KABLOSUZ AĞLARDA EAP TABANLI BİR KİMLİK DOĞRULAMA PROTOKOLÜ

Çağdaş Kurt

YÜKSEK LİSANS TEZİ

BİLGİSAYAR BİLİMLERİ

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

OCAK 2013

ANKARA

Çağdaş KURT tarafından hazırlanan KABLOSUZ AĞLARDA EAP TABANLI BİR KİMLİK DOĞRULAMA PROTOKOLÜ adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Doç.Dr. SUAT ÖZDEMİR
Tez Yöneticisi

Bu çalışma, jurimiz tarafından oy birliği ile Bilgisayar Bilimleri Anabilim Dalında Yüksek lisans tezi olarak kabul edilmiştir.

Başkan : Prof. Dr. M.Ali AKCAYOL

Üye : Doç. Dr. Suat ÖZDEMİR

Üye : Yard. Doç. Dr. Hüseyin POLAT

Tarih : 31.01.2013

Bu tez, Gazi Üniversitesi Bilişim Enstitüsü tez yazım kurallarına uygundur.

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

Çağdaş KURT

KABLOSUZ AĞLARDA EAP TABANLI BİR KİMLİK DOĞRULAMA PROTOKOLÜ

(Yüksek Lisans Tezi)

Çağdaş KURT

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Ocak 2013

ÖZET

İletim ortamı olarak havanın kullanılmasından dolayı kablosuz ağlar saldırılara karşı elverişli olmaktadır. Bundan dolayı kablosuz ağlarda güvenlik kablolu ağlardakine göre daha karmaşık hal almaktadır. Kablosuz ağlarda sunulan servislere ve ağ kaynaklarına sadece geçerli kullanıcıların erişebilmesini sağlamada kimlik doğrulama en önemli yöntemdir. Korumalı Genişletilebilir Kimlik Doğrulama Protokolü (PEAP) kablosuz ağlarda kimlik asıllaması için yaygın kullanılan güvenli bir protokoldür. Ancak, yapılan araştırma ve incelemelerde PEAP'ın kimlik bilgilerini gizlemede zayıf olduğu görülmüştür. Bu çalışmada, kablosuz ağlarda kimlik doğrulama esnasında kimlik bilgilerinin gizliliğini sağlamak için yeni bir protokol geliştirilmiştir. Bu metot, PEAP'ın yönetim kolaylığı, güçlü güvenlik özellikleri ile dinamik anahtar dağıtımının sağladığı avantajlarını içermektedir.

Bilim Kodu : **902.1.014**
Anahtar Kelime : **kablosuz ağ güvenliği, kimlik doğrulama, şifreleme, peap**
Sayfa Adedi : **52**
Tez Yöneticisi : **Doç. Dr. Suat ÖZDEMİR**

AN EAP BASED AUTHENTICATION PROTOCOL FOR WIRELESS LOCAL AREA NETWORKS

(M.Sc. Thesis)

Çağdaş KURT

GAZİ UNIVERSITY

INFORMATICS INSTITUTE

January 2013

ABSTRACT

Wireless networks are susceptible to security attacks due to their open transmission media. Therefore, wireless network security is somewhat more complex than that of wired network security. In wireless network security, authentication is the most essential procedure to ensure that the service is properly used by the intended users. Protected Extensible Authentication Protocol (PEAP) is widely being used in wireless networks. However, PEAP is shown to be a weak protocol in terms of protection of user identity. In this paper, we designed and implemented a new and efficient wireless authentication protocol providing user identity secrecy. This metot takes advantage of PEAP's management easiness and the robustness of dynamic key distribution to provide user identity protection.

Science Code : **902.1.014**
Key Words : **wireless security, authentication, encryption, peap**
Page Number : **52**
Adviser : **Assoc. Prof. Dr. Suat ÖZDEMİR**

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla bana yol gösteren ve benim bu alanda gelişmemi sağlayan Danışman Hocam Sayın Doç.Dr. Suat ÖZDEMİR'e, Lisans ve Yüksek Lisans öğrenimim boyunca desteklerini esirgemeyen değerli hocalarım Prof.Dr. M. Ali AKÇAYOL ve Yrd.Doç.Dr. Hüseyin POLAT'a, maddi manevi her türlü destekleriyle her zaman yanımda olan aileme teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

ÖZET…….....iv
ABSTRACT…….....v
TEŞEKKÜR…….....vi
İÇİNDEKİLER…….....vii
ÇİZELGELERİN LİSTESİ……..…….....ix
ŞEKİLLERİN LİSTESİ……...…….....x
SİMGELER VE KISALTMALAR……...…….....xi
1. GİRİŞ……...…….....1
2. KABLOSUZ YEREL AĞLARDA GÜVENLİK……...…….....7
2.1. CIA……...…….....8
2.1.1. Gizlilik …...……...…….....8
2.1.2. Bütünlük…...…….....9
2.1.3. Kullanılabilirlik…….....9
2.2. AAA……...…….....9
2.2.1. Yetkilendirme……...…….....10
2.2.2. Loglama……...…….....10
2.2.3. Kimlik doğrulama…….…….....10
2.3. 802.1X…….……...…….....11
2.3.1. 802.1X bileşenleri…….....14
2.4. SSL……..…….…….....15
2.5. Sertifika…….....17
3. EAP…….....21
3.1. Kablosuz Ağlarda Olması Beklenen Güvenlik Özellikleri…..…...…….....23
3.1.1. Karşılıklı kimlik doğrulama…….…….…….....23
3.1.2. Kimlik gizliliği……..…….....23
3.1.3. Sözlük atağı dayanıklılığı …….…….....24
3.1.4. Tekrar atağı dayanıklılığı …….…….....24
3.1.5. Güçlü anahtar üretimi…….…….....24
3.1.6. Test……...…….....25
3.1.7. Hızlı yeniden bağlanma…….…….....25

3.2. EAP Tabanlı Kimlik Doğrulama Protokolleri……..…….....25
3.2.1. EAP-MD5……...…….....25
3.2.2. EAP-FAST……...…….....26
3.2.3. LEAP …….....26
3.2.4. EAP- TLS……...…….....27
3.2.5. EAP-TTLS ……...…….....28
3.2.6. PEAP…….....28
4. GELİŞTİRİLEN PROTOKOL : E-PEAP……..…...…….....35
4.1. Çerçeve Mimarisi……..…….....35
4.2. Protokolün Çalışması……..…..…….....36
4.3. E-PEAP Geliştirmeleri……..…..…….....39
5. PROTOKOLÜN UYGULAMASI…….…...…….....40
5.1. OPENSSL ile Sunucu Sertifikasının Oluşturulması…….....40
5.2. OPENSSL Kurulumu…….....40
5.3. Sertifikalar…….…….....41
5.3.1. CA sertifikasının oluşturulması ve imzalanması……..…….....41
5.3.2. Sunucu sertifikasının oluşturulması ve imzalanması…...…..…….....41
5.3.3. Sertifikanın testi……..…….....41
5.4. Kablosuz Adaptör Kurulumu……..…….....41
5.5. Hostapd ve Wpa_supplicant…….…..…….....42
5.5.1. Hostapd kurulumu ve E-PEAP konfigürasyonu……..…….....42
5.5.2. WPA_Supplicant kurulumu ve E-PEAP konfigürasyonu…….....43
5.6. DHCP Konfigürasyonu…….…….....44
5.7. Deneysel Sonuçlar ve Güvenlik Analizi…….…….....44
5.7.1. Güvenlik analizi……..…….....48
6. SONUÇ VE ÖNERİLER…….....50
KAYNAKLAR…….....51
ÖZGEÇMİŞ…….....54

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge 3.1. PEAP'ta kullanılan kimlik doğrulama yönteminin özellikleri ……..…….. 34

Çizelge 5.1. Protokollerin güvenlik incelemesi…….……...……. 49

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil 2.1. CIA kavram haritası……...…...…….……..…. 8
Şekil 2.2. 802.1X mimarisi...……..……...…… 12
Şekil 2.3. 802.1X'te port durumları ..…...……..…….. 14
Şekil 2.4. SSL tünelinin kurulma aşamaları……..…… 17
Şekil 3.1. EAP başlık yapısı...……...…...……..…. 22
Şekil 3.2. Katmansal EAP hiyerarşisi...…..……..…… 22
Şekil 3.3. Faz-1'de TLS tünelinin kurulması……..…….. 31
Şekil 3.4. Faz-2'de kimlik doğrulamanın gerçekleşmesi ….…… 32
Şekil 3.5. PEAP fazları……...…..…… 34
Şekil 4.1. Değiştirilmiş EAP çerçevesi.....……..……. 36
Şekil 4.2. E-PEAP'ın EAP'a entegrasyonu……..…… 38
Şekil 4.3. Şifreleme anahtarları ve S değerlerinin yer aldığı veritabanları...…….... 39
Şekil 5.1. Test topolojisi……....…….. 45
Şekil 5.2. Rastgele S değeri içeren EAP-İstek paketi…...……..……..…46
Şekil 5.3. Şifreli kimlik bilgisi taşıyan EAP-Cevap paketi ...……..…… 47
Şekil 5.4. Kimliği doğrulanan istemciye otomatik IP atanması.……..…… 47

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklama
AAA	Kimlik Doğrulama, Yetkilendirme, Loglama
CIA	Gizlilik, Bütünlük, Kullanılabilirlik
DHCP	Dinamik Host Konfigürasyon Protokolü
EAP	Genişletilmiş Kimlik Doğrulama Protokolü
EAPOL	Yerel Ağlarda Genişletilmiş Kimlik Doğrulama Protokolü
IEFT	İnternet Mühendisliği Görev Gücü
MSCHAP	Microsoft Karşılıklı Kimlik Doğrulama Protokolü
PEAP	Genişletilmiş Korumalı Kimlik Doğrulama Protokolü
SSL	Güvenli Soket Katmanı
TLS	Taşıma Katmanı Güvenliği
TTLS	Tünellenmiş Taşıma Katmanı Güvenliği
WEP	Kablo Eşdeğerlikli Koruma
WLAN	Kablosuz Yerel Alan Ağı

1. GİRİŞ

Kablosuz Yerel Alan Ağları günümüzde gelişen ağ iletişim teknolojilerine paralel hızda büyümekte ve özellikle iş dünyasında ve bilgisayar sektöründe popülerliği artmaktadır. Tüm ortamlarda verimlilik ve üretkenliği arttırmak, mobiliteden kaynaklanan esnekliği sağlamak, yedekleme amaçlı olarak ve kablolama zorluğunun bulunduğu yerlerde kablosuz olarak erişilebilirliği devam ettirebilmek için kablosuz ağlar yaygın olarak kullanılmaktadır.

Kablosuz ağlar artık ağ teknolojileri içinde çok önemli bir yer tutmakta, bilgisayar ve iş endüstrisinde hızla yükselip oldukça yaygın hale gelmektedir. Özellikle IEEE tarafından geliştirilen 802.11 ağlar gibi WLAN(Wireless Local Area Networks-Kablosuz Yerel Alan Ağları) sistemleri özel veya genel kullanıma açık ortamlarda ortak erişim alanı haline gelmektedir. Hareket özgürlüğü ve uygulanmasındaki basitlik ile WLAN sistemleri iş ve ev uygulamalarında hızla yaygınlaşmıştır. WLAN sistemleri iş adamları, yöneticiler, çalışanlar, küçük işletmeler, orta ölçekli işletmeler ve bireysel kullanıcılar gibi büyük bir kesime, internet ve üyesi oldukları kurumsal ağa kablosuz bağlanma imkânı sağlamaktadır. Kablolu ağların tüm özelliklerine sahip olan WLAN sistemleri bu ağların devamı ya da alternatifi olarak kullanılmaktadırlar. Kurumsal ve kişisel kullanımın dışında restoranlar, otobüs terminalleri, oteller, büyük alışveriş merkezleri, tren istasyonları, hava alanları cadde ve sokaklar gibi kamuya açık alanlarda erişim alanları vasıtasıyla verilen kablosuz internet hizmetinin de hızla artmakta olduğu görülmektedir. WLAN sistemlerin kullanımının hızla artması beraberinde bu ağların güvenilirlik seviyelerinin irdelenmesine sebep olmuştur.

Kablosuz iletişim teknolojisi, en basit tanımıyla, noktadan noktaya veya ağ yapısı şeklinde bağlantı sağlayan bir teknolojidir. Bu açıdan bakıldığında, kablosuz iletişim teknolojisi, günümüzde yaygın olarak kullanılan kablolu veya fiber optik iletişim yapılarıyla benzerlik göstermektedir. Kablosuz iletişim teknolojisini diğerlerinden ayıran nokta ise; iletim ortamı olarak havayı kullanmasıdır.

Kablosuz ağlardaki güvenlik riskleri kablolu ağlardaki risklerle aynıdır fakat bunlara iletim ortamı olarak hava kullanmaktan kaynaklanan yeni riskler de eklenmiştir. Sinyalin havanın götürebildiği yere kadar gidebilmesi ve muhtemel veri hırsızlığı saldırılarına açık olması, kablosuz iletişim sistemlerindeki veri güvenliğini, bilgisayar sistemlerinin güvenli biçimde kullanılmasını ve organizasyonların en önemli varlığı haline gelen bilginin en iyi şekilde korunmasını sağlamak da önem kazanmaktadır [27].

Sayısal ortamlarda verilerin korunmasına ilişkin oluşan bilgi güvenliği kavramı, bilgi varlıklarının ortamdaki tehditlerden, zarar görmeden kullanılabilmesi üzerinde çalışır. Bilgi güvenliğinin temel amacı, elektronik ve/veya diğer ortamlarda bulunan her türlü bilginin; gizliliğin, bütünlüğünü, kullanılabilirliğini sürekli olarak sağlamaktır. Kablosuz ağı kullanan kullanıcılara ait kullanıcı adı, parola, yüksek güvenlik seviyesi gerektiren, özel veya hassas veriler gibi gizli bilgileri korumak, kablosuz iletişim ortamına yetkisiz erişim, iletişim, modifikasyon ve veri tekrarı dinlemelerini, hizmet reddi ve paket üretimi gibi tehditlere karşı savunmak, güvenli olduğunu iddia eden kablosuz ağ protokollerinin sağlaması gereken özelliklerdir.

