

# Kerberos Kimlik Denetimi Altyapısı



Necdet Yücel

[nyucel~comu.edu.tr](mailto:nyucel~comu.edu.tr)

V. Linux ve Özgür Yazılım Şenliği, ODTÜ



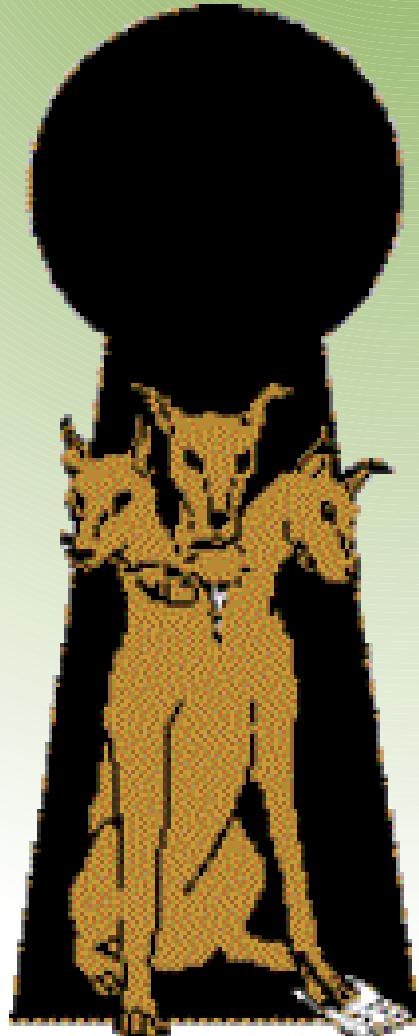
# KAPSAM

- Nedir?
- Nasıl Çalışır?
- Bilet, Oturum Anahtarı, Özel Biletler
- Süreçler
- Ataklar
- Eşzamanlama, Birebir Kopyalama
- Avantajları, dezavantajları



# Kerberos

Yunan mitolojisinde Cehennemin kapısını bekleyen üç başlı dev köpek.

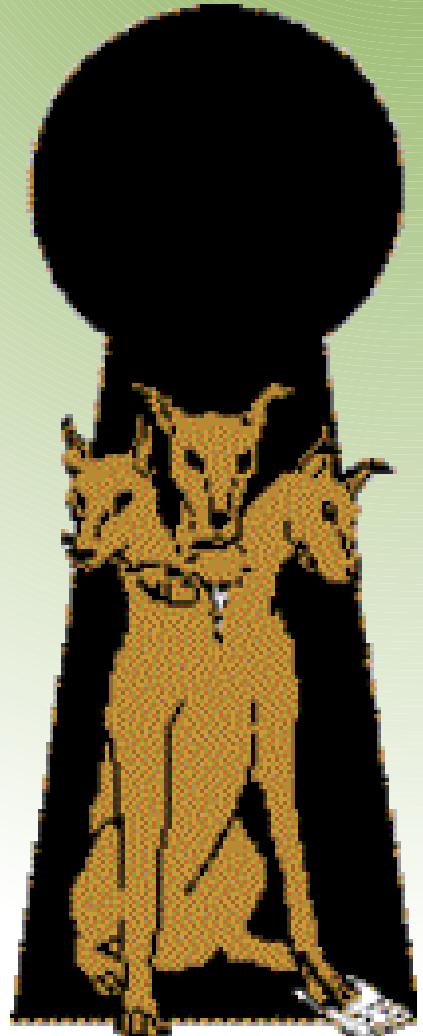


*Ereğli'deki Cehennemağızı Mağarası'nda yaşar.*

*Herkül bu mağaraya gelerek Kerberos'u yakalar ve gücünü ispatlar. Bu Herkül'ün yaşamındaki son güç gösterisi olur.*



# Kerberos



- MIT'de ATHENA projesinin bir parçası olarak geliştirilen bir kimlik denetim sistemidir.
- 1980'lerde, MIT'de kullanıcıların yerleske ağındaki kaynaklara güvenli erişimini sağlamak üzere geliştirilmiştir.
- Aktif olarak geliştirilmektedir.
- Birçok ticari uygulama tarafından kullanılmaktadır.



# Güvenlik

- Internet güvensiz bir yerdir.
- Kullanılan protokollerin çoğu güvenlikle ilgilenmez. (**http, ftp, pop, vs.**)
- Güvenlik duvarları tehlikelerin sadece dışarıdan geldiğini kabul ettikleri için güvenlik sağlamada yetersizdirler.
- Kullanılan yöntemler genellikle kullanıcıları kısıtlama yönündedir.



