

Bir 802.1x Kimlik Kanıtlama Uygulaması: EDUROAM

Figen Bozkurt
<figen@comu.edu.tr>

Şule Toker
<sule@comu.edu.tr>



Sunum Planı

- 802.1x Nedir?
- EAP ve EAP Türleri
- RADIUS Nedir?
- EDUROAM Nedir?

802.1x Nedir?

802.1x standardı kablosuz yerel ağ (WLAN) teknolojisi için IEEE (The Institute of Electrical and Electronics Engineers) tarafından geliştirilen port tabanlı standartlar ailesidir. 802.1x kimlik doğrulaması, istemci ile erişim noktasına bağlı bir RADIUS sunucusu arasında kullanılan kimlik doğrulamasıdır.

802.1x Kimlik Kanıtlamada kullanılan 4 temel yapı vardır;

- İstemci
- Kimlik kanıtlayıcı (Ağ erişim cihazları)
- Kimlik Kanıtlama Sunucusu
- Kullanıcı bilgilerinin tutulduğu sistem

EAP VE EAP TÜRLERİ

EAP kimlik kanıtama için iyileştirilmiş bir protokoldür, bir kimlik kanıtama yöntemi değildir. İstemci ile sunucu arasında yapılan iletişimde kullanılır.

EAP KİMLİK KANITLAMA YÖNTEMLERİ

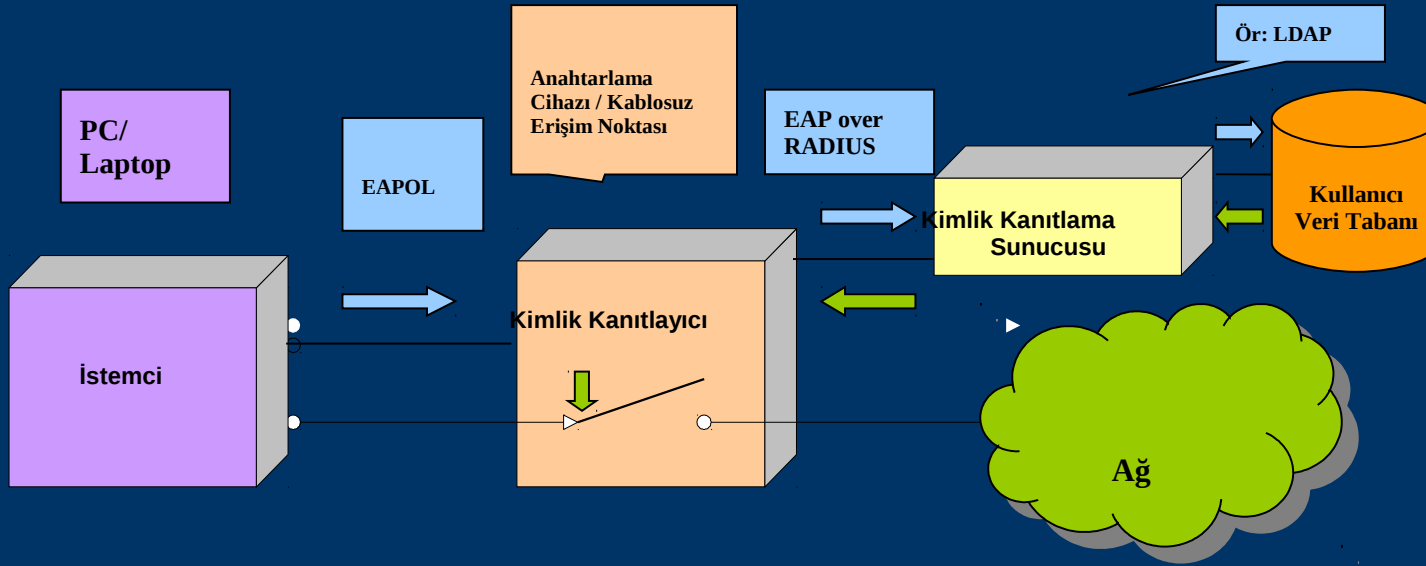
- MD5
- EAP-TLS
- EAP-TTLS
- PEAP (Korumalı EAP)
- LEAP (Hafif EAP)
- EAP-MSCHAPv2

Bunların dışında kırktan fazla EAP kimlik kanıtama yöntemi vardır.