Kablosuz ortamlarda bu özellikleri sağlamak, güvenlik risklerini azaltmak ve iletişimin hava ortamında kontrolsüz bir şekilde gerçekleştiği WLAN sistemlerinde güvenliği sağlayabilmek ve kablosuz ağ kullanıcıları için daha fazla esneklik sağlamak için IEEE, 2001 yılı Haziran ayında 802.1X protokolünü [1] tanıtmıştır. Bu standart, Internet Engineering Task Force (IETF) tarafından geliştirilen, Genişletilebilir Kimlik Doğrulama Protokolü'nü (EAP) [2] tanımlamaktadır. EAP, RFC'de "EAP çoklu kimlik kanıtlama yöntemlerini destekleyen ve tipik olarak noktadan noktaya (PPP) [13] veya IEEE 802 gibi veri bağlantı katmanı protokolleri üzerinde IP'ye ihtiyaç duymadan doğrudan çalışır" şeklinde tanımlanmaktadır.

EAP'ın başarısı, EAP'ın kendisi ve kullanmakta olduğu EAP tabanlı yöntemler arasındaki ilişkiden kaynaklanır. EAP'ın temel işlevi kimlik doğrulaması için kullanılan gizli verileri (kullanıcı adı, parola, sertifika vb) taşımaktır. EAP yöntemleri ise kimlik doğrulama sürecinden sorumludur. EAP içerisinde ihtiyaçlara

göre istenen kimlik doğrulama protokolü kullanılabilir. Kullanılacak kimlik doğrulama protokolleri EAP'tan bağımsızdır. Bu, kimlik doğrulama protokolünde bir açıklık veya zaafiyet keşfedildiği zaman güvenlik platformunu (EAP) değiştirmeden hatalı yöntemi değiştirebilme esnekliği sağlar.

Bir kablosuz iletişim sisteminin güvenlik gereksinimleri açık alanda akan verilerin gizliliğini, kullanıcı bilgileri gizliliğini ve en önemlisi de kullanıcı kimlik doğrulamayı sağlamayı içerir [14]. Kablosuz sistemlerde kullanıcı gizliliği sağlamak, veri gizliliği, bütünlüğü, tazeliğini ve güvenliği artırmak için birçok doğrulama protokolleri önerilmiştir. Şu anda 40'dan fazla EAP tabanlı kimlik doğrulama yöntemleri vardır, ancak bunların altısı IETF tarafından standardize edilmiştir [3].

Bu amaçla geliştirilen EAP-TLS protokolü [4], bir IETF standardıdır. Metot, güvenli kimlik denetimi için TLS (Transport Layer Security) [5] protokolünü kullanır. TLS'in temeli, güvenli web oturumları sağlamak için kullanılan SSL (Security Socket Layer) protokolüne dayanır. EAP-TLS kimlik denetimi için X.509 dijital sertifikaları kullanır. Bu yüzden her Erişim Noktası (AP) ve kullanıcının sertifika otoritesi tarafından üretilmiş bir sertifikaya ihtiyacı vardır. Dijital sertifikalar bir kayıt defterinde veya akıllı kart gibi bir cihazda saklanır. EAP-TLS; sunucu, kullanıcıyı her kimlik denetiminden geçmeye zorladığında otomatik olarak WEP anahtarı üreterek veri güvenliğini de sağlar. Kimlik denetiminden geçen her kullanıcıda WEP anahtarını üretmek için TLS oturum anahtarı kullanılır ve veri güvenliği sağlanır.

EAP-TLS'e alternatif olan EAP-TTLS [6] kimlik denetim sisteminde kimlik doğrulama bilgisinin güvenli bir şekilde iletilebilmesi için istemci ile sunucu arasında TLS ile şifreli bir oturum oluşturulur. Sorgulama ve yanıt paketleri, herkese açık olmayan TLS şifreli bir kanal üzerinden gönderilir. Bunun için sucunu için tek bir anahtar çifti oluşturulur. İstemci rasgele oluşturduğu anahtarı kendi açık anahtarı ile şifreleyip sunucuya yollar. Bundan sonraki haberleşme bu yeni ortak anahtar ile simetrik şifreleme ile devam eder. RADIUS sunucusu, istemcinin kimliğini kendisine gönderdiği kimlik doğrulama verisi ile doğrularken, sunucu da sunucu

sertifikası aracılığı ile doğrulama yapmaya yetkili olduğunu kanıtlar. Böylece, tek bir sunucu sertifikası ve kullanıcı adı/parola verisi kullanılarak, çift yönlü doğrulama gerçekleşmiş olur. EAP-TLS'ten farklı olarak Faz-2'de her zaman mutlaka ikinci bir kimlik doğrulama yöntemi (inner metot) kullanılması gerekir

EAP-Fast[7], Cisco tarafından, yönetimsel karışıklıkları azaltmak için geliştirilmiş, esnek bir protokoldür. Kullanıcıların dijital sertifikalar kullanmasına ve güçlü şifre kurallarına gerek yoktur. EAP-Fast ile kimlik denetim sunucusu ve kullanıcı arasında güvenli bir tünel oluşturulur. Tüneli oluşturmak için PAC (Protected Access Crediental) adında bir referansa ihtiyaç duyular. PAC, bir PAC sunucusu vasıtasıyla veya EAP-FAST fazlarında dinamik olarak oluşturulabilir. Tünel bir kez kurulduğunda, kullanıcılar kullanıcı adı ve şifreleriyle kimlik denetiminden geçerler.
LEAP [8], Cisco tarafından geliştirilmiş diğer bir protokol olup, AP'ler kullanıcıların kimlik denetimlerini bir RADIUS (Remote Authentication In User Server/Service) [30] sunucusu üzerinden gerçekleştirirler. Bu protokol ağırlıklı olarak düşük kaynaklara sahip veya kimlik doğrulamasının hızlı geçilmesi gereken cihazlarda kullanıldığından EAP-Fast'teki gibi güvenli bir tünel oluşturulmaz. Kimlik denetimi için kullanıcı adı ve şifre kullanılır. LEAP ayrıca WEP'i kullanarak veri güvenliğini de sağlar. Her kablosuz ağ kullanıcısı için dinamik olarak RADIUS sunucu tarafından bir WPA anahtarı üretilir. Böylece kullanıcı bazlı veri güvenliği sağlanmış olur.

PEAP [9], bir standart olarak Cisco Systems, Microsoft ve RSA [29] tarafından önerilmiş bir başka güçlü kimlik doğrulama protokolüdür. Kimlik doğrulama işleminin güvenli, hızlı ve pratik şekilde yapılmasını amaçlar. EAP-TLS protokolüne benzer. Farklı olarak sunucu, kullanıcıyı dijital bir sertifika ile asıllamaz. Bunun yerine tek kullanımlık şifre gibi değişik yöntemler kullanılır. PEAP temel olarak iki kısımdan oluşur. Faz-1 olarak adlandırılan birinci kısımda, bir Aktarım Katmanı Güvenliği (TLS) oturumu başlatılmadan, sunucu istemcinin kimlik doğrulamasını yapar. Bu fazda ayrıca güvenli TLS kanalın oluşturulması için gereken parametreler üzerinde anlaşma sağlanır. Veriler Faz-1'de şifrelenmeden alınıp gönderilir. Kurulması istenen tünel parametreleri üzerinde anlaşmanın sağlanmasının ardından,

konuşmanın geri kalanı şifrelenerek aktarılır. İstemci kimlik doğrulaması sağlanmadığı sürece Faz-2'ye geçilmez, TLS tüneli içinden EAP görüşmelerine başlanmaz.

PEAP protokolünün Faz-2 evresinde EAP-Request/Identity ve EAP-Response/Identity paketleri ve içerikleri güvenli TLS tüneli içerisinde şifrelenerek gönderildiğinden kullanıcıların kimlikleri için gizlilik sağlanmış olur. Ancak, Faz 1 için kimlik bilgilerinin saklanması kullanıcıların kendi insiyatiflerine bağlıdır. Ağa bağlanmak isteyen kullanıcının her defasında gerçek kimlik bilgisi yerine sahte kimlik bilgisi vermesi gerekmektedir. Çok pratik olmayan bu yöntemde, kullanıcılar sahte kimlik ayarlaması yapmadığı takdirde art niyetli kişiler gerçek kimlik bilgilerine ulaşabilecek, bu da ağda bir zaafiyete yol açacaktır. Faz-1'de kullanıcı bilgisinin ataklar ile ele geçirilebileceği ileriki bölümlerde ayrıntılı olarak anlatılmış, literatürdeki çalışmalarda dile getirilmiştir [24-26].

Bu tez çalışmasında, güvenli olduğu iddia edilen kablosuz bir ağın hangi özellikleri barındırması gerektiği tanımlanmış, literatürde yaygın olarak kullanılan kimlik doğrulama protokollerinin güçlü ve zayıf yönleri irdelenmiş, güvenlik gereksinimlerini büyük ölçüde karşılayan PEAP'ın kablosuz ortamda şifrelenmeden gidip gelen Faz-1 kullanıcı bilgisinin daha güvenli iletimi için geliştirilen, dinamik anahtar yönetimiyle semantik güvenlikli şifreleme yapan, ağ güvenlik seviyesini kullanıcı inisiyatifinden ayrıştıran, hızlı, kullanışlı, pratik bir kimlik doğrulama yöntemi önerilmiş, gerçek ortamda uygulanmış, verimliliği ve sağladığı güvenlik yararları incelenmiştir.

Önerilen protokol, PEAP ile entegre edilmiştir. PEAP, TLS şifreli kanalı aracılığıyla Genişletilebilir Kimlik Doğrulama Protokolü-Microsoft Karşılıklı Kimlik Doğrulama Protokolü (EAP-MSCHAPv2) gibi güvenli kimlik doğrulama yöntemi ile birlikte çalışabilir. Bu da, kullanıcı bilgilerinin kimlik doğrulama sunucusuna güvenli bir şekilde ulaştırılmasını sağlar. PEAP tarafından oluşturulan TLS kanalı, bir saldırganın istemci ile erişim noktası arasında paket sızdırarak güvenlik zaafiyetleri yaratmasına engel olur. Şifreli TLS kanalı ayrıca kimlik doğrulama sunucusuna

yapılacak DoS saldırılarının engellenmesine yardımcı olur. Önerilen çözüm, dinamik anahtar dağıtımı ve PEAP'ın bu güçlü yanlarını barındırmaktadır.

Konunun daha iyi anlaşılması için, ikinci bölümde; bilgi güvenliği kapsamında güvenlik kavramının tanımı yapılmış, kablosuz ağ güvenliği yetkilendirme, loglama ve kimlik doğrulama açısından incelenmiştir. Daha sonra protokollerde kullanılan sertifika ve tünel mekanizmalarından bahsedilmiş, kablosuz yerel alan ağlarında temel kimlik doğrulama protokolü olarak nitelendirilebilecek olan 802.1X ve bu sistemin bileşenleri ayrıntılı olarak verilmiştir.

Üçüncü bölümde; 802.1X altyapısını kullanarak geliştirilmiş olan EAP metodolojisi hakkında detaylı bilgi verilmiştir. Güvenli bir kablosuz bir ağdan beklenen güvenlik özellikleri ayrıntılı olarak anlatılmış, bu gereksinimleri karşılamaya çalışan EAP temelli kimlik doğrulama protokolleri analiz edilmiştir.

Dördüncü bölümde; geliştirilen protokol E-PEAP'ın çerçeve mimarisi, protokolün çalışma yapısı ve yapılan geliştirmeler ayrıntılı olarak sunulmuştur. Sonraki bölümde, E-PEAP'ın uygulama detaylarına yer verilmiş, geliştirilen protokolün donanımlara uygulanma adımları ve cihazların konfigürasyonları ayrıntılarıyla anlatılmıştır. Yine beşinci bölümde önerilen protokolün testi için oluşturulan test topolojisine, deneysel analizlere ve sonuçlara yer verilmiştir.

Bu tez çalışmasının amacı, güçlü güvenlik özellikleriyle literatürde yaygın olarak kullanılan PEAP protokolünün, kimlik bilgilerinin gizliliğini sağlamada zayıf olan Faz-1 aşaması için güvenli bir kimlik bilgisi iletim ortamı sağlamaktır.

2. KABLOSUZ YEREL AĞLARDA GÜVENLİK

ISO/IEC 27001'e göre güvenlik, bir kurumun bilgi varlıklarının gizliliğinin (bilginin yetkisi olmayan kişi, kurum ya da süreçler için kullanılabilir olmaması ya da ifşa edilmemesini temin etme özelliği), bütünlüğünün (varlıkların doğruluğunun ve eksiksizliğinin teminat altına alınması özelliği) ve kullanılabilirliğinin (yetkili bir kurumun talebi üzerine kullanılabilir olma özelliği) koruması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesinin önlenmesi, kişi ve kurumların bu teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin analizlerinin yapılarak gerekli önlemleri önceden alması olarak tanımlanmaktadır [10].

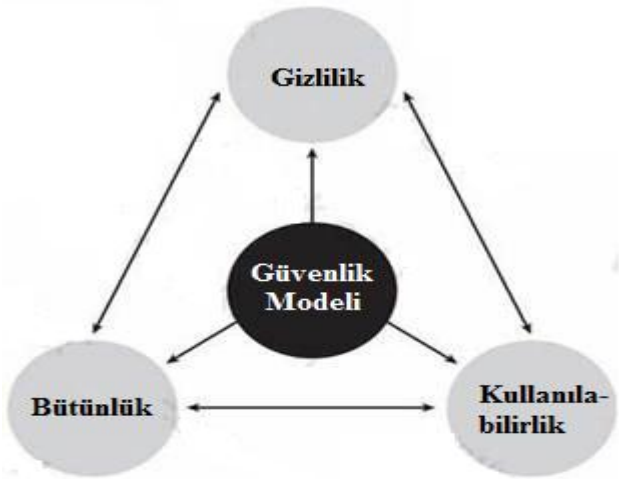
Karin'e göre ise bili güvenliği; elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür [11].