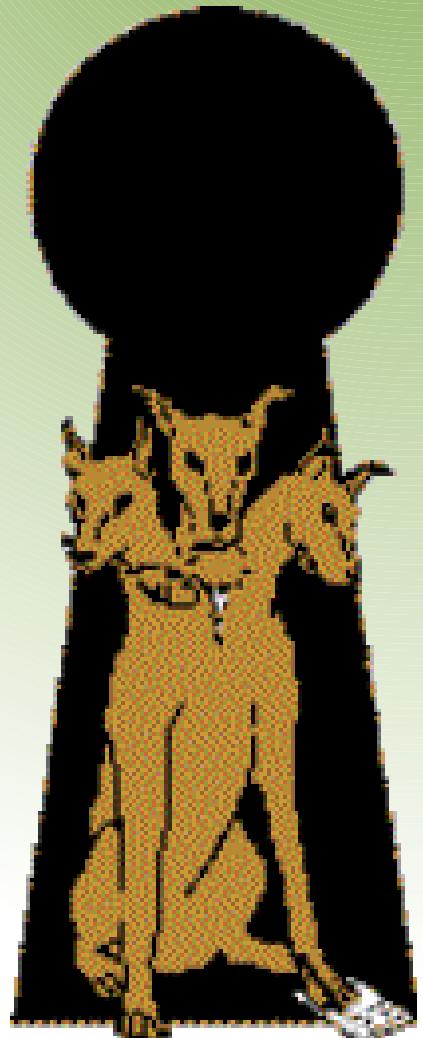
# Güvenlik - 2



Kötü çocukların hepsi ağ dışında  
olmadığından ağ içinde de önlem almak  
gereklidir.



# Güvenlik - 3



- Kerberos ağ güvenlik problemlerinde kullanılabilecek bir çözümdür.
- Güçlü şifreleme kullanır.
- Kaynak kodu açıktır, gerçekte ne yaptığından emin olunabilir.
- Sadece kimlik kanıtlamada değil, güvenli veri alış verisi yapılmasını sağlamada da kullanılır.



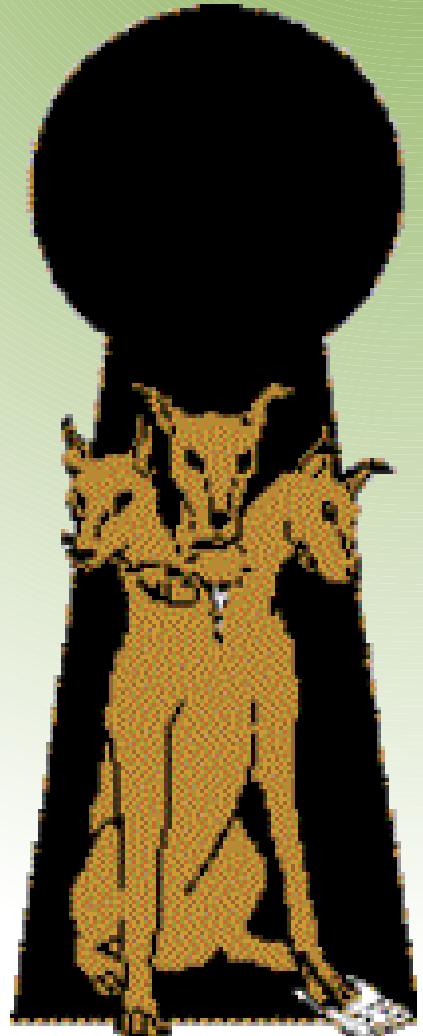
# Kerberos Nasıl Çalışır

- Kerberos istemcilerin kimlik kanıtlamaları için, paylaşılan bir sırrı ve güvenilen bir hakemi kullanır.
- Güvenilen hakem Anahtar Dağıtım Merkezi (**KDC**) olarak bilinen sunucudur.
- Paylaşılan sırrın kullanıcıının kriptografik anahtara dönüştürülmüş parolasıdır.
- Sunucular ve yazılım sistemleri için rasgele anahtarlar üretilir.



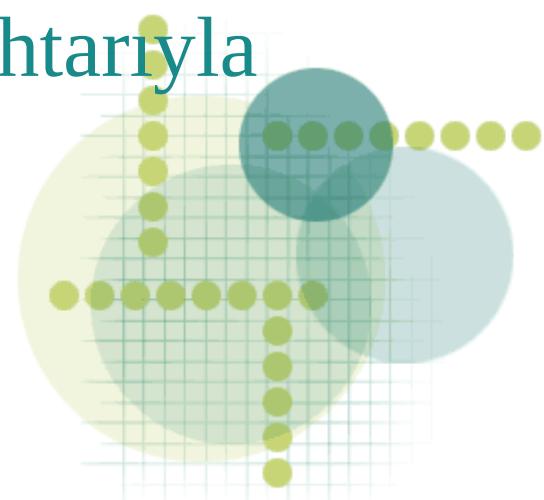
# Kerberos Nasıl Çalışır - 2

- Her kullanıcının bir parolası vardır.
- Her servisin (eposta, print, vs.) bir parolası vardır.
- Bu parolalar sadece yetkili sunucuda tutulur.
- Kimlik kanıtlaması ağda hiç düz metin iletilmeden gerçekleştirilir.