EAP TÜRLERİ

	MD5	TLS	TTLS	PEAP	LEAP
Standart	Açık	Açık	Açık	Açık	Firma
İstemci Sertifikası	-	+	-	-	-
Sunucu Sertifikası	-	+	+	+	-
Güvenlik	Yok	Güçlü	Güçlü	Güçlü	Zayıf
Kullanıcı Veritabanı	"Açık Metin" Parola	<u>"Active Directory"</u>	<u>Token Systems,</u> SQL, LDAP	<u>Active Directory,</u> NT Etki Alanı	<u>Active Directory,</u> NT Etki Alanı
Dinamik Anahtar Değişimi	-	+	+	+	+
Karşılıklı Doğrulama	-	+	+	+	+

802.1x Kullanıcı Kimlik Kanıtlama Mekanizması



RADIUS NEDİR?

Radius (Remote Authentication Dial-In User Service) , kullanıcıların kimlik bilgilerini doğrulayan ve istenen kaynaklara erişim izni veren bir kimlik doğrulama ve hesap yönetimi sistemidir. Uzaktan bağlanan kullanıcılar için kullanıcı ismi-parola doğrulama (authentication), raporlama/erişim süresi (accounting) ve yetkilendirme (authorization) işlemlerini yapar.

Radius IEEE 802.1x (genelde kablosuz ağlarda kullanılan) tarafından kullanılan en yaygın kimlik doğrulama sistemidir.

Radius'un Özellikleri

- Parolaları gizlemek için MD5 hash algoritması kullanılır .
- Genişletilebilir.
- Radius VoIP servis sağlayıcıları tarafından yaygın olarak kullanılır.

RADIUS SUNUCULARI

Açık kaynak kodlu / Özgür yazılım

- FreeRadius
- GNU Radius
- OpenRADIUS
- Cistron RADIUS
- BSDRadius
- TekRADIUS

1. FreeRadius açık kaynak kodlu Radius sunucusudur.
2. Dünya çapında en çok kullanılan Radius sunucusu olarak bilinmektedir.
3. Hızlı, esnek,yapılandırılabilir ve pek çok ticari sunucudan daha çok kimlik kanıtlama protokolünü desteklemektedir.
4. Sunucu, dialupadmin adında PHP tabanlı kullanıcı yönetim aracıyla gelmektedir.
5. LDAP, SQL ve diğer veri tabanlarıyla entegre olmasını sağlayacak modüllerle entegredir. EAP desteği PEAP ile 2001 yılı içinde ve EAP-TTLS desteği de 2003 yılında eklenmiştir.

NEDEN 802.1x?

- Ağa dahil olan kullanıcıların kayıtlarını; yani hangi kullanıcının ne zaman ve nereden ağa erişim sağladığı bilgilerinin tutulabilmesi için kullanıldı.
- 5651 sayılı yasa gereği kullanıcı kayıtlarının en az 2 yıl tutulma zorunluluğundan dolayı.
- EDUROAM ailesine dahil olabilmek için.

802.1x Alternatifleri

- Active Directory
 - Kerberos
 - NTLM (NT LAN Manager)
-
-

EDUROAM NEDİR?

Education Roaming kelimelerinin kısaltması olan Eduroam yani eğitim gezintisi, RADIUS tabanlı altyapı üzerinden 802.1x güvenlik teknolojisini kullanarak eduroam üyesi kurumlar arasında sorunsuzca ağ kullanımına olanak sağlamaktadır.

Eduroam üyesi kurumların kullanıcıları kendi kurumlarında ağa bağlanmak için kullandıkları kullanıcı adı ve parola ile yine eduroam üyesi bir başka kurumdan ağa bağlanabilirler.

Kullanıcı misafir kurumda iken aldığı eduroam yayınına bağlantı talebi yolladığında, misafir kurumun yetkilendirme sunucusu , kullanıcıyı kendi ev kurumunun yetkilendirme sunucusuna yönlendirerek, yetkili olup olmadığını belirler.

Bu sorgulamaların ,sunucular arasında oluşturulan şifreli bir tünel içinde yapılır. Kullanıcıların yapması gereken şey misafir olduğu kurumda yer alan eduroam kablosuz ağını, kendi kurumunun ağına bağlanır gibi tanımlamasıdır.

EDUROAM ÜYESİ AVRUPA FEDERASYONLARI



EDUROAM TÜRKİYE ÜYELERİ HARİTASI