Ağ güvenliği kapsamında bakıldığında güvenlik, ağ cihazları ile bu cihazlarda işlenmekte olan verilerin gizliliğini, bütünlüğünü ve sürekliliğini korumayı amaçlayan bir disiplindir. Önceleri merkezi olarak kilitli odalarda tutmak, güvenliğini tehdit edebilecek tehlikelere karşı bilgi ve belgeleri kilitlemek ve sadece yetkililerin girmesini sağlamak şeklinde olan güvenlik anlayışı günümüzde hızla gelişen ve karmaşıklaşan bilgisayar ve ağ teknolojileri sebebiyle daha kompleks bir yapıya dönüşmekte, yerel alan gibi veri paylaşım ortamlarında güvenliği sağlamak oldukça zorlaşmaktadır.

Kablosuz ağlar, verilerin fiziksel bir koruma olmadan hava ortamında iletilmesi sebebiyle saldırılara en açık iletişim şeklidir. Bu durumun bir zaafiyet oluşturmaması ve olası tehditlerin önlemesine yönelik kablosuz ağlarda güvenli iletişim için kullanılan kavram ve teknolojiler aşağıda ayrıntılı olarak anlatılmıştır.

2.1. CIA

Bilgi güvenliğinin birinci amacı bilgi gizliliğini sağlamaktır. Bununla birlikte yetkisiz erişimi, yetkisiz değişiklikleri engellemeyi amaçlar. Ayrıca erişimi reddetmeyi (denial/repudiation) de engellemek gerekir. Bu anlamda bilgi güvenliğinin üç temel terimi vardır. Bu terimler aşağıda ayrıntılı olarak anlatılmıştır.



Şekil 2.1. CIA kavram haritası

2.1.1. Gizlilik

Gizlilik, ISO tarafından "Bilgiye sadece yetkilendirilmiş kişilerce ulaşılabilmesi" olarak nitelenir. Şifreleme altyapılarının olmasının temel sebebi gizlilik ve bütünlüktür. Bilgi güvenliğinin her kavramı her kurum için eşit önemde olmayabilir fakat gizlilik özellikle kamu kurumları ve bankalar olmak üzere bütün kuruluşlar için oldukça kritik değerdedir.

Gizlilik, verinin/içeriğin görüntülenmesinin sadece veriyi görüntülemeye izin verilen şahısların erişimiyle kısıtlanmasıdır. Bu şekilde, artık çok da zor olmayan ve kişisel bilgi mahremiyetini tehdit eden iletişim trafiğinin yetkisiz olarak dinlenmesine karşı bir önlem alınmış olur. Gizlilik, bilginin şifrelenmesi ile gerçekleştirilebilir.

2.1.2. Bütünlük

Bütünlük, verinin veya bilginin yetkisiz kişilerce değiştirilmesine veya yok edilmesine karşı korunmasıdır. Verinin bozulması kasıtlı olarak veya kaza ile olabilir ama bu bütünlüğün bozulmuş olduğu gerçeğini değiştirmez. Güvenlik önlemi alanların iki tür riske karşı da tedbir almaları gerekmektedir. Bilginin bütünlüğü; kesinlik, doğruluk, geçerlilik kıstaslarını sağlamalıdır.

Verinin izinsiz olarak veya yanlışlıkla değiştirilmesinin, silinmesinin veya veriye ekleme yapılmasının önlenmesi, verinin göndericiden alıcıya, göndericiden çıktığı haliyle değişmeden ulaşmasını sağlar. Alıcı, iletinin göndericiden çıktığı haliyle kendisine ulaştığını bir bütünlük sınaması yaparak anlar. Bütünlük gereksinimi, elektronik imza ile gerçekleştirilebilir.

2.1.3. Kullanılabilirlik

Erişilebilirlik veya kullanılabilirlik, matematiksel olarak ifade edildiğinde, herhangi bir sistemin yapılış amaçlarına göre işlev gördüğü zamanın, işlev gördüğü ve görmediği toplam zamana oranıdır. Daha yalın bir anlatımla doğru yetkilendirilmiş bir kişinin ihtiyacı olduğu anda ihtiyacı olan hizmetin orada olma oranına erişilebilirlik denir. Verilen hizmetin ne kadar güvenilir olduğunun bir ölçütüdür. Kurumlar hizmetin ne kadar önemli olduğunun ölçümünü yapıp, sistemleri ve verileri bu ihtiyaca göre yedekli hale getirirler.

2.2. AAA

Ağ güvenliği tanımlamasında, Yetkilendirme, Loglama, Kimlik Doğrulama kavramlarının baş harflerinden oluşan, ağda dolaşan paketlerini bazı modellere göre dikkatlice inceleyerek kötü niyetli aktiviteleri haber veren bir sistemlerin bütünüdür.

2.2.1. Yetkilendirme

Kullanıcıların, sunucu ya da uygulamaya giriş yapması veya verilen aktiviteyi yürütmesi için verilen yetkilendirme işlemidir. Yetkilendirme, çeşitli kısıtlamalar olarak da tanımlanabilir. Örneğin gün kısıtlamalı, ya da fiziksel lokasyon kısıtlaması ya da aynı birim ya da kullanıcı için aynı anda birden çok bağlantı kurulumu kısıtlaması gibi. Kullanıcı adı ve şifre doğrulaması sağlanan kullanıcıların sisteme, programa veya ağa hangi yetkilerle erişim hakkına sahip olduklarını belirten sisteme yetkilendirme denir. Sisteme kayıtlı olan kullanıcılar gruplanarak, bu gruplara çeşitli yetkiler verilir. Kullanıcı içerisinde bulunduğu grubun bütün yetkilerine sahiptir. Eğer bir kullanıcı birden fazla gruba üye ise bu gruplara verilen yetkilerin hepsine sahiptir. Güvenliğin tam olarak sağlanabilmesi için kullanıcılara gerekenden fazla yetki verilmemelidir. Yetkiler verilirken sistem üzerindeki açık her bağlantı noktası göz önünde bulundurulmalıdır.

2.2.2. Loglama

Loglama, ağ kaynaklarının kullanıcılar tarafından tüketiminin izlemesi ile ilgili bir kavramdır. Bu bilgi, planlama, faturalama, yönetim veya diğer amaçlar için kullanılabilir. Gerçek zamanlı loglama, network kaynaklarının anlık olarak tüketim dağılımıyla ilgili bilgiler verir. Tipik olarak loglama toplam olarak sisteme giriş yapan kullanıcı bilgisi, kullanıcıların kullandıkları servis bilgilerini, servisin başlangıç ve bitiş saatleri, toplam süreleri gibi bilgiler ile ilgilenir. Sistemde bulunan kullanıcıların yaptıkları bütün işlemler ve erişim saatleri kayıt altına alınır. Bir sorun ile karşılaşıldığında sorunun tespitinin sağlanabilmesi için bu veriler kullanılarak kullanıcı aktivitelerinin tutulduğu bu kayıtlardan sorun anlaşılmaya ve çözülmeye çalışılır.

2.2.3. Kimlik doğrulama

Kimlik doğrulama, bir kaynağa erişim sırasında yapılan kontrol işlemi, bir kişinin ya da bir sistemin, olduğunu iddia ettiği kişi olduğunun ispatlanmasıdır. Tüm güvenlik

sistemlerinin en kritik parçalarından birisidir. Kimlik doğrulama işlemi kullanıcıların bilgisayara girişini, uzaktan bağlantı yapması gibi işlemlerde kullanılan ana kontrol sistemidir. Normalde bir işletim sistemi ya da aygıt tarafından, bir bilişim sistemi kullanıcısının kimliğinin doğruluğunun ve bilişim kaynaklarına erişim yetkisinin bulunup bulunmadığının saptanması, sınanması veya internet gibi bir ağ üzerinden gelen bir mesajın çıkış noktasının ya da bir belgenin aslına uygunluğunun, kurcalanmamış veya tahrif edilmemiş olduğunun kanıtlanması amacıyla uygulanır.

Veri iletişiminde mesajın iletiminin geçerliliğinin ve mesaj sahibinin kimliğinin doğrulanması gerekmektedir. Örneğin bir elektronik posta mesajı üzerinde yer alan gönderici adresi, mesajın asıl göndericisi olmayabilir. Bu nedenle alıcı, göndericinin kimliğini doğrulamak için bir takım yöntemler kullanır. Bu yöntemlerden bazıları aşağıda verilmiştir.

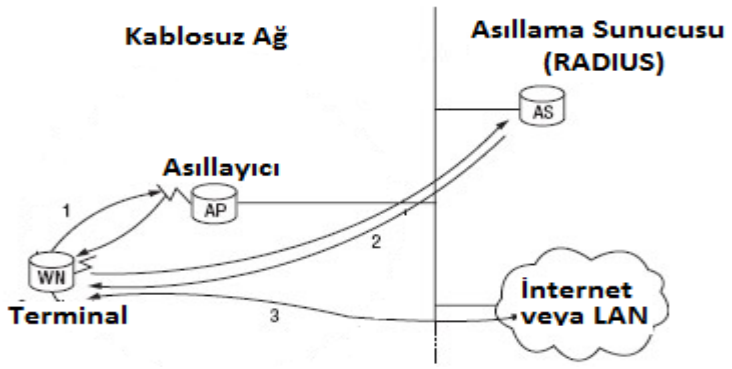
- Kullanıcı ad ve şifre
- Akıllı Kart
- Kişisel Tanımlama Numarası
- Uzak erişim doğrulaması
- Dijital İmza

2.3. 802.1x

Port tabanlı ağ erişim denetimi, noktadan-noktaya bağlantı özelliklerine sahip bir yerel ağ portuna takılan cihazların kimlik doğrulaması ve yetkilendirme için ve bu sayede kimlik doğrulaması ve yetkilendirmesi başarısız olması durumunda o portu erişimden koruyarak IEEE 802 yerel ağ altyapılarının fiziksel erişim özelliklerinin kullanımına olanak sağlayan, port tabanlı ağ erişim denetimi olan 802.1X teknolojisi, ağda port tabanlı kullanıcı doğrulayabilmek, herhangi bir kullanıcıya ya da gruba ağ erişim politikaları uygulamaya imkan tanır. Kimlik doğrulama ve yetkilendirme başarısızsa o port erişime kapatılır ve bu sayede yerel ağ altyapısı korunmuş olur. Kullanıcı doğrulama; MAC adresi, switch portu ya da harici bir yetkilendirme

politikası ile sağlanır. Ağa kimin hangi hakla gireceğinin belirlenmesi, denetlenmesi ve yetkilendirmesi; kullanıcı odaklı, ağ tabanlı erişim kontrolü olan NAC tarafından belirlenir.

802. 1X, kablolu ağlar için geliştirilmiş bir standart olup kablosuz ağlar için de kullanılmaktadır. Bu standart istemci ile erişim noktası arasında kimlik denetleme sunucusu kullanarak kimlik denetleme ve port tabanlı erişim kontrolü sağlamaktadır. 802. 1X, yerel ve metropol alan ağlarının standart ailesinin bir parçasıdır ve Wi-Fi'nin yeni güvenlik modelinin temeli olan IEEE 802.11'in Görev Grubu tarafından ayarlanmaktadır. 802.1X; Genişletilebilir Kimlik Doğrulama Protokolü (EAP-Extensible Authentication Protocol) tabanlıdır. EAP; ağ yöneticisine, birçok kimlik denetimi yönteminden, kendi ağları için uygun olanını seçmesini sağlar. Şekil 2.2'de basit bir 802. 1X mimarisi gösterilmektedir. Bu mimarinin çalışma şekli şöyledir: Kullanıcı erişim noktasına bağlantı talebinde bulunur. Erişim noktası, bağlantı isteğini alınca, tüm portları kapalı tutar ancak kullanıcı ile arasında sınırlı iletişimin olduğu bir port açar. Erişim noktası kullanıcıdan kimliğini ister. Kullanıcı kimliğini gönderir. Erişim noktası kimlik bilgisini bir kimlik denetleme sunucusuna gönderir. Kimlik denetleme sunucusu kullanıcının kimliğini denetler ve doğruladığında kabul mesajını erişim noktasına gönderir. Erişim noktası, kullanıcının portunu yetkilendirilmiş duruma getirir. Kullanıcı kimlik denetleme sunucusundan kimliğini ister, kimlik denetleme sunucusu kimlik bilgisini kullanıcıya gönderir. Kullanıcı kimlik denetleme sunucusunun kimliğini doğruladığında veri trafiğine başlanır.



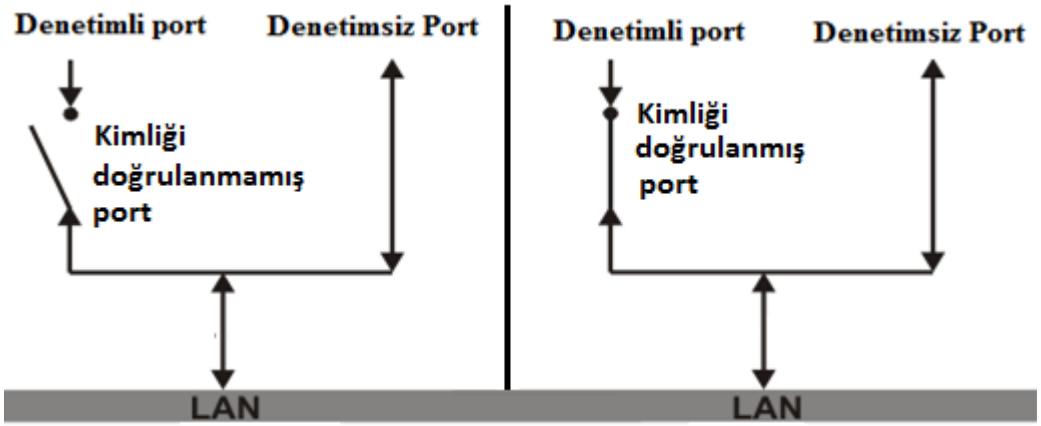
Şekil 2.2. 802.1X mimarisi

Bir kablosuz düğümün diğer yerel ağ kaynaklarına erişebilmesi için kimlik kanıtlaması aşağıdaki şekilde yapılmalıdır.

