GRID (ŞEBEKE) AĞLARDAKİ RİSKLER VE DAĞITIK ERİŞİM DENETİMİ

***Tuncay Ercan, Murat Koyuncu, *Esma Ergüner Özkoç**
*Yaşar Üniversitesi, Mühendislik-Mimarlık Fakültesi, İzmir
Atılım Üniversitesi, Mühendislik Fakültesi, Ankara
tuncay.ercan@yasar.edu.tr; mkoyuncu@atilim.edu.tr; esma.erguner@yasar.edu.tr

ABSTRACT

Grid Networks have a very popular interest in many distributed applications from the point of academic view. They enable large scale resource sharing between authorized users and facilities. The dynamic and complex nature of grid systems challenge significant security issues that require new technical approaches. This paper reviews and recommends a framework for utilising different access control technologies to pro-actively monitor for security threats impacting network and available grid applications. Network access is controlled between the grid users and the Internet. The organizational access control policy is specified for the remote business partners and required devices are determined to implement this policy. This study addresses both generic and application specific access control mechanisms to ensure the security issues in Grids and can be used as guidance by the developers.

Key words: Grid networks, distributed applications, access control, security threats.

1. GİRİŞ

Bilgi paylaşımının öneminin artması, işlenecek bilgilerin karmaşıklığı gibi teknoloji ile birlikte gelen yeni hususlar, çok büyük kapasiteli süper bilgisayarların yapılmasına sebep olmuştur. Ancak çok pahalı olan bu sistemlerin yerine, birbirine bağlı binlerce bilgisayarın yatay genişleme dediğimiz bir usulle birbirine bağlanarak sahip oldukları yüksek kapasiteli işlemci yeteneklerini kullanabilmesi "grid" (şebeke) ağlar dediğimiz ayrık bilgisayar ağlarına ve uygulamalarına doğru gidişi hızlandırmıştır.

Grid ağlar bütün dünyada farklı kurumlar tarafından sunulan özel ve ayrık bilgisayar kaynaklarının ortak paylaşılabilen bir zemine taşındığı teknolojilerdir. Sisteme dahil olan bütün birimlerin kendi ortamlarında bulundurdukları uygulamaları paylaşıma açmayı hedefler. Büyük bir geniş alan ağına yayılmış olan böyle bir hizmette alınacak güvenlik tedbirleri son derece önemlidir [1].

Bütün Grid ağ içinde standartlaştırılmış olan güvenlikle ilgili esaslara dikkat etmeksizin yapılacak bir uygulama, hem kullanıcılar için hem de sistem yöneticileri için büyük emniyet problemleri yaratabilir. Bu yüzden planlama ve deneme aşamalarından itibaren sistemin bütün parçalarında uygulanacak olan güvenlik standartları için zorunlu politikalar belirlenmelidir [2].

Bu çalışmada halihazırda Grid ağlarda güvenlik problemi olarak belirlenen hususlar hakkında bilgiler verilmiş, kullanılabilecek donanım ve yazılım ürünleri incelenmiştir. Grid ağ sistemi içinde yer alan organizasyonların herbirinde standart bir güvenlik politikası oluşturulması esas alınarak, geliştirilmiş olan teknolojilerin muhtemel kullanım usulleri araştırılmıştır. Sadece ağ içindeki kullanıcılar için değil, dışarıdan sistem kaynaklarını kullanacak kişilere de ortak bir dağıtık erişim kontrolu sağlanması için gerekli hususlar açıklanmıştır.

Bu bildiri altı bölümden oluşmuştur. Grid ağların güvenlik hassasiyetlerine ilişkin açıklamalar ve bu konuda yapılan çalışmalar ikinci bölümde verilmiştir. Üçüncü bölümde standart ağlar üzerindeki güvenlik ve riskler hakkında bilgi verilirken, dördüncü bölüm Grid ağların güvenlik gereksinimlerini açıklamaktadır. Beşinci bölümde dağıtık erişim kontrolune ait farklı uygulamalar açıklanmış, son bölümde çalışmayla ilgili sonuçlar verilmiştir.

