Uzaktan Eğitimde Güvenlik Uygulamaları

Ali Hakan IŞIK[1], İmral IŞIK[2], İnan GÜLER[3]

Elektronik Bilgisayar Eğitimi Bölümü, Teknik Eğitim Fakültesi, Gazi Üniversitesi, Ankara, Türkiye
ahakan@gazi.edu.tr imral@gazi.edu.tr iguler@gazi.edu.tr

Özet— Eğitim alacak bireylerin farklılıkları, özellikleri ve sayısı ile birlikte mekândan ve zamandan bağımsız eğitim ihtiyacının ortaya çıkması eğitimde yeni teknolojik yöntemler kullanmayı kaçınılmaz hale getirmiştir. Birçok kurum, firma ve üniversite Web tabanlı uzaktan eğitimi kullanarak bu ihtiyacı karşılamaya çalışmaktadır. Uzaktan eğitimin önemi arttıkça bu alandaki uygulamaların güvenliğini sağlamak önemli bir çalışma alanı haline gelmiştir. Çalışmada Gazi Üniversitesi Bilişim Enstitüsü bünyesinde yürütülmekte olan uzaktan eğitim sistemi güvenlik uygulamaları hakkında ayrıntılı bilgi verilmiştir.

Anahtar kelimeler— Uzaktan Eğitim, Güvenlik

Security Applications in Distance Learning

Abstract— With the emergence of individual differences, characteristics and the increase in the number of individuals who will receive education and the need for flexible education independent of time and place, the use of new technological methods have become inevitable. Many institutions, corporations and universities have started to use web-based distance learning for this purpose. As the importance of distance education has increased, provision of security applications in the field has become an important issue. In this study, detailed information has been given about security application of the learning management system which is run by Gazi University the Institute of Informatics.

Keywords— Distance Learning, Security

1. GİRİŞ

Uzaktan eğitim, geleneksel eğitim yöntemlerindeki kısıtlamalar, eğitim alacak bireylerin özellikleri, farklılıkları ve sayılarının artmasıyla ortaya çıkmış, eğitim materyallerinin zamandan ve mekândan bağımsız olarak iletişim teknolojileri aracılığıyla bir araya getirildiği bir eğitim faaliyetidir. Uzaktan eğitim, 1900'lü yılların ilk yarısında mektupla öğretim ile başlamış daha sonra radyo, teyp gibi araçlarla desteklenmiştir. İlk resmi uzaktan eğitim merkezi 1939 yılında Fransa'da kurulmuştur. Bu ve benzeri kurumlar eğitim faaliyetlerini telekonferans ile geliştirmiş ve günümüzdeki bilgisayar teknolojileri destekli web tabanlı uzaktan eğitim başlamıştır. Senkron ve asenkron olarak yürütülmekte olan uzaktan eğitimin çok yakın gelecekte görsel ve işitsel tüm teknolojik gelişmeleri içerecek şekilde üç boyutlu uygulamaların da yer aldığı bir eğitim ortamına dönüşeceği konusunda çalışmalar yapılmaktadır [1].

Bilgisayar destekli sistemlerde güvenliğin amacı herhangi bir sistemi yetkisiz kullanıcılardan korumak, erişimlerini engellemektir.

Bu çalışmada Gazi Üniversitesi Bilişim Enstitüsü bünyesinde yürütülmekte olan internet teknolojileri destekli uzaktan eğitim programlarının donanım, yazılım, eğitim yönetim sistemi yazılımı, ölçme ve değerlendirme sınavında yapılmakta olan güvenlik uygulamaları hakkında ayrıntılı bilgi verilmiştir ve ilave güvenlik uygulamaları hakkında öneriler getirilmiştir.

2. DONANIM VE YAZILIM GÜVENLİĞİ

Donanımsal güvenlik, internet altyapısı ve ateş duvarını içermektedir. İnternet teknolojileri destekli uzaktan eğitim programının internet altyapısı Türk Telekom A.Ş. tarafından verilmekte olan metro ethernet servisi üzerinden çalışmaktadır. Bu bağlantının dış dünyadan izole ve sadece bu uzaktan eğitim programları için kullanılıyor olması ile internet altyapı güvenliği sağlanmaktadır. Çoklu yönlendirici trafik grafiği (MRTG) ile bant genişliği anlık izlenmekte, günlük haftalık ve aylık raporlar ile ilave bant genişliği ihtiyacı hakkında bilgi edinilmekte ve bu şekilde yetersiz bant genişliğinden kaynaklanacak olası sorunların önüne geçilmektedir. Uzaktan eğitim yönetim sistemi yazılımı, enstitüde bulunan uygulama ve veritabanı sunucularından

