KÜTÜPHANE TEK KULLANIMLIK ŞİFRE YETKİLENDİRMELİ ÖNBELLEKLEME SERVİSİ

Ferdi AYAYDIN
ODTÜ Bilgi İşlem Daire Başkanlığı
Ağ Destek Grubu
ferdi@metu.edu.tr

Gökhan ERYOL
ODTÜ Bilgi İşlem Daire Başkanlığı
Ağ Destek Grubu
eryol@metu.edu.tr

1. ÖZET

ODTÜ kütüphanesinin üyesi olduğu yurt içi ve yurt dışı kaynaklara ODTÜ içerisindeki bir bilgisayardan otomatik olarak ulaşılabilmektedir. Kullanıcılarımızın bu kaynaklara ODTÜ dışından da gerekli şifre güvenliğinin sağlanmış olduğu yetkilendirmeli bir şekilde bağlanabilmesi zorunlu hale gelmiştir. Bu bildiri de squid web önbellekleme programı kullanılarak, yerleşke dışındaki kullanıcılarımızın, kütüphanenin üyesi olduğu kaynaklara nasıl yetkilendirmeli bir şekilde bağlanılabileceği ve bu bağlantıda şifre güvenliğinin nasıl sağlanacağı anlatılmaktadır. Şifre güvenliğinin sağlanması için kullanıcılarımızın merkezi sistem kullanıcı kodu ve şifreleriyle güvenli bir sayfaya bağlanıp buradan aldıkları "Tek Kullanımlık Şifreleri" kullanmaları gerekmektedir. Tek kullanımlık şifreler, kullanıcının açtığı her bir web penceresini yetkilendirmek için sınırlı bir süre aktif olmaktadır. Süre bitiminde, kullanıcı merkezi sistem kullanıcı kodu ve şifresiyle yeni bir Tek Kullanımlık Şifre alarak işlemlerine devam edebilir.

Anahtar Kelimeler: önbellekleme, OTP, TKŞ, tek kullanımlık şifre, proxy, webcache, squid, auth, şifre, güvenlik

2. GİRİŞ

ODTÜ kütüphanesi, yurt içinde ve yurt dışında birçok veritabanına yerleşke içinden bağlanma ve araştırma yapma imkanı sağlamaktadır. Bu veritabanı bağlantıları ODTÜ IP adresi bloğuna (144.122.0.0./16) açılmakta, ODTÜ içindeki bir bilgisayarı kullanan kullanıcımız otomatik olarak bu veritabanlarına ulaşma hakkı kazanmaktadır. Birçok kullanıcımız, araştırma işlerini ODTÜ dışında kullandıkları bilgisayarlardan da yapabilmeyi istemekte, bu durum beraberinde kullanıcı yetkilendirme ve şifre güvenliği problemlerini getirmektedir.

Mevcut teknolojiler düşünüldüğünde kullanıcıların belli bir yetkilendirme mekanizmasıyla sınırlandırılmış web sayfalarına ulaşımlarının sağlanması için bir web önbellekleme servisi kullanmak en uygun çözüm görünmektedir. Dünya çapında birçok sunucuda bulunan ve ODTÜ'de de uzun yıllardır başarıyla yerleşke içi bağlantılarda servis veren squid web önbellekleme programı bu iş için seçilmiştir.
Web önbellekleme, İnternet üzerinden istenilen objelerin (HTTP, FTP, Gopher gibi protokoller üzerinden ulaşılabilen verilerin), yerel alan ağı içerisinde bir sunucuda saklanması, ve aynı objenin aynı veya farklı bir istemci tarafından istenilmesi halinde, bu sunucu tarafından isteğin karşılanmasıdır. Aynı web önbellekleme sunucusunu kullanan tarayıcı programların, ortalamada isteklerinin karşılanması süresi düşer, ayrıca bant genişliği tasarrufu sağlanmış olur. Web önbellekleme servisinden faydalanılabilmesi için, tarayıcı programına servisin tanıtılması gerekmektedir. ODTÜ içi bağlantılara hizmet veren web önbellekleme servisi 1999 yılından beri kullanılmaktadır. Bu servis aracılığıyla kullanıcılar gerekli ayar dosyasını bilgisayarlarına tanıtarak çok kullanılan web sayfalarına ODTÜ içinden hızlı erişim sağlayabilmekteler.

