LDAP ile Güvenli Kullanıcı Kontrol Sistemi

İsmail Kavak[1], Gül Fatma Türker[2]

[1]Süleyman Demirel Üniversitesi, Bilgi İşlem Daire Başkanlığı, Isparta

[2]Süleyman Demirel Üniversitesi, Elektronik ve Haberleşme Mühendisliği Bölümü, Isparta

ismailkavak@sdu.edu.tr, gulturker@sdu.edu.tr,

Özet:
Günümüzde kullanıcı kontrol ve yetkilendirme gerektiren uygulamalarda hızlı ve güvenli çözümlere ihtiyaç duyulur. Bu çalışmada amaç, LDAP(Lightweight Directory Access Protocol) veri tabanından kullanıcı kontrolü için istekte bulunan istemcilerin, güvenli bir şekilde yönetimini sağlayan kurallar oluşturmak. Böylece LDAP ile oluşturulan SSO(Single Sign On) 'yu kullanarak tek kullanıcı doğrulama sistemine erişimin kontrolü sağlanır. Her bir istemcinin(parola kontrolü gerektiren uygulamaların) hangi kullanıcı bilgilerine ulaşabileceği ve geri dönüş cevaplarının neler olacağı, kurallar dizisi ile belirlenir. LDAP veri tabanındaki her bir kullanıcı grubunun istekte bulunan istemcilerin çalışma yöntemlerine göre doğru ve güvenli olarak kullanıma sunulması ile tek kullanıcı kontrol sistemli yapılar geliştirilebilir.

Anahtar Sözcükler: LDAP, Güvenlik, Kullanıcı Kontrol, Kullanıcı Yetkilendirme.

Secure User Control System with LDAP

Abstract: Nowadays, fast and secure solution for applications that require user authorization and control are needed. The purpose of this study is to create rules for user control of the requesting client that provides a secure way management from LDAP (Lightweight Directory Access Protocol) database. Thus, with using SSO (Single Sign On), created with LDAP; authentication system of the single-user access control is achieved. Each client's (applications which requires password control) set of rules are determined as to which user information is accesseble and what is return answer will be. Single control system can be improved with servising according to working subject of the requesting clients in the LDAP database user group, safely and correctly.

Keywords: LDAP, Security, User Authentication, User Authorization.

1.Giriş

Bir dizin hizmeti; ağ cihazları, uygulamalar, bilgisayarlar, insanla ilgili verileri tutan ve sunumunu sağlayan bir servis hizmeti sunucusudur. Hizmeti alan kullanıcıları yetkilendirmeye izin veren bir veri tabanı deposudur. Özellikle internet üzerinden bilgiye erişim ihtiyacının artışı ile son on yılda dizin hizmetleri geliştirilmiştir. Dağıtılmış yapıdaki uygulamalar için yaygın olarak kullanılan bir servis olmuştur [1].

Dizin hizmetleri çeşitli arayüzler ve uygulamalar ile oluşturulmuş bilgiye erişime imkan sağlar. " Lightweight Directory Access Protocol " açık kaynak kodlu bir endüstri standardıdır [2]. Ilk defa 1980'lerin sonlarında, ITU-T ve ISO tarafından yayımlanan, uluslararası standardı, Dizin Erişim Protokolü (DAP) idi. LDAP , DAP'ın X.500 ünün hafifletilmiş bir alternatifi olarak aynı aileden türemiştir [3].

LDAP X500 protokolünün benzeri bir veri tabanı kullanan bilgi dizinlerine erişimi sağlayan bir teknolojidir [2]. LDAP isim olarak Directory Access Protokolünün lightweight eklenerek hafifleştirilmiş şeklidir. Heavyweight olarak en çok bilinen yönetim protokolü X.500 ile veri temsilinde benzerlik bulunurken aralarında birkaç yapısal farklılıklar vardır [1]. LDAP esnekliği ve

mevcut uygulamalar ile uyumlu olmasından teknolojide artan bir öneme sahiptir [2].

Basit Dizin Erişim Protokolü olarak kullanılmakta olan LDAP ile dizin servislerini sorgulama ve değiştirme işlemleri yapılır. Veri tabanı hizmeti veren bir sistem içinde verilere merkezi olarak ulaşımı gerçekleştiren uygulama katmanında çalışan bir internet protokolüdür [4]. IBM Tivoli, Novell, Sun, Oracle, Microsoft ve diğer birçok satıcının LDAP tabanlı uygulamaları bulunmaktadır [2]. Hızlı ölçeklenebilir ve yönetilebilir bir dizin yapısı oluşturulur.