çalışmakta böylece İnternet servis sağlayıcılardan kaynaklanacak sorunların önüne geçilmektedir. Dış dünyadan gelecek internet saldırılarına karşı donanımsal ateş duvarı kullanılmaktadır. Linux işletim sistemine sahip ateş duvarının çekirdeğinde ön tanımlı olarak gelen Netfilter paketi, yeni adı ile IP tabloları(iptables), ile sistem güvenli hale getirilmekte ve ağ trafiği yönlendirilmektedir. Netfilter(iptables) kurallar oluşturmak için iptables komutu kullanılmaktadır [2]. Herhangi bir zincire gelen IP paketi kurallardan biriyle uyum sağlayıncaya kadar ilerleyerek zincirin sonuna kadar ulaşır. Herhangi bir kuralla uyuşmayan paket işleme sokulmaz. Bununla birlikte sadece kullanılan kapılar (ports) açılarak sisteme erişim, belirlenen kurallar çerçevesinde sağlanmakta, yetkisiz kullanıcıların sisteme erişip zarar vermesinin önüne geçilmektedir. Bir örnek vermek gerekirse, uzaktan eğitim içerik geliştirme grubu öğrencilerinin sistemde mevcut olan yada diğer dönem için gerekli dersleri güncelleştirmeleri sunucu üzerinde yapılmakta idi. USB flash disk ile yapılan güncelleştirmelerde bu cihaz içerisinde bulunan virüsler sisteme bulaşıp zarar vermekteydi. Bunun için, içerik güncellemeden sorumlu tek bir öğrenci belirlenip, ateş duvarından sadece gazi ağına bağlı bilgisayarlar üzerinden (194.27.x.x IP'ye sahip) ftp programının çalıştığı 21. kapıya erişim hakkı verilmesi yoluna gidilmiştir [3].

Bununla birlikte sunuculardaki yüklü olan anti virüs programı, düzenli değiştirilen yönetici şifresi, sadece sistemin ihtiyacı olan Windows 2003 bileşenlerinin yüklenmesi, en güncel servis paketinin yüklenmesi, Windows 2003 sunucu güvenlik rehberine uyulması ve güncelleştirilmelerin devamlı yapılması ile yazılımsal güvenlik sağlanmaktadır [4-5].

3. EĞİTİM YÖNETİM SİSTEMİ YAZILIMI VE ÖLÇME DEĞERLENDİRME SINAVI GÜVENLİĞİ

Özel bir firmadan alınan uzaktan eğitim yönetim sistemi yazılımın güvenliği birçok aşamada sağlanmaktadır. Bunlar SQL enjeksiyonu, XSS, kullanıcı oturumları ve yetkilerinin düzenlenmesi, yetkisiz kullanıcının bloklanması, ASP.NET hata mesajları, vize sınav sisteminin güvenliğidir. Yazılımda veritabanı sınıfları farklı bir katmanda tutulup tüm sorgular parametrik olarak çalıştırılmakta olduğundan SQL enjeksiyonu tehlikesi bulunmamaktadır. Zengin metin editörü hariç tüm kullanıcı girdileri HTML-kodlama(encode) yapılarak kabul edilmektedir. Zengin metin editörü girdileri ise sadece bu editörden gelebilecek metinlerin nizamlı deyimler (regular expression) kullanılarak ayıklanması sonucunda kabul edilir. Diğer bir XSS yöntemi adres satırına parametrik olarak tehlikeli metinlerin girilmesi sonucunda ASP.NET'in bu metinleri sayfa kaynak koduna dahil etmesidir. Bu yöntem ise, tüm bu parametrelerin alfa nümeriklik kontrolünden geçirilmesi suretiyle engellenmiştir. Kullanıcılar sisteme giriş yapamadıkları takdirde herhangi bir sayfaya ya da işleme ulaşamazlar. Bu oturumlar yönetici hesabından değiştirilebilen süreler ile kaldırılabilmektedir. Böylece kullanıcı oturumları kontrol altında tutulur. Kullanıcılar sadece yetki alanına giren sayfalarda yetkili oldukları bilgilere ulaşabilirler. Örneğin bir öğrenci adres satırına başka bir öğrencinin kodunu yazsa dahi bu sayfayı görüntüleyemez. Buna ilaveten web ara yüzünün görsel yapısı çerçeveler ile sağlanmış ve böylelikle kullanıcıların ulaşamayacağı sayfalar java betikleri (javascript) ile gösterilmiyor olması bir güvenlik açığı oluşturmaz. Nitekim java betikleri (javascript) kodları engellense dahi her sayfa kendi içinde yapmakta olduğu yetki kontrolleri sayesinde yetkisiz kullanıcıların girişlerine izin vermeyecektir. Böylece kullanıcı yetkileri düzenlenmiş olur. Uygulama seviyesinde, kullanıcıların parolalarını 3 kere arka arkaya hatalı girmeleri durumunda sisteme girişlerinin engellenmesi sağlanmıştır. Bu engelleme hem kullanıcı bazında hem de IP adresi bazında olabilir. Bu engellemeleri sistem yöneticileri kaldırabilmektedir. Veritabanında kullanıcı parolaları Microsoft SQL 2005'in sağladığı tek yönlü şifreleme algoritmasından geçerek tutuldukları için veritabanı sunucusu üzerinden elde edilemezler.