2. ÖNCEKİ ÇALIŞMALAR

Grid ağlardaki paylaşımda olan kaynaklara güvenli erişimin ilk dayanağı kurulum aşamasında artık standart hale gelen "Globus" gibi altyapı yazılımlarının kullanılmasıdır [3,10]. Bu yazılımlar, kullanıcıların kaynağın yeri ve sahibine bakmaksızın en uygun uygulamaları bulup çalıştırmasını sağlar.

Örnek ağlardan birisi ve Türkiye'ye yakın olanı hala çalışmaları sürdürülen EGEE (Enabling Grids for Escience in Europe)'dir (Şekil 1).

Şekil 1. EGEE Grid Kapsamı

Bilimsel araştırmaları destekleyen 27 ülkeden 70 lider kuruluşu kapsayan, üretim yönetim merkezi İsviçre'de bulunan, bu en büyük uluslararası Grid altyapısı akademik araştırmacılara, coğrafi konumlarından bağımsız olarak temel hesaplama kaynaklarına 24 saat erişim sağlar [4].

Grid ortamında bir uygulama geliştirmek veya kullanmak isteyen, fakat güvenlik konusunda nereden başlayacağını bilemeyenler için Humphrey ve Thompson tarafından farklı uygulamaları içerecek şekilde örnek birçok senaryo çalışması yapılmıştır [5]. Bu çalışmaların amacı grid uygulamalarının planlandıkları ilk andan itibaren güvenli bir şekilde kullanılabilirliklerinin sağlanmasıydı.

Stoker [6] ve Grid Forum tarafından ağ içindeki sistem kaynaklarına ait işletme yetkisinin kuralları belirlenen politikalara göre verilmesi istenmiş, farklı uygulamalara göre değişen kullanıcı sayısının etkin kontrolunun önemi açıklanmıştır. Erişim izinlerinin süreye veya sadece uygulamayı tekrar çalıştırma sayısına bağlı olması gerekliliği belirtilmiştir.

Bugünkü Grid projelerinin büyük kısmında uygulanmakta olan güvenlik tedbirleri hemen hemen aynıdır. Bu konuda standart haline gelmiş olan AAARP (Authorization Accounting Architecture Research Group) tarafından yayınlanmış olan RFC'ler (Request for Comments) önemli kaynaklardır [8,9].

Grid güvenliği konusunda alınabilecek tedbirlerle ilgili olarak mimari yapıda olması gereken yazılım ve donanım gereksinimleri [10]'da açıklanmıştır.

Grid ağlara yapılabilecek saldırılar sadece tek tip kullanıcı ve erişim temelli saldırılar ile sınırlı kalmaz. Protokol yapısındaki açıklardan faydalanarak farklı bölgelerdeki birçok sunucuya işlevsel uygulamalar gönderilerek sistem tıkanabilir. Bu amaçla gerçek zamanlı ve gerçek zamanlı olmayan saldırı tespit sistemleri kullanılarak güvenlik amaçlı analizler yapılır [11].

Grid ağlardaki geniş ve dinamik kullanıcı kitlesi ve bunların farklı sitelere erişim yolları için gereken yetkilendirme için sayısal sertifikalar geliştirilmiştir. EGEE içinde de kullanılan bu sertifikaların etkin kontrolu için yetkili bir otorite vardır. Uluslararası bir sistemde milli otoriteler tarafından bu hizmet sağlanır [12].

3. GÜVENLİK VE RİSKLER

Kullanılan ağın yapısı ne olursa olsun güvenlikle ilgili temel esasları yerine getirebilmek için güvenlikten sorumlu bir birim tarafından ağın sürekli kontrol edilmesi ve izlenmesi gereklidir. Ağı daha emniyetli duruma getirmek için, ağda mevcut hassasiyetleri anlamak ve bunların nasıl aşılabileceğini bilmek önemlidir.