# Kerberos Nasıl Çalışır - 3

- Bir kullanıcı kimliğini bir sistem veya bir servise kanıtlamak isterse KDC'den bir bilet talebinde bulunur.
- Bilet; istemcinin kimliği, oturum anahtarı, zaman bilgisi ve bazı diğer bilgilerden oluşan bir datagramdır.
- Datagram sunucunun gizli anahtarıyla şifrelenir.



**Bilet Sağlama  
Sunucusu**

**Kerberos  
Veritabanı**

**Kimlik Kanitlama  
Sunucusu**

**Sunucu**

**İş istasyonu**

**Kerberos Anahtar Dağıtım Servisi**



# Bilet



- istemci adı (kullanıcı adı)
- sunucu adı
- istemci ağ adresi
- istemci/sunucu için oturum anahtarı
- bilet yaşam süresi
- biletin yaratılma zamanı



# Oturum Anahtarı



- Her oturum için özeldir ve rastgele üretilir.
- İstemcinin sunucuya iletişimini imzalamak için kullanılır.
- Uygulamalar tarafından yanıtları imzalamak için de kullanılabilir.



# Süreçler

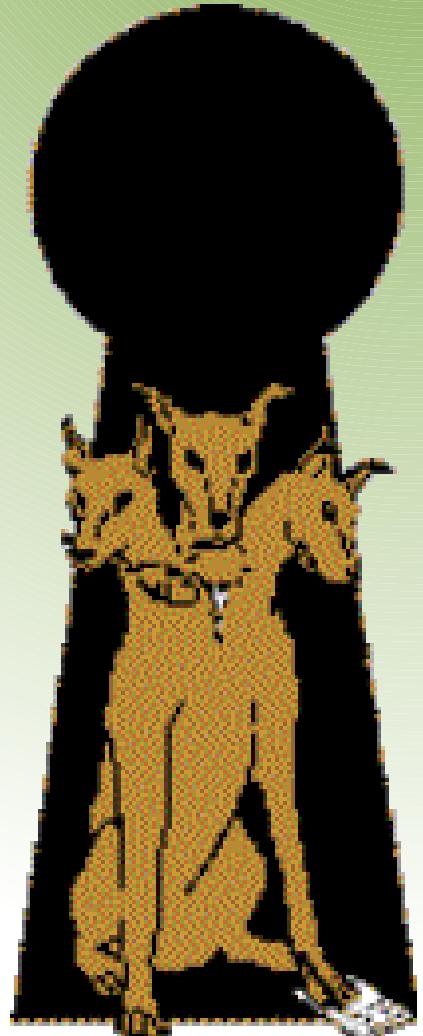
- **KDC** iki önemli Kerberos artalan süreci çalıştırır:
  - **kadmin\***
  - **krb5kdc\***
- **kadmin** Kerberos sunucusunun yönetimle ilgili sürecidir.
- **krb5kdc** Kerberos kimlik denetiminde güvenilen hakem rolünü yerine getirmekle yükümlüdür.

\* çekirdekle ilgili süreçler değildirler.



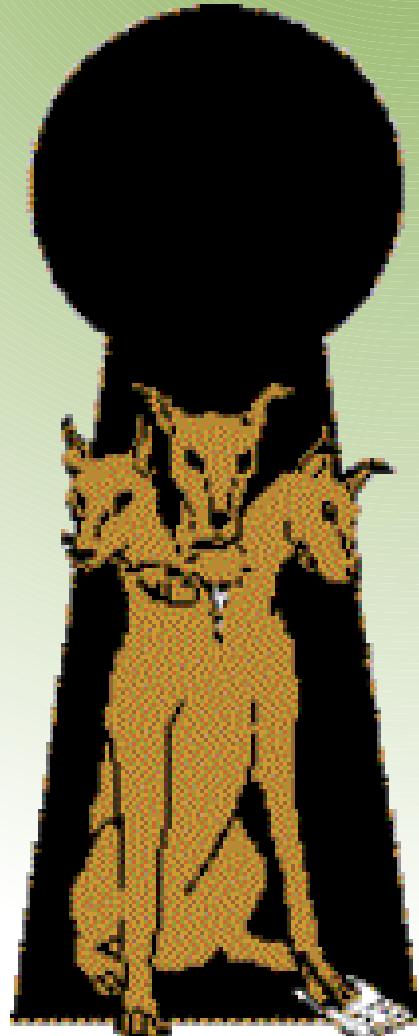
# Süreç Nasıl İşler?