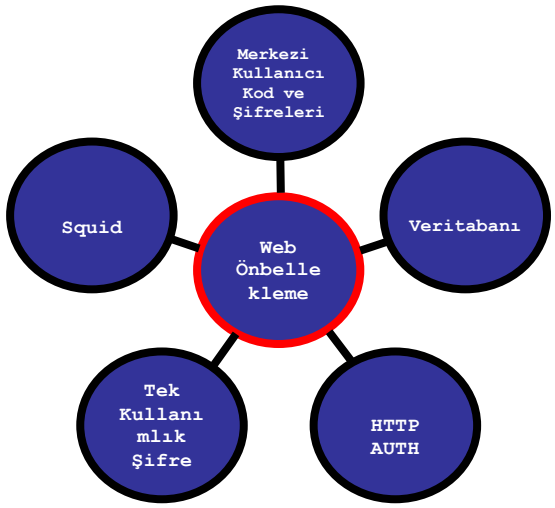
3. İHTİYAÇLAR

Kampüs dışından ODTÜ kullanıcılarının kütüphane kaynaklarına erişimlerini sağlamak için kurulacak sistem birtakım gereklilikleri sağlamalıdır. Sistemi kurarken bu gereklilikleri göz önünde bulundurarak tasarım yapmak gereklidir. Özetle bunlardan bahsedersek:

1) Hem ODTÜ öğrencisi hem de ODTÜ personeli için bir yetkilendirme mekanizması olmalıdır.
2) Kullanıcıların girecekleri kullanıcı kodu ve şifreler güvenli olmalıdır.
3) Tüm tarayıcı programlar (browserlar) tarafından desteklenmelidir
4) Kullanıcılar tarafında uygulama kolaylığı olmalıdır
5) Servisin kurulum ve işletim kolaylığı olmalıdır.
6) Kullanıcıların aynı anda tek bir bilgisayardan bağlanabilmesini sağlayacak önlem bulunmalıdır.

7) Kullanıcıların sadece yetkilendirilmiş web sayfalarına bağlanabilme izni olmalıdır.
8) Amaç dışı kullanımda kullanıcı ve IP engellemesi olmalıdır.
9) Kullanıcıların kullanıcı kodları ve şifrelerini başkalarıyla paylaşmasını sınırlandıracak yapıda olmalıdır.
10) Hata uyarma sayfaları yeterince açık olmalıdır.
11) Kullanıcıların en fazla yapabilecekleri bağlantı sayısı sınırlı olmalıdır.
12) Kullanılacak servis makinesi yeterince güvenli olmalıdır.
13) Servis makinesinin işletimi ve ayarları belgelenmiş olmalıdır.

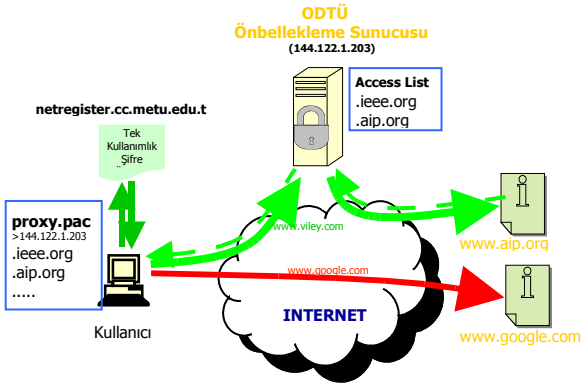
Yukarıda maddelenen bütün bu gerekliliklerin sağlanması için kurulacak yapı düşünüldüğünde sistemi oluşturan parçalar şöyle şekillenmektedir:



Şekil 1. Servis Birleşenleri

4. SİSTEMİN GENEL YAPISI

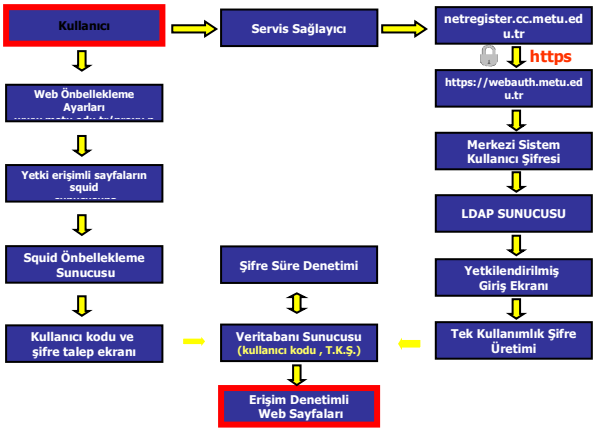
Web önbellekleme programı squid'in yaptığı iş, kendisine yönlendirilen web sayfası isteklerini kullanıcı adına alıp, kendisi adına bunu karşı tarafa gönderip, gelen sonucu istekte bulunan kullanıcıya geri döndürmek şeklindedir. Kullanıcı tarafında hangi web sayfalarına ulaşmada squid önbellekleme servisinin kullanılacağını belirtmek için bir ayar dosyası kullanılır. (proxy.pac) Bunu tarayıcı programlarına tanıtan kullanıcılar, bu ayar dosyasında yazılı web sayfalarına gitmek istediklerinde isteklerini squid servis makinesine yönlendirirler. Bu aşamadan sonra squid servis makinesinde yapılacak olan ayarlar gereği kullanıcıya kullanıcı kodu / şifre sorulacaktır. Kullanıcının yazdığı kullanıcı kodu ve şifreler açık metin (clear text) olarak iletileceği için güvenlik sorunları doğurmaktadır. Bu güvenlik kaygılarını en aza indirebilmek için kullanıcılara mektuplarını okumak, ODTÜ'ye özel servisleri kullanmak için verilen kullanıcı kodu / şifre ikilileri yerine her bir kullanıcıya verilecek bir "Tek Kullanımlık Şifre" ile bağlantılarını yapmaları sağlanmalıdır. ODTÜ'de kurulan sistemde kullanıcılardan https protokolü ile belirli bir web sayfasına merkezi sistem kullanıcı kodu ve şifrelerle bağlanmaları istenmektedir. Burada yapılan yetkilendirme işlemleri sonrası kullanıcıya bir işlem yardımıyla rastgele seçilmiş harf ve rakamlardan oluşan bir şifre verilir. Bu şifreyi alan kullanıcı, web önbellekleme servisini kullanarak bir veritabanına bağlanırken sorulan kullanıcı kodu / şifre ekranında bu bilgileri girer.



Şekil 2. Web Önbellekleme Yönlendirmesi

Tek Kullanımlık şifreler ile kullanıcı yetkilendirme işlemi iki ana başlık altında toplanabilir. Birinci bölümde kullanıcının bilgisayarında girmesi gereken ayarlar, ikinci bölümde squid servis makinesinin ayarları ve tek kullanımlık şifrelerin oluşturulup veri tabanına kaydedilmesi. Kullanıcının kendi bilgisayarında girmesi gereken tek ayar, web önbellekleme ayarıdır. Bunun için temelde üç yöntem bulunsa da (otomatik bul, bir ayar dosyası kullan ve el ile ayar yap) bunlardan ayar dosyası kullanmayı tavsiye ediyoruz. Kullanıcılarımızdan kullandıkları tarayıcı programın web önbellekleme ayarları ile ilgili bölümüne girip burada ayar dosyası olarak http://www.metu.edu.tr/proxy.pac yazmaları yeterlidir. İlgili tarayıcı program bu dosyadaki bilgilere bakarak yetkilendirmeli web sayfaları için squid servis makinesini, normal İnternet sayfaları için kullanıcının İnternet hizmeti aldığı servis sağlayıcıyı kullanır. Diğer taraftan, ikinci bölümde yapılan işlemlere gelirsek, kullanıcıdan bir servis sağlayıcı üzerinden http://netregister.cc.metu.edu.tr adresine bağlanması istenir. Bu adres, kendisine gelen bağlantı isteğini https://webauth.metu.edu.tr adresine yönlendirir. Burada kullanıcıya merkezi sistemde kullandığı kullanıcı kodu ve şifresi sorulur. Kullanıcının girdiği bilgiler LDAP sunucusunda sorgulanır ve gelen cevaba

göre kullanıcıya yetkilendirilmiş bir web sayfası ekranı çıkar veya hata mesajı döner. Yetkilendirilmiş ekranda kullanıcının tıklayarak tek kullanımlık şifre elde etmesini sağlayacak bir düğme bulunur. Buraya tıklayarak tek kullanımlık şifresini elde eder. Bu şifre aynı zamanda bir veritabanı sunucununa, kullanıcı kodu ile beraber kaydedilir. Kayıtlar belli aralıklarla kontrol edilerek 2 saatlik süreden daha eski girilmiş kayıtlar silinmektedir. Kullanıcılar squid servis makinesi üzerinden ilgili web sayfalarına giderken sorulan kullanıcı kodu ve şifre bilgilerinde daha önce aldığı tek kullanımlık şifre ve kullanıcı kodu bilgisini girer. Bu bilgiler squid servisi tarafından veritabanına sorgulanır. Veritabanında girilen bilgilerle eşleşen bir kayıt bulunursa kullanıcının girişi onaylanır ve açtığı tarayıcı penceresinden girdiği web adresleri squid servis makinesinden geçerek karşı tarafa ulaşır. 2 saatlik kullanım süresi sonrasında kullanıcı kodu ve tek kullanımlık şifre kaydı veritabanından silinince kullanıcının tarayıcı penceresi kullanıcıya tekrar şifre sormaya başlar.