1. İstemci bir yerel ağ kaynağına erişim isterse, erişim noktası istemcinin kimliğini sorar. İstemcinin kimliği doğrulanmadan EAP'den başka hiçbir akışa izin verilmez; port kapalıdır. İstemci güven ortamını oluşturacak kimlik doğrulayıcı veriye cevap vermekle sorumludur.

2. Kimlik gönderildikten sonra kimlik doğrulama süreci başlar. İstemci ve Kimlik Doğrulayıcı arasında kullanılan protokol EAP'tır; veya daha doğru olarak EAP kaplamalı yerel ağ'dır (EAPOL). Kimlik Doğrulayıcı EAP iletilerini RADIUS biçimine yeniden dönüştürür ve onları Kimlik Doğrulayıcı sunucuya aktarır. Kimlik doğrulama süresince, erişim noktası sadece istemci ve kimlik doğrulama sunucusu arasında paketleri nakleder. Kimlik kanıtlama süreci bittiğinde kimlik doğrulama sunucusu başarılı (veya doğrulama başarısız olursa, başarısız) iletisi gönderir.

3. Başarılı bir kimlik kanıtlamadan sonra Erişim Noktası portu kimliği doğrulanan istemci için açar ve istemci diğer yerel ağ kaynaklarına/internete erişmeye hak kazanır. Port tabanlı kimlik kanıtlama denmesinin sebebi kimlik doğrulama mimarisinin denetimli ve denetimsiz portlarla uygulanıyor olmasıdır. Denetimli port da denetimsiz port da mantıksal, sanal varlıklardır ama yerel ağa aynı fiziksel bağlantıyı kullanırlar. Kimlik doğrulama öncesinde sadece denetimsiz port “açıktır”. Sadece EAPOL trafiğine izin verilir. İstemci kimliği doğrulandıktan sonra, denetimli port açılır ve diğer yerel ağ kaynaklarına erişim hakkı verilir.



Şekil 2.3.802.1X'te port durumları

2.3.1. 802.1X Bileşenleri

İstemci

802.1x standardı istemciyi "bir noktadan-noktaya LAN parçasının bir ucunda bulunan ve diğer ucundaki kimlik denetleyici tarafından kimliği doğrulanacak olan varlık" olarak tanımlanmaktadır. Bu bir kablosuz dizüstü bilgisayarı, bir avuçiçi bilgisayarı veya bir masaüstü bilgisayarı kimi durumlarda da bir anahtarlama cihazı olabilir. İstemci ağa bağlanmak isteyen bir aygıttır ve 802.1x Kimlik Doğrulama işleminin öznesi durumundadır. İstemci normalde doğrudan kimlik doğrulayıcı sunucusuna değil erişim noktasına bağlıdır.

Kimlik denetleyici

Kimlik denetleyici genellikle bir kablosuz erişim noktası veya bir anahtarlama cihazıdır. Kimlik denetleyici istemciye hizmet sunan ve istemcinin kimliğini doğrulamasına 802.1x standardına göre, yardımcı olan bir cihazdır. Kimlik denetleyici basitçe, kimlik doğrulama sunucusu ile istemci arasındaki kimlik doğrulama bilgi trafiğinin ileri ve geri taşınmasını sağlayan, istemci tarafındaki bir ara cihaz yada proxy gibi çalışır. Bütün işlem istemci ile kimlik doğrulama sunucusu arasında gerçekleştiğinden dolayı kimlik denetleyicinin, çok güçlü olmasına gerek

yoktur. Bazı kimlik denetleyiciler birden fazla kimlik doğrulama Sunucusuyla çalışacak şekilde yapılandırılabilirler. Bu durumda normalde kimlik denetleyici bir sunucuyla konuşacak bu birincil sunucunun düşmesi durumunda diğer sunucuyla konuşmaya geçecektir. Bu sistemin çok daha yüksek bir verimle kullanılmasını sağlayacaktır ancak kimlik doğrulama sunucularının sürekli senkronize olmaları gerekmektedir.

Kimlik doğrulama sunucusu

Kimlik doğrulama sunucusu, kimlik doğrulama, izin verme ve hesap tutma (AAA) işlemlerini yapan gerçek cihazdır. Sunucu istemcinin kimliğine bakarak kimlik denetleyici tarafından sağlanan servislere erişip erişmeyeceğini onaylar. 802.1x standardı hangi kimlik doğrulama sunucusunu kullanılacağını belirtmez. O, sistemi kuran kişinin tercihindedir. İstemciden kimlik bilgilerini istemek ve bu bilgileri veri tabanındaki verilerle karşılaştırarak kimliği doğrulamak ya da gelen talepler geçersiz ise bu istekleri sonlandırmak kimlik doğrulama sunucusunun görevidir.

2.4. SSL

SSL (Secure Sockets Layer) network üzerindeki bilgi transferi sırasında güvenlik ve gizliliğin sağlanması amacıyla Netscape tarafından geliştirilmiş bir güvenlik protokolüdür. 1996 yılında versiyon 2'nin kararlı hale gelmesiyle Microsoft Explorer, Netscape Navigator gibi bütün İnternet tarayıcılarının desteklediği bir standart haline gelmiş ve çok geniş uygulama alanları bulmuştur.

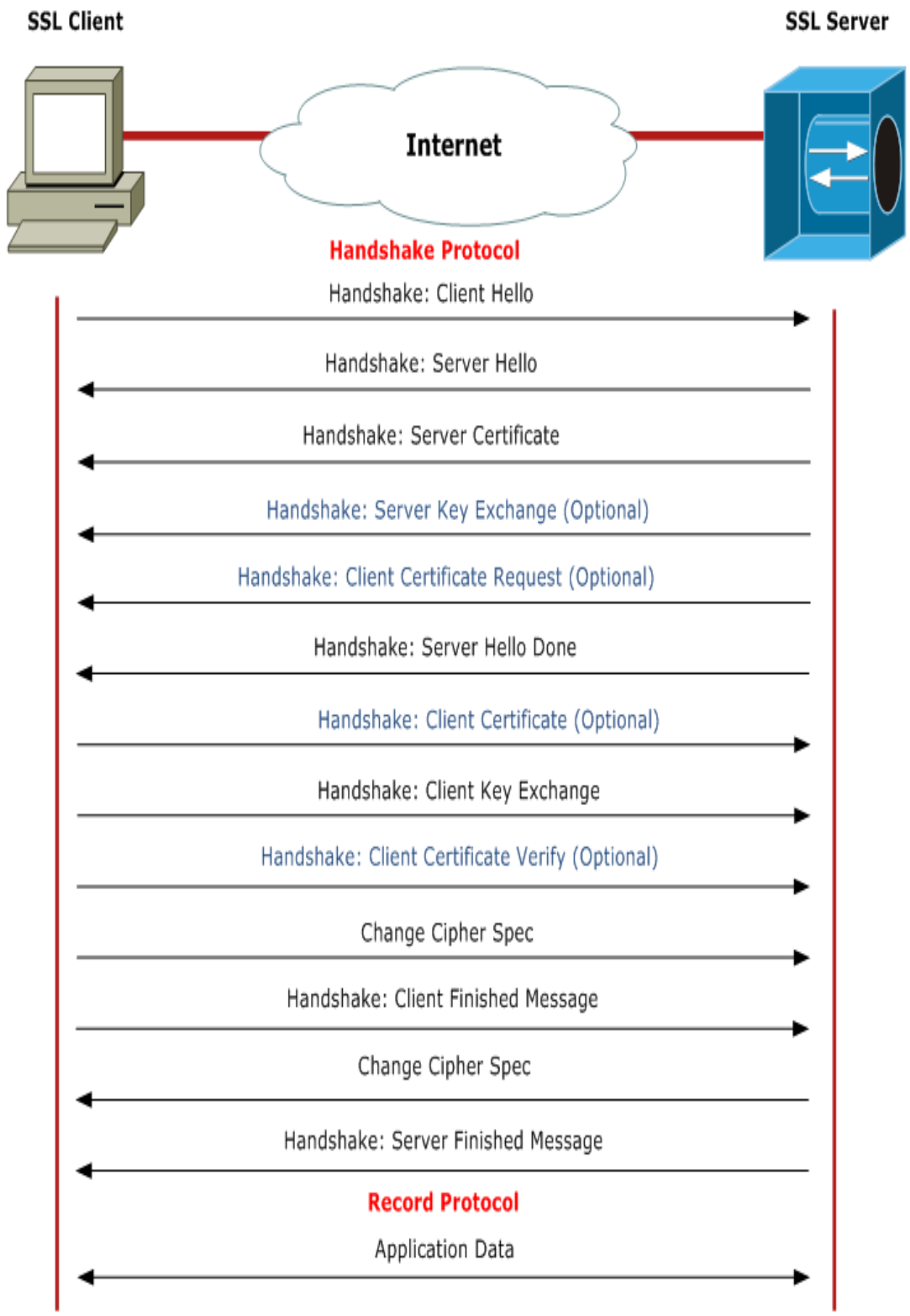
SSL gönderilen bilginin kesinlikle ve sadece doğru adreste deşifre edilebilmesini sağlar. Bilgi gönderilmeden önce otomatik olarak şifrelenir ve sadece doğru alıcı tarafından deşifre edilebilir. Her iki tarafta da doğrulama yapılarak işlemin ve bilginin gizliliği ve bütünlüğü korunur.

Veri akışında kullanılan şifreleme yönteminin gücü kullanılan anahtar uzunluğuna bağlıdır. Anahtar uzunluğu bilginin korunması için çok önemlidir. Örneğin; 8 bit

üzerinden bir iletimin çözülmesi son derece kolaydır. Bit, ikilik sayma düzeninde bir rakamı ifade eder. Bir bit, 0 veya 1 olmak üzere 2 farklı değer alabilir. 8 bit ise sadece 28=256 olası farklı anahtar içerir. Bir bilgisayar bu 256 farklı olasılığı sıra ile inceleyerek bir sonuca ulaşabilir. SSL protokolünde 40 bit ve 128 bit şifreleme kullanılmaktadır. 128 bit şifrelemede 2^{128} değişik anahtar vardır ve bu şifrenin çözülebilmesi çok büyük bir maliyet ve zaman gerektirir. Kötü niyetli bir kişinin 128 bit'lik şifreyi çözebilmesi için 1 milyon dolarlık yatırım yaptıktan sonra 67 yıl gibi bir zaman harcaması gerekir. Bu örnekten anlaşıldığı gibi SSL güvenlik sistemi tam ve kesin bir koruma sağlar.

Bilgisayarların birbirlerini tanıma işlemi, açık-kapalı anahtar tekniğine dayanan bir kripto sistemi ile sağlanır. Bu sistemde, iki anahtardan oluşan bir anahtar çifti vardır. Bunlardan açık anahtar herkes tarafından bilinebilen ve gönderilen mesajı şifrelemede kullanılan bir dijital anahtardır. Burada anahtardan kasıt, aslında bir şifreleme algoritmasıdır. Bu algoritma, yani anahtar kullanılarak gönderilecek bilgi şifrelenir. Ancak, açık anahtar ile şifrerelenen mesaj sadece bu anahtarın diğer çifti olan kapalı anahtar ile açılabilir. Kapalı anahtar da, sadece sizin bildiğiniz bir anahtar olduğundan, mesaj güvenliği sağlanmış olur. Örnek olarak, size mesaj göndermek isteyen birine kendi açık anahtarınızı gönderirsiniz. Karşı taraf bu anahtarı kullanarak mesajını şifreler ve size gönderir. Şifrelenen mesajı, sadece sizde olan bir kapalı anahtar çözebilir ve bu anahtarı sadece siz bilirsiniz.

SSL, kimlik doğrulama sunucularını tanımak için, dijital olarak imzalanan sertifikalar kullanır. Sertifika, aslında, o organizasyon hakkında bazı bilgiler içeren bir veri dosyasıdır. Aynı zamanda da, kuruluşun açık-kapalı anahtar çiftinin açık anahtarı da sertifika içinde yer alır. Sunucu sertifikası da, o sunucuyu işleten kuruma ait bilgiler içeren bir sertifikadır. Sertifikalar, VeriSign gibi güvenilir sertifika kuruluşları tarafından dağıtılır.



Şekil 2.4. SSL tünelinin kurulma aşamaları

2.5. Sertifika

Elektronik Sertifika, yani elektronik kimlik sahibinin kişisel bilgilerini ve bu kişisel bilgilere ait açık anahtar bilgisini taşıyan ve taşıdığı açık anahtar bilgisinin, belirtilen kişi veya kuruma ait olduğunu garanti eden belgedir. Sertifika açık anahtarlı kriptografi teknolojisine dayanır ve kamuya açıktır, yani sertifikalar gizli tutulması gereken dosyalar değillerdir. Elektronik kimlik belgesi kişilere ait olabildiği gibi kurumların ve web sunucuların da elektronik kimlik belgeleri olabilir. Bir elektronik kimlik belgesinde bulunması gereken bilgiler şöyledir: Sahibinin kamuya açık anahtarı, sahibinin adı, soyadı, çalıştığı kurum gibi kimlik bilgileri, elektronik kimlik belgesinin geçerlilik süresi, seri numarası, elektronik kimlik belgesini veren sertifika hizmet sağlayıcı bilgileri, sertifikanın kullanım alanlarını belirleyen bilgiler,

Elektronik imza, yukarıdaki bilgilerin tamamının sertifika hizmet sağlayıcısı tarafından imzalanmasıyla oluşturulur. Elektronik kimlik belgelerinin güvenilir kurumlar tarafından dağıtılması gereklidir. Sertifika sahibinin kimlik bilgileri ve açık anahtarı sertifika hizmet sağlayıcısı tarafından onaylanıp imzalandıktan sonra sertifikaların dağıtımı yapılmalıdır.