- Kimlik denetim talebi ilk olarak **krb5kdc** artalan sürecine gönderilir.
- Süreç bu isteği aldığında istemciyi esas veritabanından kimlik denetimi yaparak kontrol eder.
- İstemcinin gizli anahtarını bu veritabanından okur ve ona geri göndermek için **Bilet Sağlayan Bilet (TGT)** adında özel bilet olarak şifreler.

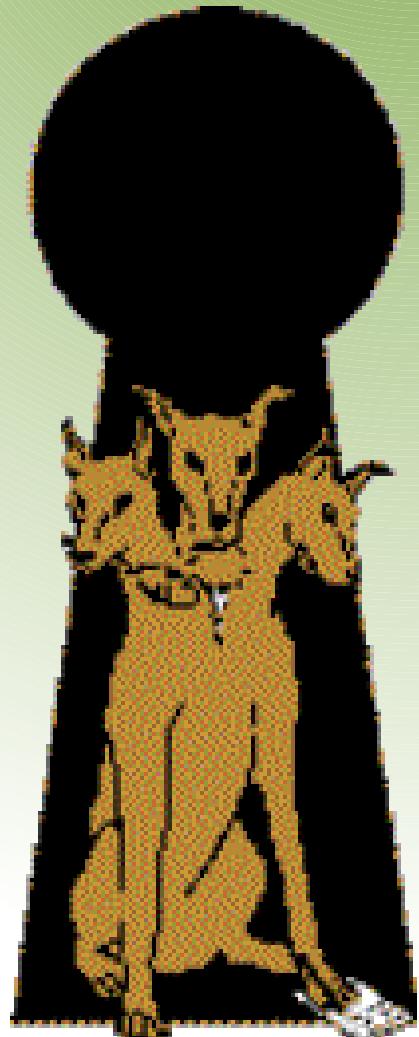


## Süreç Nasıl İşler? - 2

- İstemci oturum anahtarını içeren şifrelenmiş TGT'yi alır.
- Eğer istemci parolayı bilir (gizli anahtar veritabanında tutulur) ve başarıyla TGT'nin şifresini çözebilirse bilet oturum anahtarını da ekleyip şifreleyerek Bilet Sağlama Servisine (TGS) sunar.
- TGS daha sonra istemcinin özel bir sistem veya servisi kullanmasını sağlayacak yeni bir bilet yayınlar.



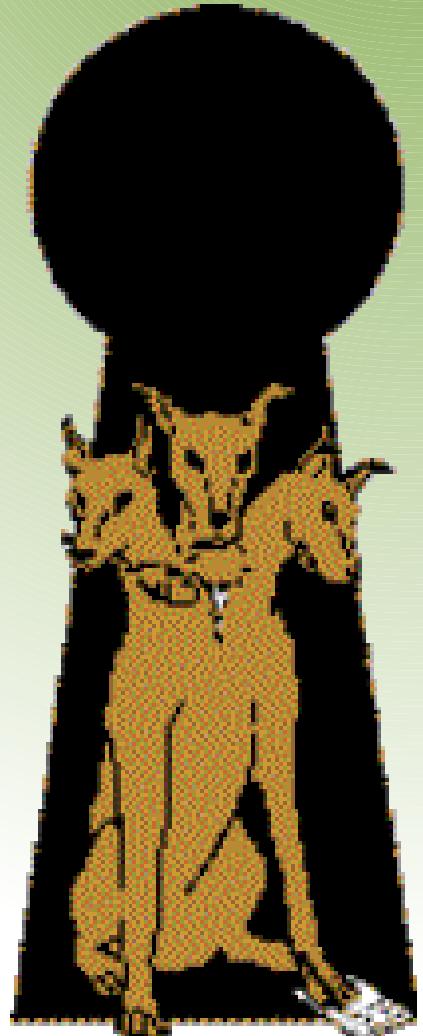
# Süreç Nasıl İşler? - 3



- Sadece gizli anahtarı bilen istemcilerin şifresini çözebileceği şifrelenmiş biletlerin kullanımı sayesinde güvenli kimlik denetimi gerçekleştirilmiş olur.