Aynı güvenlik felsefesi aynı şekilde ağın iletişim altyapısına da uygulanmalıdır. Özellikle Grid ağlar gibi birbirlerinden uzakta bulunan organizasyonlardan oluşturulan geniş alan ağlarında alınacak tedbirler gerçekte yerel ağlarda alınacak tedbirlerle aynı olacaktır. Tek fark yetki dahilinde olan yerel ağ ile beraber ağ dışındaki iletişim sistemlerinin de kontrolunun sağlanmasıdır.

Ağ altyapısının güvenliğini düzenlerken, ağdaki sistemlerin birbirleriyle nasıl iletişim kurduklarını anlamak çok önemlidir. İletişim sistemlerine yapılacak yetkisiz bir girişim sisteme ait temel özellikleri bozabilir. Güvenlik sorumluları eğer bu iletişim özelliklerini biliyor ve ortaya çıkan değişiklikleri farkedebiliyorsa, bu durumu önlemek için gereken tedbirleri alabilir [13].

Bilgiye kolay ulaşım için sunulan hizmetler (servisler, http, ftp, vs) aynı zamanda zarar verme riski de taşımaktadır. Bilgisayar ağlarının sunduğu bütün olanaklardan faydalanmak, fakat gelebilecek zararları en aza indirmek gerekir. Alınacak tedbirlerle güvenlik öne çıkarılırken, ağ hızının azalması kabul edilemez.

Ağ güvenliğindeki gelişmeler ile özellikle saldırı tespit sistemleri (intrusion detection systems) ve zayıflık inceleme araçları (vulnerability assessment tools) giderek önem kazanan diğer bilişim güvenliği uygulamaları olup, güvenlik çözüm paketinin oluşturulması esnasında dikkatle değerlendirilmesi gereken bileşenlerdir.

Grid siteleri farklı kuruluşlar tarafından yönetilmektedir. Siteler kendi hesaplama kaynaklarının nasıl kullanıldığı konusunda son kontrol hakkına sahiptir. Grid faaliyetlerinin

yaklaşık %24'ünü kapsayan orta katman kurulumu faaliyetleri, kalite güvencesini, güvenlik ve ağ hizmetlerini, bunların geliştirilmesini kapsar [14].

Grid ağlarda güvenlikle ilgili olarak düşünülmesi gereken nokta, ağda paylaşımda olan hassas bilgilerin farklı ağlar arasında nasıl kullanıldığını bilmek gerekliliğidir. Dolayısıyla böyle bir bilgi kaynağı kendi yerel sahibi tarafından en iyi şekilde korunabilecekken uzaktan erişim sağlayan ağ kullanıcılarının herhangi bir hatalı kullanımı sonucu yetkisiz kişilerin eline geçebilir.

Bu yüzden bütün Grid ağ üzerindeki hizmet çeşitlerini çok iyi analiz etmek gereklidir. Genelde ihmal edilen bir elektronik posta hizmetinde bile çok sayıda hassas bilgi yanlış şekilde kullanıcılar arasında yer değiştiriyor olabilir. Hemen hemen bütün posta hizmetlerinin düz metin olduğu düşünülürse konunun önemi ve devamlı olarak izlenmesi gerekliliği ortaya çıkar.

Ağa yetkisiz olarak giren bir kişinin varlığı ağ mevcudu fazla değilken kolaylıkla anlaşılabilir. Ancak bu sayı birkaç bin kullanıcıya çıktığında saldırganın bulunması güçleşir. Ağ yöneticisi olan kişilerin ağa erişim için fiziksel kontrol sağlamaları diye bir güvenlik sistemi oluşturmaları mümkün değildir.

Eğer bir saldırgan ağı gözlemek istiyorsa, yapacağı işlem büyük bir ihtimalle en çok bilgiyi toplayacağını düşündüğü merkezdeki birimlere erişim sağlamak olacaktır. Böyle bir durumda yetkisiz erişimin imkan verdiği kablolama dolapları ve sistem sunucu odaları temel hedefler ve sonrada ulaşılacak olan diğer iletişim imkanları için merkez olacaktır.