Sertifikalar, kullanıcı ve bilgisayar kimliklerini doğrulamada çok güçlü güvenlik sağladıkları ve daha az güvenli olan, parolaya dayalı kimlik doğrulama yöntemlerine olan gereksinimi ortadan kaldırdıkları için, ağ erişimi kimlik doğrulaması için kullanılır. Bu konuda, Internet Kimlik Doğrulama Hizmeti (IAS) ve VPN sunucularının, VPN ve kablosuz bağlantılar dahil olmak üzere çeşitli ağ erişim türleri için sertifika tabanlı kimlik doğrulaması gerçekleştirmek amacıyla EAP-TLS, PEAP veya Internet Protokolü güvenliği IPSec'te kullanılmaktadır.

EAP-TLS ve PEAP'ta sertifika kullanmaktadır. Her iki yöntem de, sunucu kimlik doğrulaması için her zaman sertifika kullanır.

Sertifika Yaşam Döngüsü

1. Sertifika talebinde bulunacak kişi/kurum kendine özel private-public key çiftini oluşturur. Şifreleme bu haliyle de yapılır. Ancak bu durumda sadece şifreleme sağlanmış olur. Kimlik doğrulama, bütünlük ve inkar edilememezlik için oluşturulan açık anahtarın herkesin bildiği/güvendiği bir sertifika otoritesi (CA) tarafından onaylanması gerekir.

2. Sertifika başvurusu (kişi/kurumun gizli anahtarı ve kimlik bilgileri) Kayıt Otoritesine (RA) yapılır. RA gerekli kimlik doğrulama işlemlerini yaparak (kimlik araştırması, ticaret sicil gazetesi vb) başvuru ve gerekli bilgileri CA'ya gönderir. CA, başvuran kişi/kurumun açık anahtarının hash'ini alıp kendi gizli anahtarı ile şifreler/imzalar. Yani, dijital imza; kullanıcının açık anahtar hashi'nin CA'nin gizli anahtarı ile şifrelenmesidir. CA, başvuruyu yapan kişi/kurumun açık anahtarını ve hash'ini kullanarak sertifika üretir.

3. Sertifika kullanılacağı zaman kaynağından indirilir (https web sayfası, file server vb). İçindeki açık anahtar ve dijital imza ayrıştırılır. CA'in gizli anahtarı ile imzalanmış hash, CA'nın herkes tarafından edinilebilen açık anahtarı ile deşifre edilir. Elde edilen hash değeri, gelen sertifikadaki açık anahtarın hashi alınarak hangi metodla hashlenmişse; MD5, SHA-1 vb. karşılaştırılır. Aynı ise, sertifikanın doğru olduğu değerlendirilir. Artık, sertifikanın gerçekten sahibi tarafından kullanıldığından emin olunur.

4. Kullanıcı, şifrelemede kullanmak üzere oturum anahtarı üretir. Bunu, kişi/kurumun açık anahtarı ile şifreleyerek kişi/kuruma gönderir. Kişi/kurum, kendi açık anahtarı ile şifrelenmiş oturum anahtarını gizli anahtarı ile deşifre eder. Böylece anahtar değişimi yapılmış olur. Gidip gelen veriler bu simetrik oturum anahtarı ile şifrelenir. Her yeni bağlantıda rassal olarak üretilir. Kullanıldıktan sonra silinir.

5. Anahtar Değişimi asimetrik şifreleme ile, veri şifrelemesi simetrik şifreleme ile yapılır.

6. Kullanım süresi dolan sertifikalar sertifika iptal listesine (CRL) kaydedilir. CA, sertifikayı üreten ve kullanan kişiler/kurumlar için güvenilir üçüncü taraf rolündedir. Kullanıcı sertifikasını kullanacağı kişi/kuruma doğrudan güvenmese de CA'ye güvenir. Kişi/kurum da aynı CA'ya güvendiğinden dolaylı olarak aralarında güven sağlanmış olur.

3. EAP

Genişletilebilir Kimlik Kanıtlama Protokolü EAP, 802.1X'in kullanıcı doğrulama işlemi boyunca noktadan noktaya iletim katmanı üzerinde IP'ye ihtiyaç duymadan genel bir çerçevede kimlik tanımlama sistemi olan iyileştirilmiş bir iletim protokolü standardı, çoklu kimlik kanıtlama yöntemlerini destekleyen bir kimlik kanıtlama çalışma çerçevesidir.

EAP; 3.katmanın kullanılamadığı durumlarda 2.katmanı kullanarak kimlik doğrulaması yapmak için dizayn edilmiştir. Kimlik sorgulamasının güvenli olarak yapılmasını sağlayacak sınırlılıkta paket taşır. Ayrıca diğer protokollerden farklı olarak kimlik doğrulama istemci tarafından değil kimlik denetleyici tarafından başlatılır. Kimlik denetleyicinin akıllı bir cihaz olmasına, denetlemeyi sağlayan algoritmayı anlamasına gerek yoktur. İşlemleri istemci ve kimlik doğrulama sunucusu yapar. Kimlik denetleyici; sunucu için hangi porta gidileceğini gösteren bir geçiş noktası özelliği taşır. Bu özelliğinden dolayı 802.1x, tipik olarak küçük ve hafızası az ve işlemci gücü düşük olan kablosuz erişim için idealdir. EAP'ın farklı alanlarda kullanımı, güvenlik sorunu gibi nedenlerden dolayı EAP için birçok algoritma geliştirilmiştir.

EAP'ın çalışma şekli şöyledir:

Kimlik doğrulaması yapmak isteyen kullanıcı ve kimlik denetiminin yapıldığı sunucu arasında bulunan denetleyici cihaz, bağlantı durumunda istemciye EAP-Request/Identity paketi göndererek kendisini tanıtmasını ister.

1. İstemci, kimliğini tanıtan EAP-Talep/Kimlik paketi ile cevap verir. Bu paket RADIUS paketleriyle enkapsüle edilerek sunucuya gönderilir.

2. Sunucu, denetleyiciye şifreli token sistemi gibi bir davetiye atar. Denetleyici bu paketi açıp EAPOL içerisinde istemciye gönderir. İstemci davetiyeye denetleyici üzerinden cevap gönderir.

3. Eğer istemci gerekli kullanıcı tanımına ve haklarına sahipse, sunucunun gönderdiği doğrulayıcı mesaj denetleyicinin istemciye LAN'a erişim izni vermesiyle sonuçlanır.

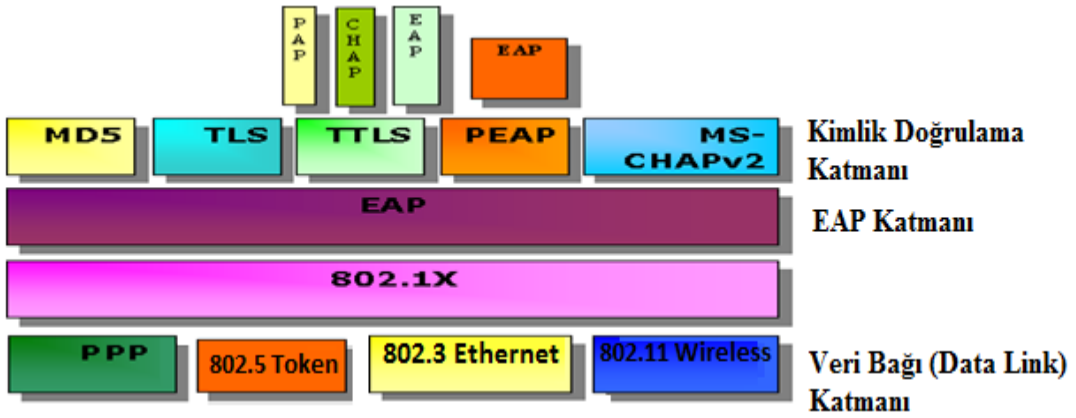
8 bit	8 bit	16 bit
Code	Identifier	Length
Data :::		

Code

Code	Description	References
1	Request.	RFC 3748
2	Response.	RFC 3748
3	Success.	RFC 3748
4	Failure.	RFC 3748
5	Initiate.	RFC 5296
6	Finish.	RFC 5296
7 - 255		

Şekil 3.1. EAP başlık yapısı

Katmansal olarak EAP hiyerarşisi Şekil TT'de gösterilmiştir.



Şekil 3.2. Katmansal EAP hiyerarşisi

3.1. Kablosuz Ağlarda Olması Beklenen Güvenlik Özellikleri

Güvenli olduğunu ileri süren her kablosuz ağ protokolünü bazı özellikleri yerine getirmesi beklenir. RFC 4017 [15] ve RFC 3748 [16] kablosuz ağlarda sağlanması gereken zorunlu güvenlik özelliklerini tanımlamıştır.

3.1.1. Karşılıklı kimlik doğrulama

Karşılıklı kimlik doğrulaması, client ve kimlik doğrulama sunucusunun iletişime başlamadan önce birbirlerine kendilerini tümüyle tanıtması işlemidir. Bu sistem birçok şekilde sağlanır; bir secret paylaşılır ya da Diffie-Hellman anahtar değişim sistemi [28] kullanılır. Diffie-Hellman Anahtar sistemi daha güvenlidir.Kimliklerin doğrulanması için CA her iki taraf tarafından da bilinmelidir. Genellikle SSL tarafından kullanılır. Bunun dışında mutual authentication işlemi RADIUS sunucusu üzerinden yapılacak kimlik doğrulama işleminde de kullanılır. Mutual authentication sayesinde Man-in-the-Middle (MITM) ataklarına karşı korunma sağlanır. Online bankacılık uygulamalarında SSL sertifikalarının kullanılmasını bu konuya tipik bir örnek olarak verilebilir. Diğer bir örnek olarak, bir istemci ile sunucu arasındaki IPSEC oturumunda güvenli iletişime başlamadan önce karşılıklı kimlik doğrulama işlemi yapılır.

3.1.2. Kimlik gizliliği

Kablosuz bir ağdan beklenen bir diğer önemli özellik, ağa bağlanmak isteyen kullanıcıların kimlik bilgilerini (kullanıcı ad, şifre, eposta adresi, domain adresi vb.) yetkisiz erişimlerden gizleyebilmesidir. EAP tabanlı kimlik doğrulama protokollerinde Request-Identity ve Response-Identity paketleri kullanıcının kimlik bilgilerini taşımakla görevli paketlerdir. Eğer veriler bu paketler içersinde şifresiz halde giderse ağı dinlemekte olan bir saldırganın o kimlik bilgilerini edinmesi ve daha sonra aynı verileri kullanarak ağa kendini geçerli bir kullanıcı gibi doğrulaması oldukça yaşanan bir saldırıdır. Bundan dolayı kullanılan kimlik doğrulama protokolünün kullanıcı kimlik bilgilerini tamamen gizleyebilmesi özelliği istenir.

3.1.3. Sözlük atağı dayanıklılığı

Eğer kullanıcı kullanıcı ad veya şifresinde, yaygın kullanılan veya birbiriyle ilişkisi bulunan kelime veya kelime gruplarını kullanırsa, bu tip kelimelerden oluşan bir veritabanındaki tüm değerler teker teker denenmek şartıyla kullanıcının bilgileri saptanabilir. LEAP ve MSCHAP gibi bazı kimlik doğrulama protokolleri bu tarz ataklara karşı dayanıksızdır [12].

3.1.4. Tekrar atağı dayanıklılığı

Tekrar ataklarında saldırgan, gerçek kullanıcının kimlik doğrulama esnasındaki süreçlerini ve paketlerini kaydeder. Bu saldırıda saldırganın geçerli paketlerin içeriğini bilmesine gerek yoktur. Daha sonra, ağa bağlantı talebinde bulunan saldırgan, kimlik doğrulama sunucusundan gelen bilgi taleplerine daha önceki geçerli kullanıcının paketleriyle cevap vererek ağa bağlanmaya çalışır. Böyle bir atağı kimlik doğrulama protokolü oluşturulacak tekrar etmeyen, rastgele bir değerin (nonce) paketlere eklenerek paketlerin tanımlanması sağlanabilir. Tek kullanımlık bu değer daha sonraki bir kimlik doğrulama sürecinde yeniden gelirse o taleplerin tekrar atağı olma ihtimali oldukça yüksektir.

3.1.5. Güçlü oturum anahtarlarının üretilmesi

Eğer saldırgan aynı anahtar ile şifrelenmiş çok sayıda paket elde ederse anahtarı keşfetmesi muhtemeldir. WEP protokolünün en temel zayıflıklarından birisi aynı anahtarların kullanılıyor olmasıdır. Bu sorunların önüne geçebilmek için her oturumda farklı anahtarların kullanılması gerekmektedir. Ağdan çok sayıda paket elde edilerek anahtar bulunmuş olsa bile daha sonraki oturumlar için farklı anahtar kullanılacağından kablosuz ortam güvenli bir şekilde kullanılabiliyor olacaktır.

3.1.6. Test

Bir protokol yeni ise varolan protokollerden çok daha fazla güvenlik açığı barındırıyor olması muhtemeldir. Bu sebeple bir protokol yaygınlaştırılmadan önce çok sıkı testlerden geçmeli ve limitleri belirlenmelidir. Örneğin IEEE 802.11 çalışma grubunun, Kablolu ağa eşdeğer güvenlik ismiyle ortaya çıkardığı WEP protokolünün uygulanmaya başladıktan kısa bir süre sonra o kadar da güvenli olmadığı, büyük zaafiyetlerinin olduğu ortaya çıkmıştır. Eğer kullanıma açılmadan yeterince test edilmiş olsaydı muhtemelen bu zaafların bir kısmı giderilebilirdi.