# Kerberos'un Ele Geçirilmesi



- İlk hedef Kerberos sunucularıdır.
  - Yazılım
  - Parolalar
  - Veri tabanı
- Diğer teknikler
  - tekrarlama atakları
  - parola tahmin atakları



# Ataklar



- Tekrarlama atağı bir Kerberos biletinin durdurulması veya ele geçirilmesi ve ardından sahtekarlıkla yetkisiz erişim kazanmaya çalışmak için kullanılmıştır.
- Parola tahmini bir Kerberos sisteminde ağdaki bütün Kerberos biletlerinin yakalanarak onları desiflemek için mümkün tüm parolaların denenmesidir.



# Güvenlik

- Kerberos KDC servisi verecek sunucu adanmış sunucu olmalıdır.
- Sunucu üzerinde, SSH hariç, başka süreçler çalışmamalıdır.
- Sunucunun fiziksel güvenliği sağlanmalıdır.
- Sunucuyu çalıştıracak işletim sisteminin ve tüm yazılımların güncellemeleri yapılmalıdır.

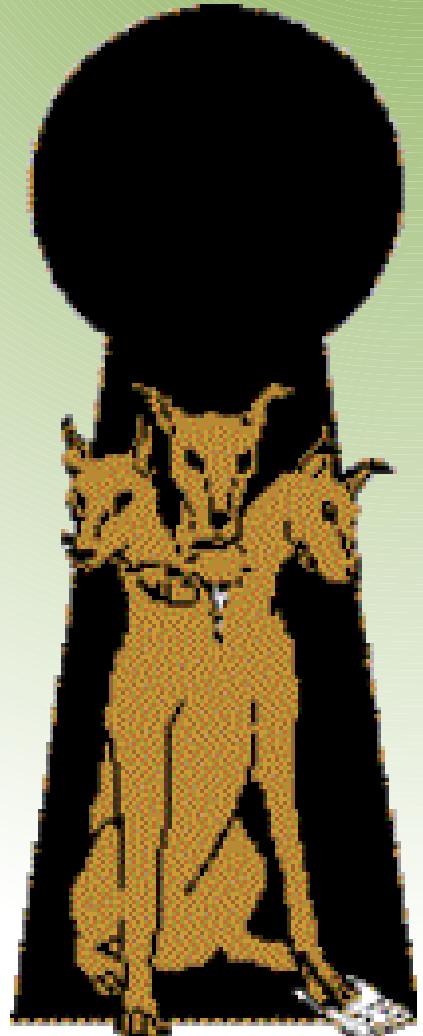


# Güvenlik - 2

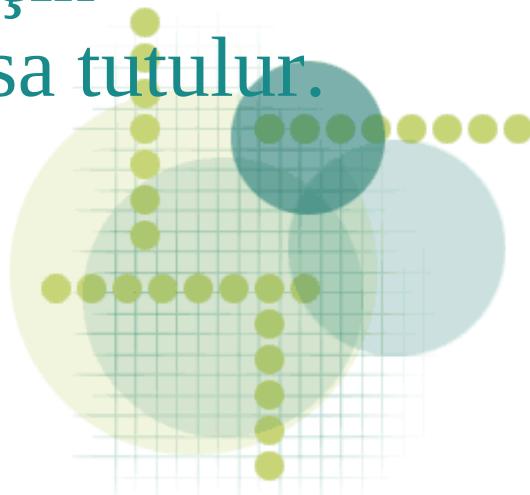
Eğer KDC ele geçirilirse tüm Kerberos  
altyapısı ele geçirilmiş olur!!



# Eşzamanlama

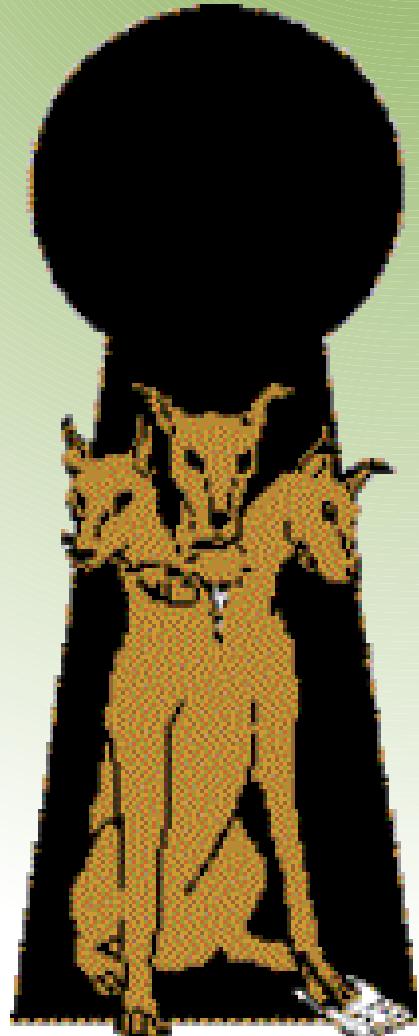


- Kerberos kimlik denetimi kısmen biletlerin zaman bilgisine dayandığı için, Kerberos sunucuların saatlerinin dakik olarak ayarlanması kritik öneme sahiptir.
- Saldırganların tüm parolaları denedikleri veya tekrarlama atağı yaptıkları durumlarda başarısız olmaları için biletlerin yaşam süreleri çok kısa tutulur.