4. GRİD GEREKSİNİMLERİ

Grid sistemdeki bütün kullanıcıların ihtiyaç duydukları uygulamaları gerçekleştirebilmeleri için hem yerel hem de bütün Grid sistemi içinde kendilerine ait kimliklerinin doğrulanması gereklidir. Kaynakların dinamik olarak değiştiğini varsayarsak her yeni kaynak için en azından bu kaynağa ihtiyaç duyacak, ilgili uygulamayı çalıştıracak kullanıcılar için bir giriş hakkı verilmelidir.

Bazı kaynaklar sadece yerel kullanıcıların erişimine izin veriyorsa, grid sistemden gelen diğer kullanıcılar için de birer yerel kimlik ataması yapılabilmelidir.

Sisteme dahil olan bütün organizasyonlar kendi kaynaklarının yanlış veya hatalı kullanımı üzerine uygulayacakları yaptırımları daha önceden belirlemiş olmalıdırlar. Erişim kontrolu sağlayan kişisel sertifikaların iptal edilmesi durumunda o yerel ağ içindeki kaynaklara erişim gerçekleşmeyecektir [15].

Ağ güvenliği ile ilgili teknolojilere bakıldığında, bu alanda en yaygın uygulaması bulunan teknolojinin güvenlik duvarları (firewall) olduğunu öne sürmek doğru olacaktır. Temel olarak bir güvenlik duvarı, bir ya da daha fazla ağ arasına yerleştirilen ve bu ağlar arasında belirlenen bir politika çerçevesinde izolasyon sağlayarak onları birbirinden yalıtan bir ağ bileşenidir [16]. Güvenlik duvarları, yaygın kanaatin aksine, Grid ağlar için tek başlarına eksiksiz bir güvenlik çözümü oluşturamamaktadır. Mevcut güvenlik duvarlarının hızları 1-10 Gb/s civarındadır ve bu değer grid ağların çok büyük bant genişliği ihtiyacını karşılamaktan çok uzaktır.

Grid ağlar içindeki super bilgisayarlar veya uygulamalarda kullanılan özel sistemler birbirlerine atanmış ve karşılıklı güven duyma (trust relationship) prensibine göre bağlanırlar. Böyle bir durum da sistem içindeki kullanıcıların sebep olabileceği güvenlik açıklarını ortaya çıkarır [14].

Yalnızca kaynak ve hedef bilgilerine bakarak seçici geçirgenlik gösteren "paket filtreleme" güvenlik duvarı uygulamalarının yanlış kullanımlarıdır. İnternet'e açık web hizmeti veren bir sistemi korumak üzere kurulan bir "paket filtreleyen güvenlik duvarı sistemi" kaçınılmaz olarak bu sisteme doğru gelen tüm web istemlerini geçirmek zorundadır; böylece saldırganların web üzerinden yapabilecekleri saldırılar için herhangi bir koruma sağlanamamaktadır.

Güvenlik duvarlarına ilave olarak yüksek performanslı fiziksel mantıksal (logical) iletişim kanalları (fiber, dalgaboyu-wavelength, VPN-Virtual Private Network- gibi) kullanılabilir. Bu sistemlerin ortak özelliği sistem dışından kullanımlarının mümkün olmamasıdır.

Grid sistemin kapsadığı donanım ve yazılım ürünleri ile mevcut bütün kurumsal ağların durumu hakkındaki güncel bir bilgi sistemi yapılabilecek kötü maksatlı girişimleri belirlemekte faydalı olacaktır [18,19]. Sistemin ortak kaynakları hakkındaki yanlış veya yetersiz bilgiler hatalı kararlar alınmasına sebep olabilir. "Globus Toolkit" yazılımı ile grid ağların kurulumdan işletmeye kadar olan potansiyel problemleri bir ölçüde çözülmüştür. Bu yazılımın sisteme üye bütün organizasyonlar tarafından etkin olarak kullanımı, herkes tarafından kabul edilen güvenlik donanımlarına ilişkin hususların (açık portlar, protokollar, uygulamalar) önceden doğru olarak belirlenmesine bağlıdır [10].