3.1.7. Hızlı yeniden bağlanma

Kablolu bağlantıların aksine kablosuz ağlar kullanıcının erişimi kopmadan bir erişim noktasından diğerine hareket edebilmesine olanak verir. Erişim noktaları arası geçişlerde oturumların kopmaması için bazı süreçlerin daha çabuk geçilmesi gerekmektedir. Bir erişim noktasında kimliği başarıyla doğrulanmış bir kullanıcının diğer erişim noktasına geçtiğinde kimliğinin en baştan doğrulanmaya başlaması oturumların düşmesine sebep olacaktır. Kullanılacak kimlik doğrulama protokollerinin bu özelliği desteklemesi, kimliği doğrulanmış kullanıcıların periyodik kimlik doğrulama süreçlerinin daha hızlı olması güvenli kablosuz ağlardan beklenen özelliklerden biridir.

3.2. EAP Tabanlı Kimlik Doğrulama Protokolleri

3.2.1. EAP-MD5 (Message Digest 5)

MD5, EAP kimlik denetleme yöntemlerinin en basitidir. Kablosuz ağlarda şifrenin açık gitmesinden dolayı önerilmez. Kablosuz ağlarda kullanıldığı zaman, en az güvenli olanıdır, bu sebeple daha çok kablolu ağlarda kullanılır. MD5; istemciden ağa tek yönlü bir kimlik denetleme yöntemidir. MD5'in asıl eksikliği; kimlik denetleyicisine giriş ve tek yönlü bir kimlik denetleme yöntemi için açık metin modunda şifreyi içermesidir. Bu özelliğinden dolayı MITM ataklarına karşı oldukça

zayıftır. MD5, anahtar yönetimini desteklemez. Bu yüzden saldırganlar, WEP anahtarlarının şifresini kırabilirler.

3.2.2. EAP-FAST (Flexible Authentication via Secure Tunneling)

Cisco tarafından tasarlanan EAP-FAST; karşılıklı doğrulamayı sertifika kullanmak yerine, sunucu tarafından dinamik olarak yönetilen PAC (Protected Access Crediental) teknolojisi kullanır. EAP-FAST ile kimlik denetim sunucusu ve kullanıcı arasında güvenli bir tünel oluşturulur. Tüneli oluşturmak için PAC adında bir referansa ihtiyaç duyular. PAC bir PAC sunucusu vasıtasıyla veya EAP-FAST fazlarında dinamik olarak oluşturulabilir. Tünel bir kez kurulduğunda, kullanıcılar kullanıcı adı ve şifreleriyle kimlik denetiminden geçerler. Yönetimsel karışıklıkları azalttığı için esnek bir protokoldür. Kullanıcıların dijital sertifikalar kullanmasına ve güçlü şifre kurallarına gerek yoktur.

3.2.3. LEAP (Lightweight EAP)

LEAP; Cisco tarafından geliştirilen, özellikle Cisco Aironet kablosuz ağlarında kullanılan çift yönlü kimlik denetimini destekleyen bir EAP kimlik denetleme yöntemidir. RADIUS (yaygın kullanılan kimlik denetleme sunucusu) sunucusu yolu ile kimlik denetimi için; kullanıcı adı ve şifresini ve erişim noktası (AP) kimliğini kullanır. Kimlik denetimi üzerine; LEAP, oturum kullanımı için tek zamanlı WEP anahtarları üretir. Data transferini her şifrelemede değişen WEP (wired equivalent privacy) anahtarı ile şifreler ve karşılıklı kimlik doğrulamayı sağlar. LEAP kullanarak, her kullanıcı kablosuz ağa farklı WEP anahtarı kullanarak bağlanır. Oturum anahtarları, kullanıcının yeniden log-in olmasına neden olan RADIUS zaman aşımı özelliğini kullanarak yenilenebilir. Yeniden log-in olma, kullanıcının bilgisi ve müdahalesi olmadan meydana gelebilir. LEAP'ın saldırılara açık olması, çift yönlü kimlik denetimi için MS–CHAPv1 protokolünü kullanıyor olmasından gelmektedir. LEAP'ın eksikliği; sadece Cisco tabanlı ağlarda uçtan uça çalışıyor olmasıdır.

3.2.4. EAP- TLS (Transport Layer Security)

TLS, SSL in atası olan bir kriptografi protokolüdür. Bu protokolün amacı haberleşen iki uygulama arasında veri güvenliği ve bütünlüğünün sağlanmasıdır. TLS, çift yönlü kimlik denetimi sağlamak için X.509 dijital sertifika kullanan, standart haline gelmiş bir IETF denetleme yöntemidir. TLS'nin üretimi, dağıtımı ve genel yönetimi için bir Açık Anahtar Altyapısı (PKI) gerektirir. PKI bilgisini iletmek için; TLS, SSL kullanır. Protokol iki katmandan oluşur. İlk katman TLS kayıt protokolü, diğeri ise TLS el sıkışma protokolüdür. TLS kayıt protokolü ile veriler simetrik şifreleme anahtarları ile şifrelenir. Her bağlantı için farklı bir simetrik şifreleme anahtarı kullanılır. Bu anahtar TLS el sıkışma protokolü kullanılarak alıcı ve verici tarafından paylaşılır. TLS el sıkışma protokolü ile haberleşecek tarafların birbirlerini yetkilendirmeleri, şifreleme algoritması ve anahtarların karşılıklı değişimi sağlanır. Bu çift yönlü doğrulama özelliği ile EAP-TLS en güvenilir EAP yöntemlerinden biri olarak bilinir. Bununla birlikte, her istemciye özgün sertifika üretilerek, güvenli bir şekilde dağıtılmasını gerektiren bu yöntem, uygulamada getirdiği bu zorluk nedeni ile çok sık uygulanan bir yöntem değildir.

EAP-TLS karşılıklı doğrulama işlemi şu şekilde yapılır:

1. Kullanıcı AP'ye üye olur.
2. Tüm erişim istekleri doğrulama yapılana kadar bloklanır.
3. Kullanıcı, dijital sertifika ile sunucuyu asıllar.
4. Sunucu, dijital sertifika ile kullanıcıyı asıllar.
5. Sunucuda ve kullanıcı kartında dinamik bir WEP anahtarı oluşturulur.
6. Sunucu bu anahtarı güvenilir kablolu ağ üzerinden AP'ye gönderir.
7. AP ve kullanıcı tek kullanımlık bu anahtarı aktif hale getirirler ve iletişim esnasında kullanırlar.

İstemci ile ağ arasında sertifika temelli, karşılıklı kimlik doğrulama sağlar. Tam güvenliği sağlamak için hem istemci hem de sunucu sertifikası kullanılabilir. Bu sertifikalar dinamik olabilir. Dezavantajı sertifikaların yönetim gerektirmesidir. Çok geniş kablosuz ağlarda büyük sorunlar yaratabilir.

3.2.5. EAP-TTLS (Tunneled Transport Layer Security)

TTLS; Funk Software'in öncülük ettiği, şimdi bir IEFT standartı olan, TLS'nin istemci sertifikası ihtiyacını ortadan kaldırmak için geliştirilen, iki kimlik denetleme (diğeri PEAP'dir) yönteminden biridir. TTLS, istemci ile kimlik denetleme sunucusu arasında kurulan SSL tünelini kullanarak güvenli bir biçimde kimlikleri iletebilir.

EAP-TLS'e alternatif olan TTLS kimlik denetim sisteminde kimlik doğrulama bilgisinin güvenli bir şekilde iletilebilmesi için istemci ile sunucu arasında TLS ile şifreli bir oturum oluşturulur. Sorgulama ve yanıt paketleri, herkese açık olmayan TLS şifreli bir kanal üzerinden gönderilir. Bunun için sucunu için tek bir anahtar çifti oluşturulur. İstemci rastgele oluşturduğu anahtarı kendi public anahtarı ile şifreleyip sunucuya yollar. Bundan sonraki haberleşme bu yeni ortak anahtar ile simetrik şifreleme ile devam eder.

TTLS, çoklu yetki talep mekanizmalarını (PAP, CHAP, MS-CHAPv1, MS-CHAPv2, PAP/Token Card or EAP) destekleyebilir. TTLS; RADIUS protokolünde kullanılanla aynı olan "Attribute Value Pairs" (AVPs) değişimi yolu ile farklı kimlik denetleme yöntemleri uygulayabilir. PAP, CHAP, MS-CHAPv1 gibi az güvenlikli kimlik doğrulama metodları kullanıyor olması ise güvenlik seviyesini düşüren bir özelliktir.

TTLS'nin TLS'ye göre diğer bir avantajı; bilginin kurulan tünel üzerinden sunucuya gönderilirken, kullanıcı kimliğinin dışarıdan dinleyenlere açık olmamasıdır. TTLS; çok güvenli olarak dikkate alınır, birçok ticari uygulama tarafından uygulanır. Bununla beraber, 802. 11 kimlik denetim yöntemi tarafından kapsanmaz. TLS'ten farklı olarak sadece sunucu bazlı sertifika kullanır ve doğrulama işlemini şifrelenmiş, güvenli bir tünelin (encrypted tunnel) içinden geçirerek yapar.

3.2.6. PEAP (Protected EAP)

EAP protokol kümesine ait olan PEAP (Protected Extensible Authentication Protocol) istemci ve kimlik doğrulama sunucusu arasında gidip gelen paketleri TLS

tüneli ile şifreleyerek gönderir. Microsoft, Cisco ve RSA Security'nin geliştirdiği, şu an IEFT standardı olan bir kimlik doğrulama metodudur. EAP-TLS protokolüne benzer. Farklı olarak sunucu, kullanıcıyı dijital bir sertifika ile doğrulamaz. Kimlik doğrulama bilgilerini güvenli bir şekilde taşımak için şifrelemeye dayalı protokolleri (legacy password-based protocols) kullanan metottur. EAP-TTLS'ten farkı ise PAP, CHAP gibi az güvenlikli kimlik doğrulama metodlarının kullanımını engelleyerek MS-CHAPv2 gibi yüksek güvenlikli metodların kullanımını zorunlu tutar. PEAP güvenli transferi istemci ile sunucu arasına kurduğu tünel ile sağlar. Aynı TTLS de olduğu gibi PEAP da kablosuz ağ istemcisinin sadece sunucu bazlı sertifika kullanarak kimliğini doğrular. Bu da yönetimsel olarak büyük bir kolaylık sağlar.

PEAP, EAP kimlik doğrulama yöntemlerine ek güvenlik özellikleri katan EAP-MS-CHAPv2 adında, TLS tüneli içerisinde çalışabilen yeni bir yöntem kullanır. Paketlerin şifreli tünel içerisinden gitmesi birçok atağa karşı dayanıklılık sağlar.

PEAP bir kimlik doğrulama yöntemi belirtmez, ancak PEAP tarafından sağlanan TLS şifreli kanalı aracılığıyla çalışabilen Genişletilebilir Kimlik Doğrulama Protokolü-Microsoft Karşılıklı Kimlik Doğrulama Protokolü (EAP-MSCHAPv2) gibi diğer EAP kimlik doğrulama protokolleri için ek güvenlik sağlar.

PEAP hem EAP protokollerini hem de ağ güvenliğini geliştirmek için şunları sağlar :

- İstemci ile sunucu arasında oluşan EAP yöntemi görüşmesi için koruma sağlayan bir TLS kanalı. Bu TLS kanalı bir saldırganın istemci ile ağ erişim sunucusu arasında paket sızdırarak daha az güvenli bir EAP türünde görüşmeye neden olmasının engellenmesine yardımcı olur. Şifreli TLS kanalı ayrıca Kimlik Doğrulama sunucusunda hizmet reddi saldırılarının engellenmesine yardımcı olur.
- İletilerin parçalanması ve yeniden montajı desteği, bu işlevselliği sağlamayan EAP türlerinin kullanılmasına olanak verir.

- İstemciler, Kimlik Doğrulama sunucusunun veya başka bir RADIUS sunucusunun kimlik doğrulamasını yapabilir. Sunucu aynı zamanda istemcinin kimlik doğrulamasını yaptığı için, karşılıklı kimlik doğrulama gerçekleşir.
- EAP istemcisinin Kimlik Doğrulama sunucusu tarafından sağlanan sertifikanın kimlik doğrulamasını yaptığı sırada yetkili olmayan bir kablosuz erişim noktasının dağıtılmasına karşı koruma sağlanır. Ayrıca, PEAP doğrulayıcısı ve istemci tarafından oluşturulan TLS ana sırrı erişim noktasıyla paylaşılmaz. Bu nedenle, erişim noktası PEAP tarafından korunan iletilerin şifresini çözemez.
- Bir istemci tarafından yapılan kimlik doğrulama isteği ile Kimlik Doğrulama sunucusu veya başka bir RADIUS sunucusunun yanıt vermesi arasındaki gecikmeyi azaltan PEAP hızlı yeniden bağlanma. PEAP hızlı yeniden bağlanma aynı zamanda yeniden kimlik doğrulama isteği gönderilmesine gerek kalmadan, kablosuz istemcilerin aynı RADIUS sunucusu için RADIUS istemci olarak yapılandırılmış erişim noktaları arasında hareket etmelerine olanak verir. Böylece, hem istemci hem de sunucu gereksinimleri azaltılır ve kullanıcılardan kimlik bilgileri istenme sayısı en aza indirilir.

PEAP kimlik doğrulama işleminde PEAP istemcisi ile doğrulayıcı arasında iki aşama vardır. İlk aşamada, PEAP istemcisi ile kimlik doğrulama sunucusu arasında bir güvenli kanal oluşturulur. İkinci aşamada, PEAP istemcisi ile doğrulayıcı arasında EAP kimlik doğrulaması sağlanır.