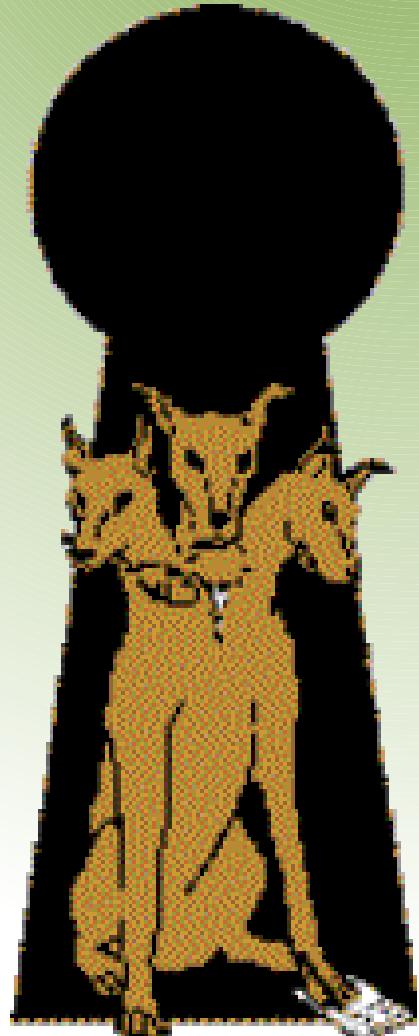
## Eşzamanlama - 2

- Saatlerin birbirinden farklı olmasına izin verilirse, ağ ataklara karşı savunmasız olur.
- Saatler kabul edilebilir bir aralık içinde eşzamanlanmamışsa Kerberos kaçınılmaz hatalar raporlayacak ve çalışmayaçaktır.
- Saati hatalı bir bilgisayardan kimlik doğrulaması yapmaya çalışan istemciler reddedilecektir.



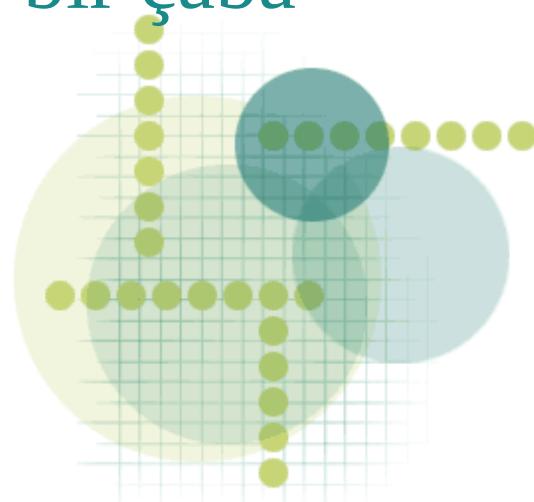
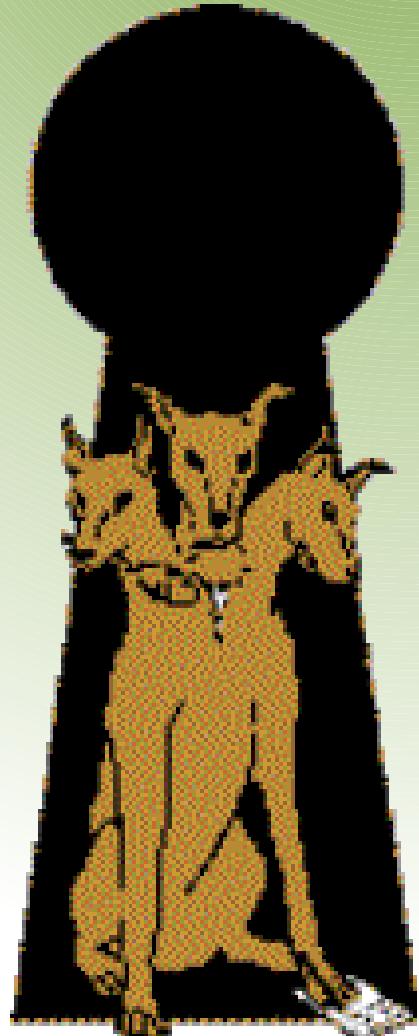
# Birebir Kopyalama

- Kerberos master/slave birebir kopyalama kümelemesine izin verecek şekilde tasarlanmıştır.
- Birincil sunucu olarak bir ana sunucu ve onu yedeklemek için en az bir yardımcı sunucu bulunmalıdır.
- Kerberos sakladığı verileri diğer sunuculara yedekleyecek veya kopyalayacak yazılımları da içerir.