Şekil 3. Sistemin Genel İşleyişi

5. SQUID AYARLARI

Bu bildiride squid servisinin ve hizmetin verileceği makinenin işletim sisteminin kurulması anlatım dışı tutulmuştur. Bu konuda "Kaynaklar" kısmında bulunan referanslardan yararlanılabilir. Squid, varsayılan olarak squid.conf ayar dosyasını kullanır. Bu dosya içerisinde yapılması gereken ayarlar aşağıda sıralanmıştır.

1) Tüm web sayfaları ulaşımında yetkilendirme iste

```
acl authenticate proxy_auth REQUIRED
http_access allow authenticate
http_access deny all
```

2) Sadece izin verilen alan adlarına / IP adreslerine servis ver

```
acl kutuphane_domain dstdomain "~<dosya yeri>"
http_reply_access allow kutuphane_domain
acl kutuphane_ip dst "~<dosya yeri>"
http_reply_access allow kutuphane_ip
acl deny_all_replies src all
http_reply_access deny deny_all_replies
```

3) kutuphane_domain ve kutuphane_ip dosyaları

kutuphane_domain dosyası içeriği:

```
.accesssurgery.com
.acm.org
.acs.org
.aip.org
.
.
```

kutuphane_ip dosyası içeriği:

```
140.234.29.0/24
63.89.64.0/24
194.27.216.0/24
.
.
```

4) Kullanıcı yetkilendirme yöntemi belirt

```
auth_param basic program ~<dizin_adi>/yetki.pl
#
auth_param basic realm http://netregister.cc.
metu.edu.tr adresinden aldiginiz kullanici kodu ve
TEK KULLANIMLIK SIFREYI giriniz !!!
#
auth_param basic casesensitive on
```

5) yetki.pl dosyası

```
.....
while (<>) {
      chop;
      ($usr,$pass) = split;
      $ret = &chk($usr,$pass);
      print "$ret\n";

sub chk
{
query = "select count(*) from $table where u=$usr
and p=$pass";
$res = selectcol_arrayref($query,
{Columns=>[1] } );
return 'OK' if ('1' eq @$res[0]);
return 'ERR';
}
```

6) Diğer ayarlar

error_directory /usr/local/etc/squid/errors/Turkish
acl max-ip-connection max_user_ip -s 1
http_access deny max-ip-connection
acl maximum-connection maxconn 6
http_access deny maximum-connection
acl denied-users proxy_auth username "~<dizin adı>/denied-users"
http_access deny denied-users
authenticate_ip_ttl 120 seconds

7) Yoğun miktarda kullanıcı kodu / şifre denemesi yapan kullanıcıları engelle

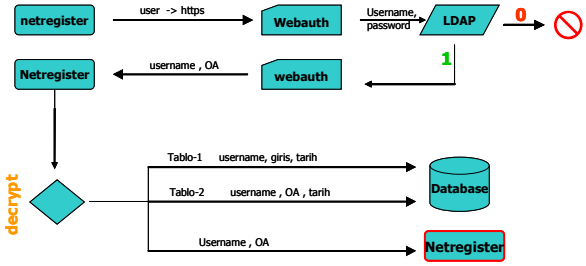
/<dizin_adı>/squid-abuse.sh

tail -f -n0 $squid_log > "~dosya_adı" &
...
sleep 60
...
grep "TCP_DENIED/407"
...
(awk , sort , uniq, wc ...)
...
pfctl -t KAPALILAR -T add <ip_adresi>/32

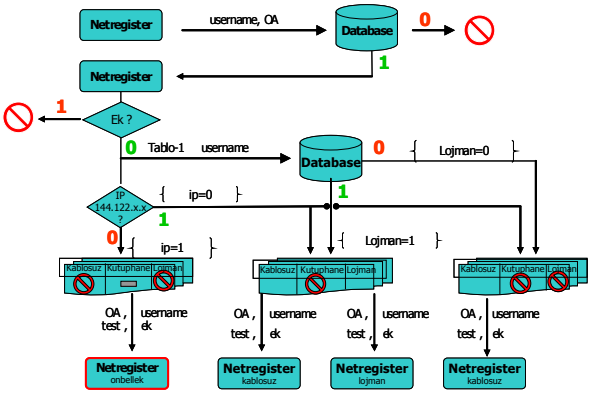
6. TEK KULLANIMLIK ŞİFRE AŞAMALARI

Sistemin işleyişi, kullanıcının tarayıcı programı aracılığıyla http://netregister.cc.metu.edu.tr adresine bağlanmasıyla başlar. Bağlantı isteği https: protokolüyle webauth.cc.metu.edu.tr adresine yönlendirilir. burada kullanıcıdan kullanıcı kodu ve şifre istenir. Bilgiler WebAuth sistemi yardımı ile LDAP sunucusunda sorgulanır. Yetkilendirme olumlu ise WebAuth sistemi kullanıcı kodunu gönderir. Netregister, gelen kullanıcı bilgisini ve sonraki sayfaların güvenlik bütünlüğünü sağlamak için kullanılan oturum anahtarını (OA) ilgili veri tabanına işler.

