية العمل وتغييرها Policy:

إنه لمن المهم لطالب الخدمة معرفة كيفية ارتباط السياسة مع الخدمة، أي كيف يتم تطبيق السياسة الأمنية، ما إن يتم معرفة السياسة الأمنية يتم تطبيق الآليات اللازمة لتحقيقها وتنفيذها. يجب على طالبي الخدمات service requestors ضمن بيئة Grid التعرف مباشرة على السياسات بشكل ديناميكي واتخاذ القرارات وقت التنفيذ Runtime، بعض السياسات يمكن أن ترتبط مثلا بمعرف خدمات ويب مثل WDSL على سبيل المثال. يجب ان يتضمن نموذجنا الأمني على إمكانية تعديل السياسة وتطويرها دون أن يؤثر ذلك على الأليات المستخدمة.

3.5 الارتباط الأمن Secure Association :

يجب أن يتم تبادل الرسائل بشكل آمن بين الأطراف المختلفة، عندما نتكلم عن الارتباط الآمن نتحدث عن برتوكولات أمنة جاهزة لاستخدامها مثل IPSEC)،SSL،(IIOP بالاضافة للعديد من الآليات مثل Kerberos والتي تدعم الارتباطات الآمنة .

4.5 تحقيق التحقق من الهوية Authorization :

يجب أن يتضمن النموذج الأمني على آلية واضحة للتحقق من الهوية، ويعتبر التحقق من الهوية الحجز الأساس في أي نموذج أمني، ولكل نطاق سياسته الخاصة في تحقيق التحقق من الهوية وغالبا ما يستخدم التحقق من الهوية لانجاز التحكم بالوصول المعتمد على الهوية، ويساهم التحقق من الهوية في إنجاز عملية الثقة مابين مزود الخدمات وطالبيها.

5.5 تحقيق الخصوصية Privacy Enforcement :

يعتبر عدم تسريب معلومات خاصة أحد أهم الخصائص الواجب تحقيقها في أي نموذج أمني، لذلك على كل منظمة تستخدم بيئة Grid بناء سياستها المعتمدة على الخصوصية الخاصة بها.

6.5 تحقيق الثقة Trust :

يجب على كل منظمة افتراضية VO أن تمتلك بنيتها التحتية الآمنة الخاصة بها، والتي تتضمن خدمات التحقق من الهوية authentication service، تسجيل المستخدمين user registry، محرك الترخيص authorization engine وحماية الشبكات وخدمات أمنية أخرى.لكي تتم معالجة الطلبات المختلفة بين أعضاء النطاق الواحد لا بد من بناء علاقة ثقة بينها،وهذه العلاقة ضرورية جدا في حالات وجود جدار ناري ينبغي تجاوزه مثلا، أوفي

حالة وجود نظام تحقق من الهوية مرتبط بخدمة ما، وهكاذا فإن وجود علاقة ثقة أمر ضروري جدا في أي نموذج أمني وذلك لبناء علاقات ثقة بين الأعضاء المختلفة ضمن نفس المجال domain .

7.5 تسجيل الدخول الآمن Secure Logging :

تعتبرأحد الأمور الهامة لتحقيق الأمن على مستوى عالي High level وذلك لتحقيق خدمات المراقبة auditing.

8.5 إدارة الأمن Management of Security :

يجب أن يتضمن نموذج الأمن على إدارة الأمن بحيث يتم إدارة كل الوظائف السابقة معا.

الخلاصة:

لقد انتشرت بيئة عمل Grid على مجال واسع وتم تعريف العديد من المنظمات الافتراضية VO التي تعمل ضمنها،لقد قدمنا في هذا البحث رؤية متكاملة للجانب الأمني الهام، حيث قمنا بتقديم اقتراح متكامل لتنفيذ نموذج أمني لبيئة Grid .

المراجع

[ANA] **The Anatomy of the Grid: Enabling Scalable Virtual Organizations**. I Foster،C. Kesselman،S. Tuecke. *International J. Supercomputer Applications*،15(3),2001.

[PSY] **The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration**. I. Foster،C. Kesselman،J. Nick،S. Tuecke;January،2002.

[COMP] **A Security Architecture for Computational Grids**. I. Foster،C. Kesselman،G. Tsudik، S. Tuecke. *Proc. 5th ACM Conference on Computer and Communications Security Conference*،pp. 83-92،1998>.

[NEUMAN] Lai،C.،Medvinsky،G. and Neuman،B.C. Endorsements ،Licensing ،and Insurance for Distributed System Services. in *Proc. 2nd ACM Conference on Computer and Communication Security*،1994.

[WSR] **Security in a Web Services World: A Proposed Architecture and Roadmap**،http://www-6.ibm.com/ developerworks /library /ws-secmap/

[SSL] **The SSL Protocol Version 3.0**. http://home.netscape.com/eng/ssl3/draft302.txt.

[TLS] RFC 2246: **The TLS Protocol**. ftp://ftp.isi.edu/in-notes/rfc2246.txt.

[CORBA] **The Common Object Request Broker: Architecture and Specification،Version 2.3.1.** The Object management Group (OMG), http://www.omg.org/cgi-bin/doc?formal/99-10-07.

[CSI] **Common Secure Interoperability Version 2 Final Available Specification.** The Object Management Group (OMG), http://www.omg.org/cgi-bin/doc?ptc/2001-06-17.

[J2EE] **Java 2 Platform،Enterprise Edition،v1.3 (J2EE)**. http://java.sun.com/j2ee.

[P3P] **The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, W3C Recommendation** 16 April 2002،http://www.w3.org/TR/P3P/

[GRIDSPEC] **Grid Service Specification**. S. Tuecke،K. Czajkowski،I. Foster،J. Frey،S. Graham،C. Kesselman; Draft 2،6/13/2002،http://www.globus.org

[SOAP] **Simple Object Access Protocol** (SOAP) 1.1, W3C, 2000.

Czajkowski, K., Foster, I., Kesselman, C., Sander, V. and Tuecke, S., SNAP: A **Protocol for Negotiating Service Level Agreements and Coordinating Resource Management in Distributed Systems**. 8th Workshop on Job Scheduling Strategies for Parallel Processing, 2002.

IBM, Microsoft, RSA Security and VeriSign. Web Services Secure Conversation Language (WS-SecureConversation)Version 1.0, 2002.