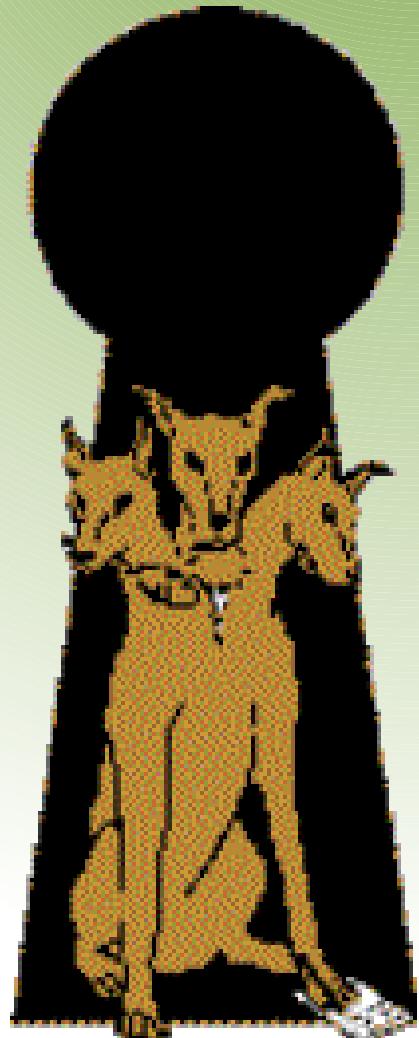


## Birebir Kopyalama - 2

- Kerberos istemci uygulamaları eğer master sunucuya ulaşılamaz ise slave sunucudan kimlik denetimi yapmayı deneyecek şekilde tasarlanmıştır.
- Bir sistem arızası durumunda Kerberos kimlik denetimi servisinin slave sunucudan yapılması için ilave bir çaba harcamaya gerek yoktur.



# Özel Biletler



- **postdatable ticket:**

- Alındığında henüz geçerliliği olmayan ama gelecekte geçerli olacak bilet.
- İleri tarihli görev atamalarında kullanılır.

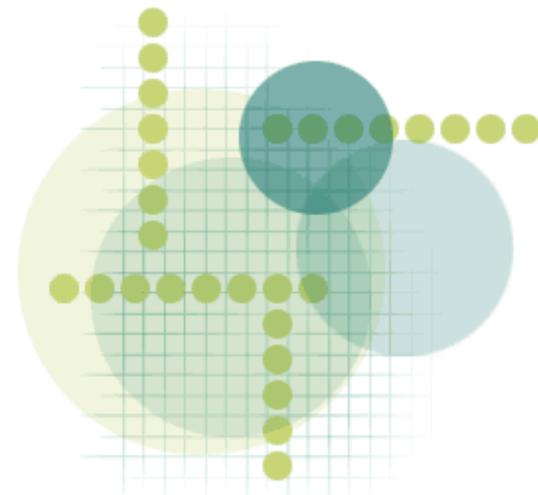


# Özel Biletler - 2



- **renewable ticket:**

- Uzun süreli çalışmalarda kullanılabilen geçerlilik süresi uzatılabilen bilet.
- Biletin bir geçelilik süresi, bir de maksimum yenilenebilme süresi vardır.
- Bilet geçerlilik süresi bitmeden yenilenmelidir.



# Özel Biletler - 3



- **forwardable ticket:**

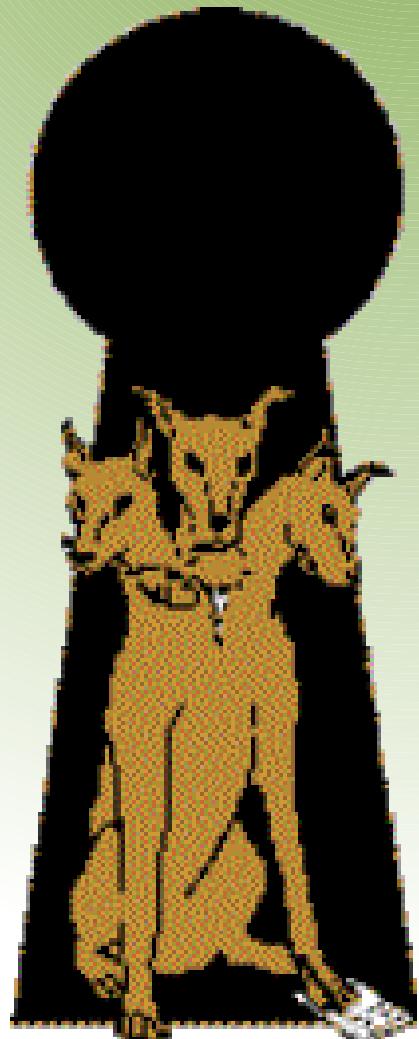
- Normal biletler istemcinin IP adresini de içerirler ve sadece o adresde geçerli olurlar.
- İletilebilir biletler ise birden fazla IP adresinde geçerliliğini sürdürürler.
- Yöneticinin onayı ile verilirler.
- Kullanıcı veya yazılım için kısıtlama yapılabilir.