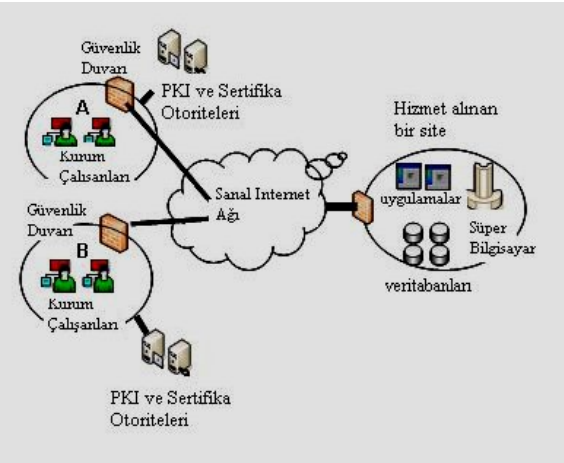
Verinin son derece önemli olduğu grid ağlarda büyük risk taşıyan gizlilikle ilgili güvenlik üzerinde durulmalıdır. Bir çok kişi ya da kuruluş için gizli bilgiler bilgisayar üzerinde tutulur. Bu bilgisayarların güvenliği en iyi şekilde bazı kurumlarda olduğu gibi internet bağlantısı kopartılarak sağlanmaktadır. Ancak bu durumda da kolay ulaşılabilirlik ortadan kalkmış olur. Bu yüzden grid ağ bünyesinde ortak olacak şekilde güvenlik politikaları belirlenmelidir.

Ağ bütünü için toplu olarak değerlendirilen bir yetkilendirme veya hatalı davranışlarda uygulanacak politikalara getirilebilecek esneklik ve kapsam farklılıkları grid ağlarda karar verilmesi gereken ortak faktördür [20].

Erişim haklarının uygun olarak düzenlenmesi için organizasyonların büyük bir kısmı kullanıcı ismi ve parolaya dayanan LDAP (Lightweight directory Access protocol) kullanır. LDAP sadece genel anahtarları değil, aynı zamanda erişim hakları gibi farklı şekillerdeki ağ bilgilerinin kaydını yapıp dağıtan bir protokoldür [21].

5. DAĞITIK ERİŞİM DENETİMİ

İyi işleyen bir grid ağ içinde sunulan hizmetlerin durumunu ve mevcudiyetini tespit etme kabiliyeti son derece önemlidir [19]. Ağ içindeki herhangi bir organizasyondan, herhangi bir kullanıcı tarafından yapılan istek hizmet verecek ağdaki bilgi sistemleri merkezinde, istekte bulunulan uygulamanın gerektirdiği erişim kontrol politikasına göre değerlendirilir (Şekil 2).



Şekil 2. Grid Ağı Bileşenleri

Geleneksel erişim kontrolu ağ üzerinde bulunan bir erişim kontrol sunucusunda erişim kontrol listeleri (ACLs) tutularak sağlanmaktadır. Bu sunucular ağa kimlerin erişebileceğini ve hangi servislerin kullanılabileceğini belirler. Her kullanıcı için ayrı bir yetki değeri saklayan bu sunucular kullanıcılara sadece tanımlanmış yerlere giriş izni verirler. Ağ kullanıcılarının dinamik olarak değiştiği varsayılırsa bütün erişim kontrol işlemlerinde otomatik güncellemeler önem kazanır.