Kullanıcı kodu, lojmanlar veritabanında sorgulanarak kullanıcının lojmanlarda oturup oturmadığına bakılır. Aynı zamanda kullanıcının IP adresi kontrol edilerek ODTÜ içinden mi, ODTÜ dışından mı geldiğine bakılır. Bu değişkenlere göre kullanıcının ekranı üç bölüme ayrılır. Bunlar kablosuz ağ kayıt bölümü, kütüphane kaynakları için tek kullanımlık şifre alma bölümü ve lojman kullanıcıları IP kayıt bölümü. Kütüphane kaynaklarına ulaşım için kullanılan altyapı, aynı zamanda ODTÜ içinde kablosuz ağ kullanıcılarının MAC adresi kayıtları ve lojmanlarda kalan kullanıcılarımızın IP adreslerinin kaydı için de kullanılmaktadır. (Bknz. Şekil-4)

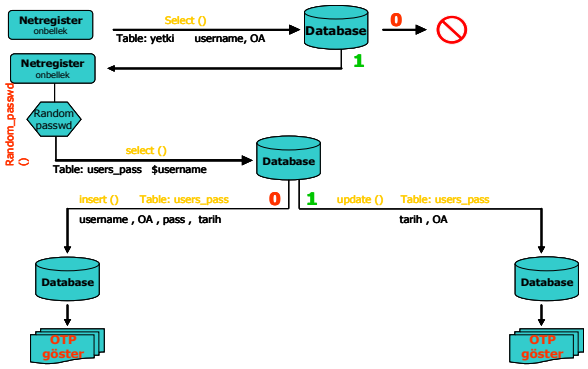


Şekil-4 Sistem İç İşleyişi

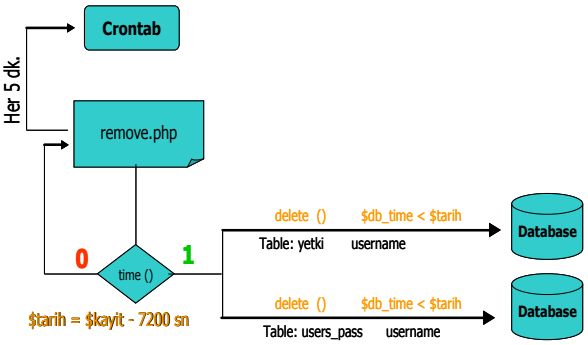


Şekil-5 Sistem İç İşleyişi (devam)

devam eden yapıda, ekranda tek kullanımlık şifre alma ile ilgili düğme tıklandığında ilgili kod, kendisine iletilen kullanıcı kodu ve OA değişkenlerini veritabanında sorgular ve daha önce bu kaydın yetki aldığını kontrol eder. Sonrasında 8 haneli rastgele sayı ve harf üreten bir işlem kullanıcıya şifre üretir. kullanıcı kodu eğer daha önce veritabanında işlenmiş ise yeni üretilen şifre kullanılmaz, eski verilen şifre kaydının tarih bilgisi güncelleştirilir. Kullanıcı kodu değişkeni veritabanında bulunamamışsa yeni üretilen şifre veritabanına kaydedilir. Her iki durumda da şifre kullanıcının ekranına yansıtılır.



Şekil 6. Sistemin İç İşleyişi (devam)



Şekil 7. Tek Kullanımlık şifrelerin silinmesi

Veritabanında kayıtlı tek kullanımlık şifrelerin aktif olma süresi iki saattir. Bu süre içerisinde kullanıcı http://netregister.cc.metu.edu.tr adresine girip kaydını yenilemezse bilgileri veritabanından silinir. Bu kontrol için crontab'da bir işlem çalışır ve şu anki saatten 2 saat öncesine kadar alınmış şifreler dışında kalan şifreleri siler. (Bkz. Şekil-6)

KAYNAKLAR

[1] http://www.squid-cache.org

[2] http://enderunix.org/docs/squid.html

[3] http://www.freebsd.org/docs.html