Standart olarak depolanan LDAP verilerinin tutulduğu servis ayarlarında; servisin verildiği ağ ayarları, yetkili kullanıcı bilgisi, uygulama ayarlama parametreleri, kullanıcı ve sunucu sertifikaları ile erişim kontrol listeleri yer almaktadır. LDAP, uygulamaların ihtiyaç duyduğu her türlü özelliğin eklenmesini sağlayan esnek bir yapıya sahiptir. Örneğin eposta servisi için ihtiyaç duyulan mailLocalAddress, mailHost, UserCertificate gibi özellikleri ihtiyaç duyulan her bir kullanıcı için ayrı ayrı tanımlanabilmesini olanak sağlar [2].

Yapılan çalışmalar 2000'nin ilk yıllarında hızla geliştirilmiştir. World Wide Web ulaşım izinlerinin ve bilgilerinin LDAP içinde tanımlanması ve yönetilmesi [5], İlişkisel tablolar ile LDAP hiyerarşik arama yöntemleri tanımlanması [6], LDAP sunucularda ön bellek mekanizması ve yöntemleri [7], Efficient Implementation of LDAP Search Queries with Structured Query Language (SQL) [8], Trusted Network Binding Using LDAP [9], LDAP Based Distributed Cache Technology for XML [10] gibi çeşitli uygulamalar gerçekleştirilmiştir.

Kurumsal ve kamusal alanlarda hizmet veren sistemler üzerinden kullanıcılara çok sayıda servis sunmak ve bu servislerin çalıştığı makinalarda ayrı ayrı kullanıcı hesapları açmak gerekebilir. LDAP ile sistemin ve kullanıcıların yönetimini kolaylaştıran bir sistem geliştirilmiştir. LDAP desteği veren servislerin LDAP sunucusu üzerinden tek bir kullanıcı girişi ile kullanıcı bilgilerine erişim ve doğrulama yapmalarını sağlar. Bu çalışma ile LDAP veri tabanından kullanıcı kontrolü için istekte bulunan istemcilerin, güvenli bir şekilde yönetimini sağlayan kurallar oluşturulmuştur. SSO (Single SİgnOn) için kullanılan LDAP kullanıcı kontrol ve yetkilendirmede gerekli olan güvenlik tanımlarını en esnek şekilde yapılması sağlanmıştır.

2. LDAP

İlk defa 1980'lerin sonlarında kullanılan Dizin Erişim Hizmeti olan DAP'ın X.500 dizin hizmetine erişmek için istemciler tarafından kullanılması amaçlanmıştır. DAP, bu süre için donanım üzerinde konuşlanmış olması, çok karmaşık olması gibi sebeplerden dolayı çok fazla popülerlik kazanamadı. Daha sonraki yıllarda ise LDAP hafifletilmiş olarak X.500 protokolünden geliştirilmiştir [3].

Bugüne kadar, çok sayıda LDAP sunucusu BigFoot (http://www. Bigfoot.com / index.jsp) ve Infospace (www. infospace.com) gibi Megaölçekli olmak üzere, kamu küçük işletmelerde kullanılmaktadır. Birçok üniversite ve işletme, posta hizmeti, kimlik sistemleri, personel ve öğrenciler hakkında bilgi saklamak ve hızlı ulaşmak için dizin sunucusu olarak yüklenmiş ve yapılandırılmış olan LDAP protokol servisi kullanılmaktadır. Temel dizin arayüzlerin bir listesi Avrupa araştırma ve Gelişmiş Ağ Teknoloji (DANTE) kurumunca standardize edilmiştir [2].

LDAP dizinleme sisteminde her kayda ait özellikler (attributes) ve bu özelliklerin değerleri (values) vardır. Her kaydın ait olduğu bir nesne sınıfı (object class) vardır. Bu yapı sayesinde dünya üzerindeki her LDAP kaydı biricik olur. Bunun için dns de olduğu gibi hiyerarşik bir isimlendirme kullanılmıştır. Kullanıcı bu biricikliğini DN (Distinguished Name) özelliğinden alır [11].

LDAP terimi şu hizmetleri kapsamaktadır:

- TCP/IP protokolü üzerinde çalışan, istemci-sunucu modeline dayanan dağıtık bir dizin hizmet protokolü.
- Lightweight Directory Access Protocol; dizin hizmetlerine (directory services) erişebilmek için kullanılan, standart, genişletilebilir bir Internet protokolü.
- Bir dizini kullanmakta rehberlik edecek dört model içerir:
- Bir dizin (directory) içine verinin nasıl ekleneceğini tanımlayan bilgi modeli (information model)

- Dizin içinde bulunan verinin nasıl referanslandırılacağını ve düzenleneceğini belirleyen adlandırma modeli (naming model)
- Dizin verisi ile ne yapılacağını belirleyen işlevsel model (functional model)
- Dizin verilerini yetkisiz kullanıcılardan koruyacak güvenlik modeli (security model)
- LDAP Data Interchange Format (LDIF); dizin verilerini değiş-tokuş etmek için standart metin biçimi.
- LDAP sunucu yazılımı; Ticari veya açık-kaynaklı implemantasyonlar (OpenLDAP, Sun Directory Server, Microsoft Active Directory)
- LDAP sunucularla ya da LDAP–tabanlı programlarla bir arada gelen komut-satırı araçları
- LDAP istemci uygulamaları geliştirebilmek için kullanılacak LDAP API'leri.