Ağ güvenliğiyle ilgili olarak güvenlik duvarlarının (firewall) kullanımıyla ilgili verilecek ilk karar ağ içi ve dışı veri trafiğini yönetmek için gereken prensiplerin neler olacağını belirlemektir [17,18,19]. Bunun sonucunda ağ erişim kontrol politikası belirlenir. Erişim kontrolu kurumsal özelikler içermelidir. Erişim kontrol politikası grid ağın farklı organizasyonlarındaki dahili ağların farklı alanlarına uygulanabilir. Bu durumda erişim kapsamı yalnız belirli maksatlı kullanımlar için belirlenebilir. Böyle bir erişim politikası ağın farklı parçalarından gelen ve giden veri akış istikametlerini belirler Ayrıca diğer bütün veri cinslerinin engelleneceğini ifade eder.

Ağ adres dönüşümü (NAT-Network Address Translation) genel olarak bir güvenlik tedbiri olmamakla beraber, özel ağları yeni bir ağ adres grubu kullanarak İnternet'e bağlamak için kullanılan bir tekniktir. Kapı adres dönüşümü (PAT-Port Address Translation) bu tekniğin imkanlarını arttırır[22].

Sanal kurumsal bağlantılar (VPN-Virtual Private Networks) grid ağ içindeki farklı organizasyonların birbirleriyle olan iletişimlerinde kullandıkları ve karşılıklı olarak yetkilendirilmiş, güvenli erişim sağlayan bir iletişim teknolojisidir [23,24]. Bu sistemde güvenlik için gereken teknolojiler, grid ağlar için süper bilgisayarlarda veya başka sistemlerdeki özel uygulamaları çalıştırmak için kullanılabilecek CAs (Certificate Authorities) ve PKI (Public Key Infrastructure)'dır [23]. Bu anahtar ve sertifikalar organizasyon içinde veya dışında yetkilendirilmiş, kullanıcılara ait güvenlik anahtarlarını tek elden kontrol ve koordine eden, güvenilir birimler tarafından değerlendirilir. Bu birimler, ağ içindeki kullanıcı ve sistemlerin kimliğini belirlemek üzere sertifikalar yayınlar ve bu sertifikaların başka kullanıcılar tarafından doğrulanmasını sağlamak üzere yayınladığı sertifikaları sayısal olarak imzalar [25].

6. SONUÇLAR

Bilgisayar sistemlerini ve ağ teknolojilerini korumak için kullanılan güvenlik çözümlerinin büyük bir bölümü gerçek hayatta sıkça kullanılan farklı güvenlik çözümlerine paralellik göstermektedir. Ancak Grid ağlar gibi özel kullanımlı ve çok büyük ölçekli ortamlarda kullanılacak olan güvenlikle ilgili donanım ve yazılım ürünlerinin paylaşımdaki uygulamalara göre

dinamik olarak değişen özel geçiş kapılarına (ports) sahip olması gereklidir. Erişim kontrolu için yüksek performanslı yeni cihazlar geliştirilmelidir. Temel olarak Grid ağ politikasında belirlenebilecek güvenlik ile ilgili hususlar şu şekilde düzenlenebilir:

- Grid sistemlerinin her biri Internetten gelebilecek saldırılara karşı standart grid politikasına uygun olarak korunmalıdır.
- Internetin hatalı kullanımı güvenlik duvarlarıyla engellenmeli, hatalı bir uygulama erişim kontrolu ile anında sonlandırılmalıdır.
- Güvenlik duvarları yüksek performanslı ve gerekirse yük paylaşımlı olmalıdır.
- Çalıştırılacak uygulamalar için "net to trust" birimler birbirine güvenmelidir.
- Kullanıcı yetkilendirmeleri için ortak bir CA birimi seçilip, sertifikalar buradan yönlendirilmelidir.
- Ağa eklenecek her yeni birim için mevcut güvenlik tedbirleri aynen uygulanmalı ve erişim listeleri için otomatik bir sistem gerçekleştirilmelidir.

KAYNAKLAR

[1] Sarbjee, S., Seema, B., "Design of a Framework for Handling Security Issues in Grids", Information Technology, ICIT 06. 9th International Conference,, pp.178-179, Dec. 2006.