Faz-1: Güvenli TLS tüneli oluşturma

PEAP kimlik doğrulamasının ilk aşamasında, PEAP istemcisi ile Kimlik Doğrulama sunucusu arasında TLS kanalı oluşturulur. Aşağıdaki adımlarda, bu TLS kanalının kablosuz PEAP istemciler için nasıl oluşturulduğu gösterilmektedir.

1. PEAP istemcisi, kimlik doğrulama amacıyla çalışan bir sunucuya RADIUS istemcisi olarak yapılandırılmış bir kablosuz erişim noktasıyla ilişkilendirilir. PEAP istemcisi ile erişim noktası arasında güvenli bir ilişki oluşturulması için IEEE 802.11 tabanlı ilişki ilk olarak bir açık sistem veya paylaşılan anahtar kimlik doğrulaması sağlar.

2. İstemci ile erişim noktası arasında IEEE 802.11 tabanlı ilişki oluşturulduktan sonra, erişim noktasıyla TLS oturumu görüşülür.
3. Kablosuz PEAP istemcisi ile Kimlik Doğrulama sunucusu arasında bilgisayar düzeyinde kimlik doğrulaması başarıyla tamamlandıktan sonra, TLS oturumu bunların arasında görüşülür. Bu görüşme sırasında türetilen anahtar, kullanıcının kuruluş ağına bağlanmasına izin veren ağ erişimi kimlik doğrulaması da dahil olmak üzere sonraki tüm iletişimi şifrelemek için kullanılır.

Şekil 3.3. Faz-1'de TLS tünelinin kurulması

Faz-2: EAP ile kimlik doğrulama

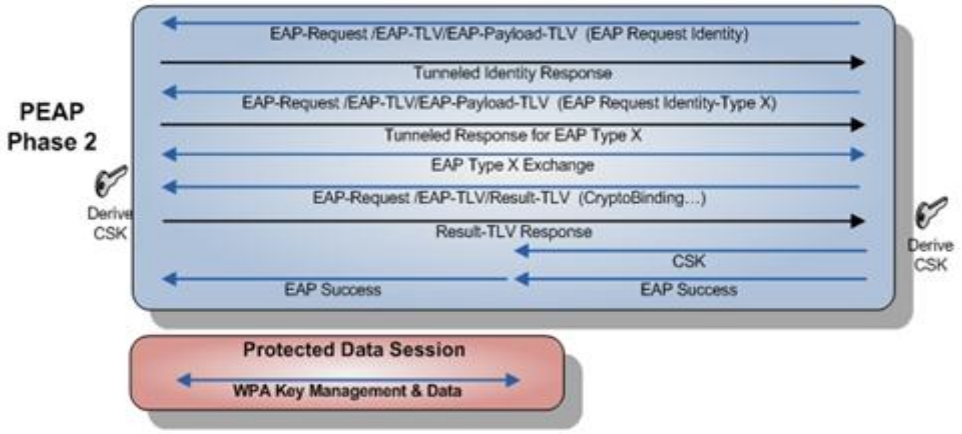
EAP görüşmesi de dahil tüm EAP iletişimi, TLS kanalı üzerinden gerçekleşir ve PEAP kimlik doğrulamasının ikinci aşamasıdır. Aşağıdaki adımlarda önceki örnek genişletilerek, kablosuz istemcilerin PEAP kullanarak Kimlik Doğrulama sunucusuyla kimlik doğrulama işlemini nasıl tamamladığı gösterilir.

1. Kimlik doğrulama sunucusu ile PEAP istemcisi arasında TLS kanalı oluşturulduktan sonra, istemci kimlik bilgilerini (kullanıcı adını ve parolayı veya kullanıcı ya da bilgisayar sertifikasını) şifreli kanal üzerinden kimlik doğrulama sunucusuna aktarır.

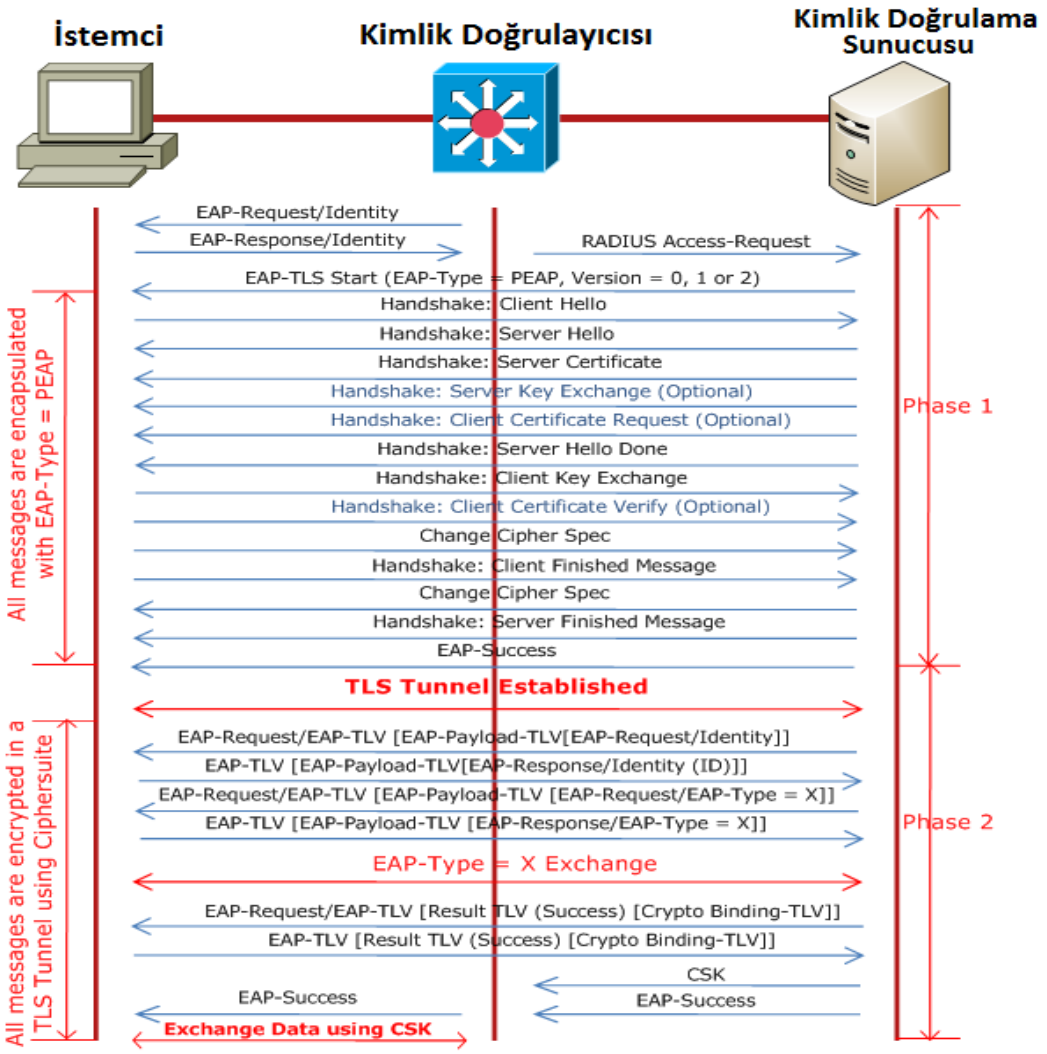
2. Erişim noktası iletileri yalnızca kablosuz istemci ile RADIUS sunucusu arasında iletir; erişim noktası veya onu izleyen bir kişi, TLS uç noktası

olmadığı için bu iletilerin şifresini çözemez.

3. Kimlik Doğrulama sunucusu, PEAP ile kullanılmak üzere seçilen kimlik doğrulama türüyle kullanıcının ve istemci bilgisayarın kimliğini doğrular. Kimlik doğrulama yöntemi EAP-MS-CHAPv2'dir



Şekil 3.4. Faz-2'de kimlik doğrulamanın gerçekleşmesi



Şekil 3.5. PEAP fazları

EAP-MSCHAPv2 kimlik doğrulama yöntemi

Kullanıcı kimlik doğrulaması, sertifikalar veya akıllı kartlar yerine parola tabanlı kimlik bilgileri kullanılarak gerçekleştirilir. PEAP-MSCHAPv2 kimlik doğrulamasının başarılı olması için, istemcinin sunucu sertifikasını inceledikten sonra kimlik doğrulama sunucusuna güvenmesi gerekir. İstemcinin kimlik doğrulama sunucusuna güvenmesi için, sunucu sertifikasını yayımlayan sertifika yetkilisinin (CA), istemci bilgisayarlardaki Güvenilen Kök Sertifika Yetkilileri sertifika deposunda kendine ait bir sertifikası olması gerekir.

Kimlik Doğrulama Sunucusu tarafından kullanılan sunucu sertifikası, kuruluşunuzun güvenilen kök CA'sı veya istemci bilgisayar tarafından zaten güvenilen VeriSign ya da Thawte gibi bir ortak CA tarafından yayımlanabilir.

Çizelge 3.1 PEAP'ta kullanılan kimlik doğrulama yönteminin özellikleri

Özellik/İşlev	MS-CHAPv2	PEAP-MS-CHAPv2
Parolalar kullanılarak istemci kimlik doğrulaması yapılmasını sağlar	Evet	Evet
Sunucunun kimlik bilgilerine erişimi olmasını sağlar	Evet	Evet
Sunucunun kimlik doğrulamasını yapar	Evet	Evet
Kablosuz erişim noktası sızdırmasını engeller	Hayır	Evet
Yetkili olmayan sunucununaz güvenli kimlik doğrulama yöntemiyle görüşmesini engeller	Hayır	Evet
Bir ortak anahtar tarafından oluşturulan TLS anahtarlarını kullanır	Hayır	Evet
Sıra ile şifreleme sağlar	Hayır	Evet
Sözlük veya kaba kuvvet saldırılarını engeller	Hayır	Evet
Yeniden gönderme saldırılarını engeller	Hayır	Evet
Kimlik doğrulama yöntemlerinin zincir olarak kullanılmasına izin verir	Hayır	Evet
Sunucu tarafından sağlanan sertifikalar için istemci güveni gerektirir	Hayır	Evet

4. GELİŞTİRİLEN PROTOKOL : E-PEAP

Bütün EAP kimlik doğrulama mekanizmalarında olduğu gibi PEAP'ta da tünelin kurulması için gerekli parametreler üzerinde anlaşılan başlangıç fazı kriptosuz ve korunmasız olarak gerçekleşmektedir. PEAP, 1. fazda kullanılan gerçek kullanıcı kimliğini saklamak için anonim kimlik (anonymous identity) tanımlanmasını olanaklı kılsa da bu özellik zorunlu değil opsiyoneldir. PEAP'ı kullanarak ağa bağlanmak isteyen kullanıcı konfigürasyon sırasında anonim kimlik tanımı yapmayı unutabilir veya her defasında anonim bir kimlik girmeyi pratik bulmayabilir. Bu tür yaklaşımlar ağı Faz-1 ataklarına karşı savunmasız ve korumasız bırakacaktır. Bu zaafiyeti ortadan kaldırmak ve Faz-1 ataklarına karşı daha güçlü kılmak için E-PEAP (Enhanced PEAP) protokolü geliştirip uygulanmıştır.

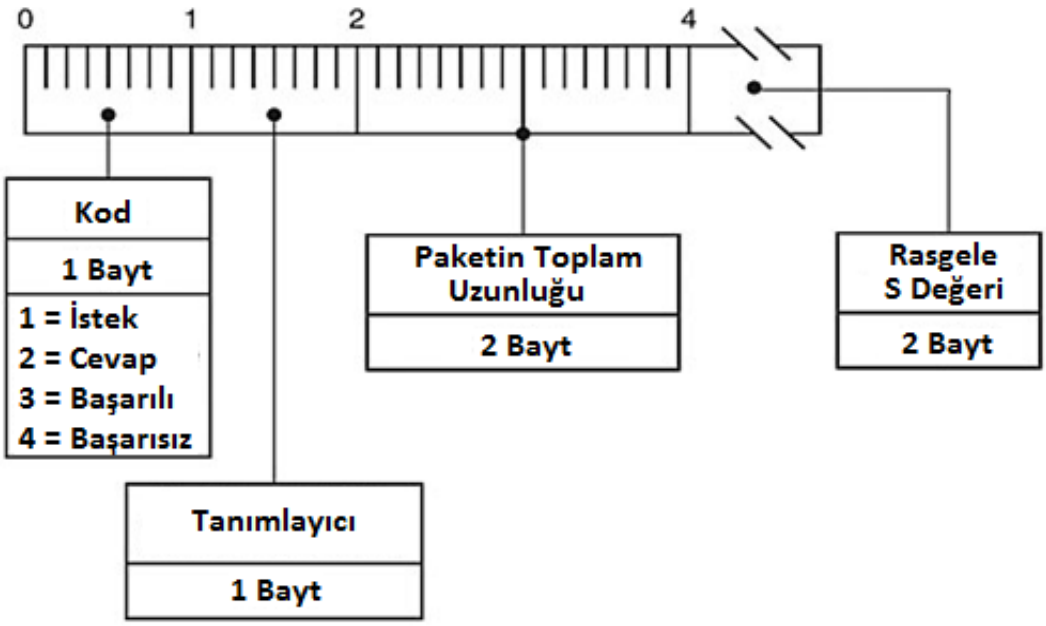
Geliştirdiğimiz protokol ile kimlik bilgisi kablosuz ortamda hiçbir zaman açık olarak gönderilmemekte, her oturumda (session) dinamik anahtarlar ile kriptolanarak taşınmaktadır. Bu sayede MITM (Man-In-The-Middle), Sözlük, Tekrar ataklarına karşı daha güçlü bir kimlik doğrulama protokolü geliştirilmiştir.

