



MERKEZİ KULLANICI TANIMA SERVİSLERİ

Mustafa Atakan

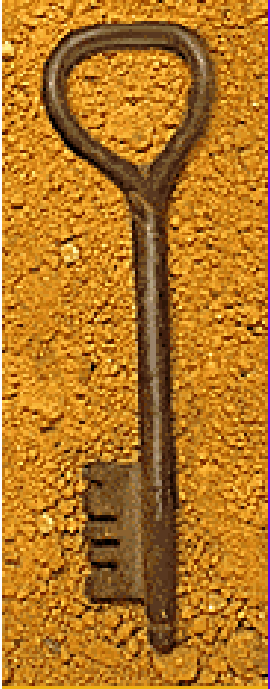
ODTU-BIDB

Teknik Destek Grubu

SUNUM ÖZETİ

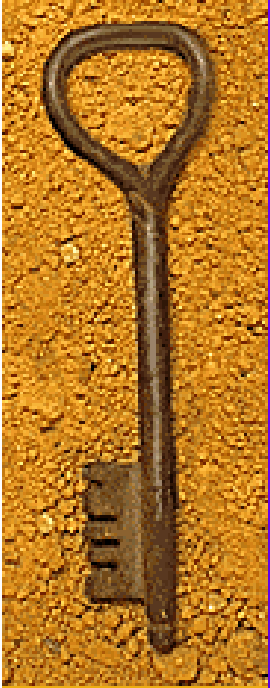
- ◆ Kullanıcı tanıma (authentication) nedir
- ◆ Kullanıcı tanımadaki temel sorunlar
- ◆ Merkezi kullanıcı tanıma (centralized authentication) nedir
- ◆ ODTÜ'deki uygulama





Kullanıcı Tanıma

- ◆ Bir nesnenin (kullanıcı, program, vb...) kendisini tanıtırken iddia ettiği tanımlamanın doğru olup olmadığını belirleme süreci



Kullanıcı Tanıma Süreci

- ◆ Temel olarak kullanıcı ismi (username) ve şifre (password) ikililerinden oluşur
- ◆ Bu ikililer veritabanında tutulur
- ◆ Kullanıcı tanıma sırasında, kullanıcı tarafından girilen şifre veritabanındaki şifre ile karşılaştırılır. Eğer birbirini tutuyorsa kullanıcı tanıma süreci başarı ile tamamlanmış olur
- ◆ En temel haliyle kullanmak güvenli değildir

KULLANICI TANIMADA GÜVENLİK ÖNLEMLERİ

- ◆ Veritabanı güvenliği için şifreler veritabanında “crypted” şekilde saklanır (/etc/shadow)
- ◆ Bilgisayar ağları üzerinde akan bilginin güvenliği için kullanıcı bilgileri hat üzerinden çarpıtılmış olarak gönderilir (ssl)
- ◆ Yine bilgisayar ağları üzerinde akan bilginin güvenliği için şifre yerine şifre ile harmanlanmış bilgiler gönderilir
- ◆ Günümüz teknolojisinde, güvenilir sertifika otoriteleri tarafından imzalanmış elektronik sertifikalar kullanılmaktadır ve bu yapı (PKI) internet üzerinde kullanıcı tanıma sürecinde yaygın şekilde kullanılmaktadır



HETEROJEN SİSTEMLER

- ◆ Kullanıcı tanımadaki en temel sorunlardan bir tanesidir
- ◆ Birbirinden farklı donanımlar, işletim sistemleri ve bunlara bağlı kullanıcı tanıma şekilleri:
 - /etc/passwd ve /etc/shadow (Linux/Unix)
 - NIS (Linux/Unix)
 - Yerel SAM dosyaları ve Active Directory (Microsoft OSs)
 - NDS (Novell)
 -
- ◆ Eğer kullanıcıların bütün sistemleri tek bir şifre ile kullanmalarını gerekiyorsa büyük yönetimsel zorluklar çıkabilir