LDAP protokolü message-oriented (mesaj kaynaklı) bir protokoldür. Bunun anlamı şudur: istemci istek içeren bir LDAP iletisi oluşturur, ve mesajı sunucuya gönderir, sunucu ise bu istemi işler, ve sonucu bir veya birden fazla LDAP mesajı olarak istemciye yanıtı gönderir.

LDAP mesaj tabanlı bir protokol olduğu için, istemci bir anda birden fazla istemde bulunabilir. Örneğin bir istemci aynı anda iki arama işlemini aynı anda yapabilir. Birden fazla işlemi aynı anda yababilmeyi mümkün kılması LDAP protokolünü buna izin vermeyen HTTP ve benzeri protokollere göre daha esnek ve verimli bir protokol yapmaktadır [12].

LDAP dizinlerde assagidaki islemlerin yapilmasina izin verir:

*Kullanicin girdigi kritere gore arama yapma (search)
*Bir girdi(**entry**) ekleme (add)
*Bir **entry** silme (delete)
*Bir girdiyi degistrime (modify)
*Distinguished name (DN) 'i yada RDN(Relative Distinguished Name)' in dizindeki yerini degistirme (modifydn)
*Iki entry'i karsilastirma (compare)

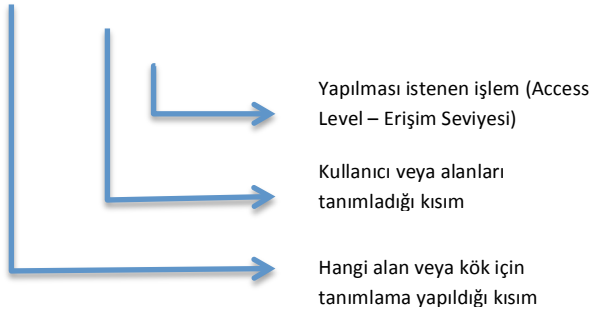
LDAP üç kategori içinde tanımlanabilecek 9 temel protokol operasyonuna sahiptir:
Sorgulama Operasyonlar: arama ve karşılaştırma (search, compare) güncelleme Operasyonları: ekleme, silme, güncelleme, yeniden isimlendirme (add,delete, modify, modify DN (rename)) Kimlik doğrulama (authentication) ve kontrol operasyonları: bağlanma, bağlantıyı kesme ve bağlantı iptali (bind, unbind, abandon.)[11].

3. LDAP Yetkilendirme Tanımları

Ldap konfigurasyonları statik ve dinamik olarak iki şekilde yapılmaktadır. Eski stil statik configurasyon için kullanıcı yetkilendirme tanımlaması "access to ... " ile başlarken, dinamik konfigurasyonda yetkilendirme, yine ldap tablolarından alınmaktadır. Yetkilendirme tanımı "olcAccess" alanına yazılarak yapılmaktadır.

Yetkilendirmeler hangi alanlarda kimin ne yapması üzerine kurulmuştur.

access to * by * read



Level	Privileges	Description
none =	0	Hiçbir erişim yok
disclose =	d	Oluşan hatalar için bilgi alabilmesini sağlar
auth =	dx	Kullanıcının şifre ile giriş yapıması gerektiğini bildirir
compare =	cdx	Karşılaştırma yapabilmesini sağlar
search =	scdx	Arama yapabilmesini sağlar
read =	rscdx	Bilginin okuma yetkisini verir
write =	wrscdx	Bilgiyi değiştirme ve silme yetkisi verir
manage =	mwrscdx	Bilgiyi yönetme yetkisi verir.

Tablo 1. Erişim Seviyeleri

Specifier	Entities
*	Tüm kullanıcıları kapsar
anonymous	Yetkisiz kullanıcı(lar)
users	Kullanıcı ve şifre ile giriş yapmış kullanıcı(lar)
self	İşlem yapılması düşünülen alan ile ilişkili kullanıcı(lar)
dn[.<basic-style>]=<regex>	Düzenli ifade ile eşleşen Kullanıcı(lar)
dn.<scope-style>=<DN>	Bir DN kapsamında Kullanıcı(lar)

Tablo 2. Erişim Hakları

1. to *
   Tüm ağaç yapısı için yapılan tanımlamadır.

2. to dn[.<basic-style>]=<regex>
   DN üzerinde düzenli ifade tanımlaması.