[2] Ferrari, A., Knabe, F., Humphrey,M. et a1., "A Flexible Security System for Metacomputing Environments", Proc. High Performance Computing and Networking, Amsterdam, April 1999.

[3] S. Andreozzi, N. De Bortoli, S. Fantinel, A. Ghiselli, G. Tortone, and V. Cristina. Gridice: a monitoring service for the grid. In Third Cracow Grid Workshop, Cracow, Poland, October 2003.

[4] Gagliardi, F., "EGEE projesine giriş", Enabling Grids for E-science in Europe, CERN, Geneva, 2004.

[5] Humphrey, M., Thompson, M.R., "Security Implications of Typical Grid Computing Usage Scenarios", Grid Forum 4, Seattle, July 2000.

[6] Stoker, G., White, B., Stackpole, E., et a1, "Toward Realizable Restricted Delegation in Computational Grids", In Proceedings of the International Conference on High Performance Computing and Networking Europe, Amsterdam, Netherlands, June 2001.

[7] Grid Forum, http://www.gridforum.org.,2008

[8] Farrell, S., Vollbrecht, J., Calhoun, P., et a1, "AAA Authorization Requirements. RFC 2906", Informational, work-in-progress, August 2000.

[9] Vollbrecht, J, Calhoun, P., Farrell, S., et a1, "AAA Authorization Application Examples. RFC 2905", Informational, work-in-progress, August 2000.

[10] The Globus Toolkit 4.0 Documentation. GT Information Services: Monitoring & Discovery System (MDS). http://www.globus.org/ toolkit/mds/., 2008.

[11] Erol, M., "Saldırı Tespit Sistemlerinde İstatistiksel Anormallik Belirleme Kullanımı", Ağ Güvenliği, 2005.

[12] Zengin, A., Temizsoylu, O., "gLite Grid Servisleri ve Güvenlik", ULAKBİM, TR-Grid Kullanıcı Eğitimi, http://www.grid.org.tr, 2007.

[13] Chivers, H., "Grid Security: Problems and Potential Solutions", University of York,UK, 2003.

[14] Chakrabarti, A., "Grid Computing Security", Springer Berlin Heidelberg, pp.159-161, 2007.

[15] Nataraj Nagaratnam, Janson,P., Dayka, J., et al., "The Security Architecture for Open Grid Services", 2002.

[16] Niederberger, R., Allcock, W., Gommans, L., "Firewall Issues FI-RG", Open Grid Forum, 2006.

[17] Milani, M., Brown, J.S., "Some Security Considerations for Service Grids", 2002.

[18] Welch, V., "Globus Toolkit Firewall Requirements, Version 9, http://www.globus. org/, 2006.

[19] D-Grid, "Design and deployment of firewall concepts within grid environments, Performance and dynamic configuration", http://www.d-grid.de, 2007.

[20] Foster, I., Kesselman, C., Tsudik, G., and Tuecke, S., "A Security Architecture for Computational Grids", 5th ACM Conference on Computer and Communications Security, pp. 83-92, 1998.

[21] Cambazoğlu, T., "VPN'de Doğrulama ve Sertifikalar", http://www.bilisimrehber.com.tr /arastirma/tr_arastirma_vpn_dogrulama_1.phtm l, 2003.

[22] Eric Knipp, E., Browne,B., Weaver, W. et a1., "Network Address Translation/Port Address Translation", Managing Cisco Network Security (Second Edition), pp.233-272, 2002.

[23] Rowan, T., "VPN technology: IPSEC vs SSL", Network Security, Volume 2007, Issue 12, pp.13-17, December 2007.

[24] Foster, I., Kesselman, C., Tuecke, S., "The Anatomy of the Grid: Enabling Scalable Virtual Organizations", International Journal of Supercomputer Applications, No:15**,** 2001.

[25] Rana, O., Hilton, J.,"Securing the virtual organization, Part 2 – Grid computing in action", Network Security, Volume 2006, Issue 5, pp.6-10, May 2006.