MERKEZİ KULLANICI TANIMA

- ◆ Kullanıcı tanıma sürecinin tek bir noktadan yönetilmesidir
- ◆ Avantajları:
 - Kullanıcı bilgileri tek bir veritabanında tutulur. Ekleme/Çıkarma durumunda bütün veritabanlarını güncelleme zorunluluğu yoktur
 - Sistem yöneticisinin yanlışlıkla bazı veritabanlarına eksik/fazla kullanıcı bilgisi girme ihtimali yoktur
 - Kullanıcı, şifresini değiştirmek istediğinde birden fazla yerde aynı işlemleri yapmak zorunda kalmaz
 - Kullanıcı herhangi bir sistemde şifre değiştirdiğinde, diğer sistemlerde değişikliğin aktif hale gelmesi için beklemek zorunda kalmaz

AVANTAJLAR (devam)

- Dağıtık kullanıcı tanıma servislerinde bütün veritabanlarının güvenliğini ve servis kalitesini sağlamak için daha fazla kaynağa (insan, zaman, para, vb...) ihtiyaç vardır.
- Kullanıcı bilgileri sistem yöneticisinin kontrolü altında olmayan platformlara taşınmaz

ODTÜ'deki UYGULAMA

- ◆ ODTÜ Bilgi İşlem, merkezi kullanıcı tanıma sistemi kurmadan önce, bu sistemin bulundurması gereken özellikleri belirlemeye çalıştı
- ◆ Bunlar:
 - Tek bir noktadan yönetilebiliyor olması (maintenance cost)
 - Veritabanındaki bilgilerin güvenli şekilde saklanıyor olması (encryption)
 - İstemci ile sunucu arasındaki veri akışının güvenli olması (ssl/tls)



BULUNMASI GEREKEN ÖZELLİKLER (devam)

- Sunucunun değişik platformlarda çalışabiliyor olması (portability)
- İstemci program ve kütüphanelerinin bütün kampus platformlarında çalışabiliyor olması (integribility)
- Veritabanı alanları için giriş kuralları tanımlayabilme (access control list)
- Sunucunun dağıtık yapıda çalışabiliyor olup, yük dağıtımını yapabilme (bknz. dns)
- Sunucunun birden fazla klonlanabilip, yine yük dağıtımını yapabilme (replication)



BULUNMASI GEREKEN ÖZELLİKLER (devam)

- Kullanıcı şifrelerinin istemci üzerindeki dosya sisteminde yedeklenmemesi (password caching)
- Ölçeklenebilir olması (scalability)
- Ve GPL’li olması 😊





SEÇİLEN SİSTEM

- ◆ Yukarda anlatılan özellikleri sahip OpenLDAP seçildi
 - LDAP (rfc 1777, 2251, 2829, 3377) protokolü kullanır
 - TCP/IP protokolu üzerinde çalışır
 - Sadece kullanıcı tanımada değil, sorgulama yapılabilecek her türlü dizin servisinde (directory service) başarıyla kullanılmaktadır (host names, mail addresses, addressbook, dns, vb...)
 - OpenLDAP veritabanındaki bilgiler hiyerarşik ağaç yapısı şeklinde tutulur
 - Sorgulamalar DN (distinguished name) kullanılarak yapılır

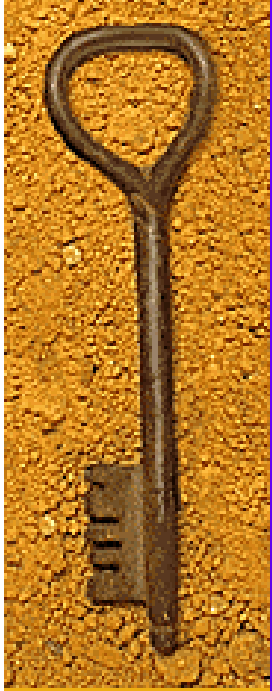
İSTEMCİ YAPILANDIRMASI

- ◆ Linux ve Unix sistemlerde pam_ldap ve nss_ldap kütüphaneleri (<http://www.padl.com>) kullanıldı
- ◆ Windows (2000 ve XP) sistemlerde ise pGINA (<http://pgina.xpasystems.com>) istemcisi kullanıldı
- ◆ İstemci tarafında kullanılan programlar GPL'lidir.



BAŞARIM SEVİYESİ

- ◆ Windows ve Linux istemcilerde kullanıcı tanıma denemeleri başarı ile tamamlandı
- ◆ Pilot uygulama olarak kampüsteki bilgisayar laboratuvarları (windows istemci) kullanılacak



ZAMAN AYIRDIĐINIZ İÇİN

☺ TEŞEKKÜR EDERİM ☺

SORULAR ?