3. to dn.<scope-style>=<DN>
   scope-style için base, one, subtree, children tanımlarını kullanılmaktadır.

   base : tanımlanan tam DN ile eşleştiğinde,

   one: tanımlanan DN e ait sadece tek bir alt ağaç dalına ait tanımlamalar için geçerli olsun

   subtree: tanımlanan DN e ait tüm alt dallanmaları için geçerli

   children: tanımlanan DN hariç tüm alt dalları için geçerli tanımlamadır.

4. to filter=<ldap filter>
   to filter=(objectClass=person) gibi tanımlı bir DN e ulaşmak için kullanılır.

5. to attrs=<attribute list> veya to attrs=<attribute> val[.<style>]=<regex>
   ile veritabanı içinde tanımlanan her hangi bir niteliğin olduğu tanımlamara ulaşım için kullanılır.

Dinamik ldap tanımlamasındaki alt parametreler:

olcAccess: <access directive>

<access directive> ::= to <what>

[by <who> [<access>] [<control>]]+

<what> ::= * |

[dn[.<basic-style>]=<regex> | dn.<scope-style>=<DN>]

[filter=<ldapfilter>] [attrs=<attrlist>]

<basic-style> ::= regex | exact

<scope-style> ::= base | one | subtree | children

<attrlist> ::= <attr> [val[.<basic-style>]=<regex>] | <attr> , <attrlist>

<attr> ::= <attrname> | entry | children

<who> ::= * | [anonymous | users | self

| dn[.<basic-style>]=<regex> | dn.<scope-style>=<DN>]

[dnattr=<attrname>]

[group[/<objectclass>[/<attrname>][.<basic-style>]]=<regex>]

[peername[.<basic-style>]=<regex>]

[sockname[.<basic-style>]=<regex>]

[domain[.<basic-style>]=<regex>]

[sockurl[.<basic-style>]=<regex>]

[set=<setspec>]

[aci=<attrname>]

<access> ::= [self]{<level>|<priv>}

<level> ::= none | disclose | auth | compare | search | read | write | manage

<priv> ::= {=|+|-}{m|w|r|s|c|x|d|0}+

<control> ::= [stop | continue | break]

4. Sonuç ve Öneriler

SSO (Single SİgnOn) için kullanılan LDAP kullanıcı kontrol ve yetkilendirmede gerekli olan güvenlik tanımlarını en esnek şekilde yapılması sağlanmıştır. Böylece internete açık olan bu servisin olası tüm güvensiz erişimlere karşı yasaklama mekanizması oluştururken, doğru uygulama ve kullanıcıların ilgili tablo ve verilere ulaşımının esnek bir yapılandırma ile yapılmasını sağlamış oluyor. Single Sign On LDAP ile yapan tüm kurumların kullanıcı kontrolü için kullandıkları 3.parti uygulamalarından kaynaklanan güvenlik açıklarının merkezi olarak önlenmesini ve kontrol edilmesini sağlayacaktır.

5. Kaynaklar

[1] T.A. Howes, *The Lightweight Directory Access Protocol: X.500 Lite*, tech. report TR-95-8, Center for Information Technology Integration, Univ. of Michigan, 1995.

[2] Vassiliki Koutsonikola Athena Vakali , **"**LDAP: Framework, Practices, and Trends, IEEE Computer Society,2004 IEEE INTERNET COMPUTING ***Spotlight***

[3] Kobsa A., Fink J., "An LDAP-based User Modeling Server and Its Evaluation", Springer, User Model User-Adap Inter (2006) 16: 129–169

[4]www.ulak.net.tr/dokumanlar/programlama/2000 php/ldap/index.html

[5] Aldred K. B., Brown C.S., Hahn T.J., Stokes E.J., Management of and Access to Informaiton and other Material via The World Wide Web in an LDAP Environment, 2001

[6] Bachmann D.W., Corn C.F., Fichtner G.L., Mancisidor A.R., Shi S., Method of Hierarchical LDAP Searching with Relational Tables, 2000

[7] Byrne D.J., Murthy C.R., Shi S., Shu C., " Lightweight Directory Access Protocol (LDAP) Directory Server Cache Mechanism and Method ",2002

[8] Corn C.F., Fichtner G.L., Mancisidor R.A., Shi S., ,Efficient Implementation of LDAP Search Queries with Structured Query Language (SQL),2002

[9] Borsato L.W., Gaudet M., Hamilton I., Anderson R., Waters G., Trusted Network Binding Using LDAP, 2003

[10] Marron P. J., Lausen G., LDAP Based Distributed Cache Technology for XML, 2005

[11] Ldap nedir http://ldap.nedir.com/#ixzz2qYKJ0rq5

[12] http://tr.wikipedia.org/wiki/LDAP