Böylece parola güvenliği sağlanmaktadır. ASP.NET hata mesajları sistemin arka planında çalışmakta olan mekanizmalar ile ilgili çeşitli ayrıntıları içermektedir. Uygulamadaki tüm sayfaların teknik olarak belli bir hiyerarşiye bağlanması ve tüm hata mesajlarının güvenli bir sayfaya yönlendirilmesi sayesinde bu tehlike giderilmiştir. Buna ilaveten, sayfa adreslerinin başlarına tarayıcı adres satırında '~' işareti konarak elde edilebilen hata mesajları da engellenmiştir. Öğrencilerin sınavları aldıkları süre içerisindeki hareketleri kısa zaman aralıklarıyla kaydedilir ve danışmanlar bu kayıtlara ulaşarak öğrencilerin sınav süresi içerisinde ne yaptıkları bilgisini ayrıntılarıyla görebilir. Bu ayrıntılar arasında işleme harcanan saniye bilgisi, hareket bilgileri ve IP adresi de bulunmaktadır. Böylece vize sınav güvenliği sağlanmaktadır [6].

İnternet teknolojileri destekli uzaktan eğitim final sınavının yılsonu başarı puanı üzerindeki ağırlığı yüzde seksen olduğundan bu ölçme ve değerlendirme sınavının güvenliğinin önemi artmaktadır. Sınav oturumlarında A-B kitapçığının yapılması, daha önceki sınavlarda öğrencilerin beraber sınava gireceği arkadaşları ile irtibata geçtiği anlaşıldığından öğrencinin sınava gireceği sınıf ve sırasının sınav günü daha önceden verilen numara ile belli olması, ders veren öğretim üyelerinin sınav sorumlusu yapılması ile sınav esnasında çıkacak olası soru ve seçenek yanlışlarına anında müdahale edilmesi yoluna gidilmiştir [7].

4. SONUÇLAR

Yukarıda anılan güvenlik uygulamalarının, sistem ilk kurulduğunda alınan önlemlerle beraber zamanla karşılaşılan sorunları aşmak için geliştirildiğinden uzaktan eğitim verecek kurum ve kuruluşlara ışık tutacağı düşünülmektedir. Bu güvenlik uygulamalarına ilaveten

eğitim yönetim sistemi yazılımı kullanıcı girişi SSL (Güvenli Soket katmanı), her bağlantıda yenilenen güvenlik kodu veya sanal klavye ile sağlanabilir. Benzer şekilde, hali hazırda çalışmaları yürütülmekte olan, öğrencilerin değişik illerde ikamet etmelerinden dolayı almakta güçlük çektikleri öğrenci belgesi ve benzeri belgelere internet sayfası üzerinden ulaşabilmeleri ve bu belgelere istekte bulunduktan sonra ekranda oluşan kodu mobil imza ile onaylamaları yoluna gidilebilir.

KAYNAKLAR

[1] S. Tornincasa, "Great Leap Forward for Distance Learning", **International Workshop on New WEB technologies for collaborative design, learning and training,** pp. 2-16, 2003.

[2] T. Katic, P. Pale, "Optimization of Firewall Rules", **Information Technology Interfaces International Conference**, pp. 685 – 690, 2007.

[3] G. Lawton, "Open source security: opportunity or oxymoron?" **IEEE Computer Society**, Volume 35, no. 3, pp. 18 – 21, 2002.

[4] İnternet: Microsoft, "Microsoft Güvenlik", http://www.microsoft.com/turkiye/guvenlik/default.mspx , 2008.

[5] İnternet: Microsoft ,"Windows 2003 Güvenlik Yönetimi", http://support.microsoft.com/winsrv2003 , 2008.

[6] Enocta, "LMS akademik 50 kullanım kılavuzu", **Enocta**, Ankara, 2008.

[7] P. Kitsos, N. Sklavos, O. Koufopavlou, **"**An efficient implementation of the digital signature algorithm**", Electronics, Circuits and Systems, 2002. 9th International Conference,** pp. 1151 - 1154, 2002.