# Özel Biletler - 4

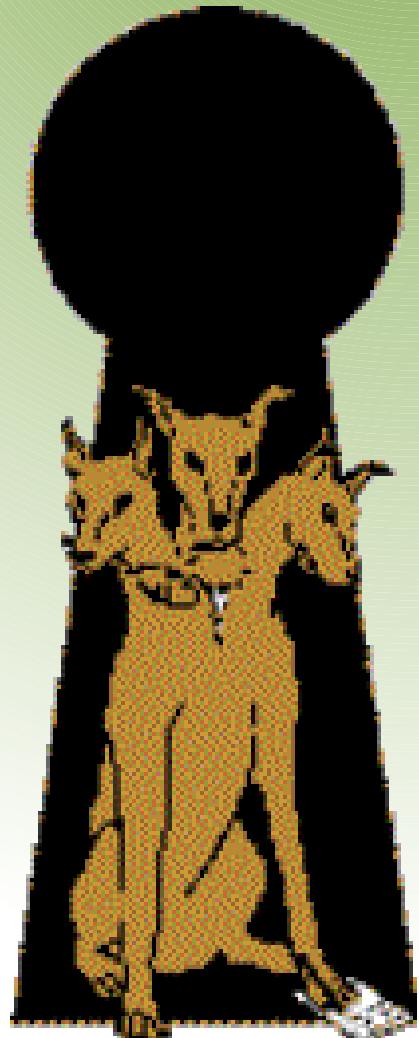
- **proxiable ticket:**

- İletilebilir biletler gibi bir IP adresinden alınan ama başka bir IP adresinde de geçerli olabilen bilet.
- İletilebilir biletlerde istemcinin tüm kimliği yeni bilgisayara aktarılabilirken bu biletlerde sadece kısmi bilgilerin aktarılması mümkündür.
- Pratikte pek sık kullanılmazlar.



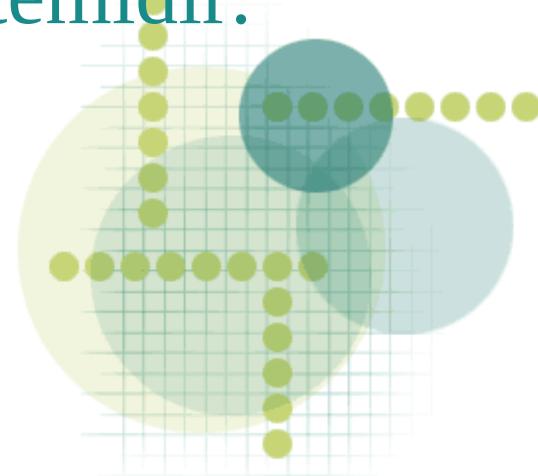
# Kerberos vs. SSL

- **Kerberos:** Gizli anahtarlı, güvenilen üçüncü taraf hakemli
- **SSL:** Açık anahtarlı, sertifika tabanlı



# SSL'in Avantajları

- Güvenilen üçüncü taraf bir hakem'e erişmeye gerek yoktur.
- Taraflardan biri *anahtarı* bilmiyor olsa bile güvenli iletişim kurmak mümkündür.
- Bu iki avantajı sayesinde web iletişimini için ideal kimlik kanıtlama sistemidir.



# Kerberos'un Avantajları



- Anahtar iptal edilebilme
- Anahtar güvenliği
- Kullanım maliyeti
- Açık standartlar
- Esneklik



# KAYNAKLAR

- <http://web.mit.edu/kerberos/www/>
- <http://www.faqs.org/faqs/kerberos-faq/general/preamble.html>
- [www.belgeler.org/howto/kerberos-howto.html](http://www.belgeler.org/howto/kerberos-howto.html)



# LKD

Linux  
Kullanıcıları  
Derneği