4.1. Çerçeve Mimarisi

RFC 3748'de tanımlandığı üzere EAP protokolü sadece 4 adet türde paket gönderebilir: Sorgu (Request), Cevap (Response), Başarılı (Success), Başarısız (Failure). Sorgu ve Cevap mesajları kimlik bilgisini sorgulamak ve gelen cevabı taşımak üzere Tip (Type) alanına sahiptir. Buna göre, Sorgu mesajında tip olarak kimlik bilgisi isteniyorsa, istemci bu isteğe cevap olarak göndereceği paketin içerisine ağa bağlanmak istediği kullanıcı adını (identity) koyarak gönderir.

Tasarladığımız protokolde, sunucu ile istemci arasında gerçekleşen bu kimlik bilgisi sorgu-cevap paketleri içerisinde 2 baytlık, Merkle's Puzzle çalışmasında kullanılmış olan S_Değeri adında yeni bir veri alanı oluşturulmuştur. Bu anahtar taşıma yöntemi için Merkle's Puzzle şeması [17] kullanılmıştır. Bu veri alanı, sunucudan istemciye gönderilen kimlik sorgu paketleri içerisinde daha önceden oluşturduğumuz S

veritabanından rastgele bir değerin istemciye ulaştırılmasını sağlamaktadır. 2 baytlık bu veri alanı 1-65535 aralığında onaltılık tipte veri taşıyabilmektedir.

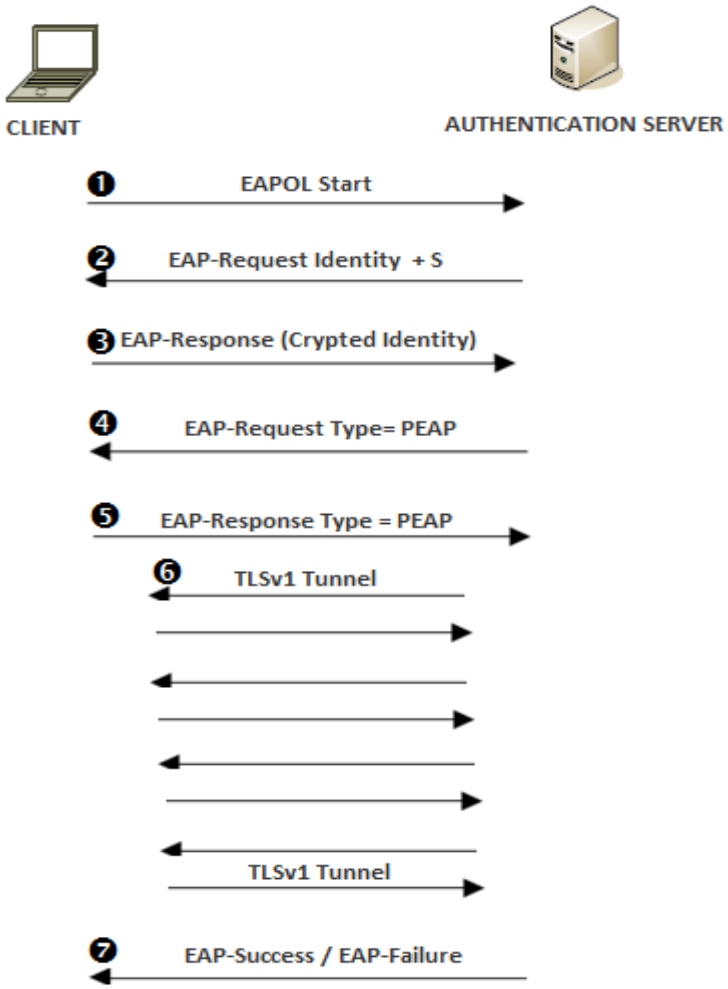


Şekil 4.1. Değiştirilmiş EAP çerçevesi

4.2. Protokolün Çalışması

Geliştirilen protokol, Faz-1'deki kimlik bilgisini dinamik anahtar dağıtım yöntemi ile şifreleyerek kimlik bilgisinin Faz-1 güvenliğini arttırmaktadır. Bunu sağlamak için sunucu ve istemci tarafında, herbiri güçlü bir şifreleme anahtarı ile ilişkili olan 10,000 adet S değeri tanımlanmıştır. İstemci "EAPOL-Başlangıç (1)" mesajı gönderdiğinde kimlik doğrulama sunucusu EAP-İstek mesajı (2) ile istemcinin kimlik bilgisini isterken aynı zamanda oluşturduğumuz 16 bitlik S veri alanı içerisine 10,000 S değerinden bir tanesini rastgele istemciye gönderir. Gönderilen S değeriyle ilişkili şifreleme anahtarının tahmin edilmesini önlemek için, EAP-İstek mesajları ve içerisindeki S değeri üç saniyede bir tazelenir. 3 saniye içerisinde EAP-İstek mesajına cevap alamayan sunucu, yeni bir S değerini istemciye yollar. EAP-İstek mesajını ve S değerini alan istemci, kendinde varolan veritabanını kontrol ederek S değerine karşılık gelen doğru şifreleme anahtarını bulur. Gerçek kimlik bilgisini bu

şifreleme anahtarı birlikte özelleştirilmiş bir XOR şifreleme algoritmasından geçirerek yalın kullanıcı adını şifreleyerek şifreli kimlik bilgisini elde eder ve bu şifreli kullanıcı ad bilgisini EAP-Cevap paketi (3) içerisinde gönderir. EAP-İstek mesajına karşılık gelen EAP-Cevap paketi içerisinde gelen şifreli kullanıcı ad bilgisini alan sunucu, bir önceki mesajda gönderdiği S değerine karşılık gelen şifreleme anahtarını bu sefer şifreli kullanıcı ad verisini çözmek için kullanır. Gerçek kullanıcı ad verisini artık öğrenen sunucu, kullanıcı veritabanında gerekli kontrolleri yaparak istek yapan kullanıcının Faz-1 kimliğini doğrulamaya çalışır. Faz-1 kimliği doğrulandığı takdirde, bir önceki oturumda kullanılmış olan S değeri ve ona karşılık gelen şifreleme anahtarı arasındaki ilişki sunucu ve istemci tarafında kırılarak veritabanında bulunan farklı değerlerle eşleşmeleri sağlanır. Örneğin, sunucu Şekil 4.3'te gösterilen S veritabanından S değeri olarak 50871 göndermiş, istemci gerçek kimlik bilgisini 10894 ile şifrelemiş ve Faz-1 başarıyla geçilmiş ise, sunucu ve istemci S veritabanlarını kullanılan algoritma sonucunda belirlenen değerlere göre yeniden düzenler. Buna göre oluşan yeni S veritabanında 50871 olan S değerine karşılık gelen şifreleme anahtarı artık 10894 değil, bir başka değer, örneğin 96498 olacaktır. Bu geliştirme, ağı dinleyen bir saldırganın, S değerine bağlı olarak tekrar paket gönderme saldırılarını tamamen zararsız ve geçersiz kılmaktadır. EAP entegrasyonu ve paket alışverişi Şekil 4.2'de gösterilmektedir.



Şekil 4.2. E-PEAP'ın EAP'a entegrasyonu

Bilindiği gibi PEAP bir tünelleme metodudur. Tünel metodlarının birincil faydası kimlik ve diğer oturum bilgilerini gizleyebilmesidir. Tünel kullanıldığında ağı dinlemekte olan saldırganın, istemcinin kimlik bilgileri ele geçirmesi oldukça zorlaşır. Fakat tünel mekanizması Faz-2 verilerinin ele geçmesini önlemektedir. Faz-1'deki kimlik bilgileri için önerilen anonim kimlik, güvenlik seviyesini son kullanıcının dikkatine bırakmaktadır. Bu şekilde tasarlanan bir ağ hiçbir zaman tam olarak güvenli sayılamaz. Tasarladığımız protokol ile istemcinin Faz-1 kimlik bilgileri de dinamik anahtarlar ile şifrelenmekte, ağa bağlanmak isteyen son kullanıcı anonim kimlik kullanmasa bile güvenli kimlik doğrulama sağlanmaktadır.

4.3. E-PEAP Geliştirmeleri

Veritabanlarının oluşturulması

İstemci ve sunucuda rasgele belirlenen10,000 adet S değeri ve bu değerlere karşılık gelen kripto anahtarı içeren veritabanları oluşturulmuştur. Sunucu veri tabanındaki 50871 değeri istemci tarafında c6b7 hex değerine eşittir. Veritabanları şekildeki gibidir :

SERVER Database

```
int dizi[10000][2]={
// S , encryption_key
{50871,"10894"},
{42452,"96498"},
{61687,"10578"},
{63219,"65353"},
{47073,"94092"},
{50592,"99061"},
{61924,"71969"},
{47524,"70639"},
{42146,"58069"},
{41890,"55282"},
{58597,"72053"},
{45521,"63359"},
{42664,"20668"},
{58617,"67657"},
{42160,"87418"},
{62421,"34182"},
{47558,"65493"},
{59857,"56455"},
{46260,"50242"},
{51671,"96374"},
{58856,"35317"},
{42993,"82758"},
{50338,"25985"},
{53713,"28842"},
{42152,"84147"},
{61625,"86003"},
{51394,"11621"},
{58803,"73510"},
{50080,"78963"},
  ---
  ---
```

CLIENT Database

```
int dizi[10000][3]={
  // S ,          encryption_key
{0xffffffc6,0xffffffb7,"10894"},
{0xffffffa5,0xffffffd4,"96498"},
{0xfffffff0,0xfffffff7,"10578"},
{0xfffffff6,0xfffffff3,"65353"},
{0xffffffb7,0xffffffe1,"94092"},
{0xffffffc5,0xffffffa0,"99061"},
{0xfffffff1,0xffffffe4,"71969"},
{0xffffffb9,0xffffffa4,"70639"},
{0xffffffa4,0xffffffa2,"58069"},
{0xffffffa3,0xffffffa2,"55282"},
{0xffffffe4,0xffffffe5,"72053"},
{0xffffffb1,0xffffffd1,"63359"},
{0xffffffa6,0xffffffa8,"20668"},
{0xffffffe4,0xfffffff9,"67657"},
{0xffffffa4,0xffffffb0,"87418"},
{0xfffffff3,0xffffffd5,"34182"},
{0xffffffb9,0xffffffc6,"65493"},
{0xffffffe9,0xffffffd1,"56455"},
{0xffffffb4,0xffffffb4,"50242"},
{0xffffffc9,0xffffffd7,"96374"},
{0xffffffe5,0xffffffe8,"35317"},
{0xffffffa7,0xfffffff1,"82758"},
{0xffffffc4,0xffffffa2,"25985"},
{0xffffffd1,0xffffffd1,"28842"},
{0xffffffa4,0xffffffa8,"84147"},
{0xfffffff0,0xffffffb9,"86003"},
{0xffffffc8,0xffffffc2,"11621"},
{0xffffffe5,0xffffffb3,"73510"},
{0xffffffc3,0xffffffa0,"78963"},
  ---
  ---
```

Şekil 4.3. Şifreleme anahtarları ve S değerlerinin yer aldığı veritabanları

Örneğin, sunucu S değeri olarak 50871 gönderirse, istemci gerçek kimlik bilgisini 10894 şifreleme anahtarıyla kriptolayarak sunucuya gönderir.

Hostapd ve WPA_Supplicant için E-PEAP geliştirmeleri

Hostapd ve wpa_supplicant programlarının E-PEAP için optimizasyonu c++ ile gerçekleştirilmiştir.

5. PROTOKOLÜN UYGULAMASI

Tasarlanan protokol gerçek ortam da test edilmiş, başarıyla çalıştığı görülmüştür. İşletim sistemi olarak Ubuntu, Linux 3.0.0-21 kullanılmıştır.

Sertifikaların üretilmesi ve imzalanması için OpenSSL (versiyon: openssl-1.0.1c.tar.gz), açık kaynak kodlu PEAP uygulaması için sunucu tarafında Hostapd (versiyon: hostapd-0.7.3.tar.gz) istemci tarafında WPA_Supplicant (versiyon: wpa_supplicant-1.0.tar.gz) kullanılmıştır.

5.1. OPENSSL ile Sunucu Sertifikasının Oluşturulması

OpenSSL [21] projesi güvenliği geliştirmek için çaba harcayan ticari, geniş özellikli ve açık kaynak kodlu, Güvenli Soket Katmanı (SSL v2/v3), İletim Seviyesi güvenliği (TLSv1) protokollerini uygulayan, çok güçlü genel amaçlı bir şifreleme kütüphanesidir. Bu proje bütün dünyada iletişim, plan ve OpenSSL araçlarını geliştirmek için interneti kullanan gönüllüler topluluğu tarafından yönetilir.

OpenSSL Eric A. Young ve Tim J. Hudson tarafından geliştirilen SSLeay kütüphanesi temellidir. OpenSSL aracı ticari ve ticari olmayan özel amaçlar için kullanmakta özgür olunan Apache lisansı ile lisanslanmıştır.

Açık kaynak kodlu yazılımlarla güvenli bir Unix sunucu kurmak için temeldir; mod_ssl, OpenSSH ve şifreli veri işlemeyi sağlayan ürünler gibi bütün ürünler buna ihtiyaç duyar.

5.2. Openssl Kurulumu

```
sudo apt-get install libssl-dev
wget http://www.openssl.org/source/openssl-1.0.1c.tar.gz
tar -xvzf openssl-1.0.1c.tar.gz
cd openssl-1.0.1c/
./config --prefix=/usr/local/openssl --openssldir=/usr/local/openssl
```

```
sudo make
sudo make install
```

5.3.1. CA sertifikasının oluşturulması

```
openssl genrsa 2048 ca-key.pem
openssl req -new -x509 -nodes -days 3600 -key ca-key.pem -out ca-cert.pem
```

5.3.2. Sunucu sertifikasının oluşturulması ve imzalanması

```
openssl req -newkey rsa:2048 -days 3600 -nodes -keyout server-key.pem -out
server-req.pem
openssl rsa -in server-key.pem -out server-key.pem
openssl x509 -req -in server-req.pem -days 3600 \
    -CA ca-cert.pem -CAkey ca-key.pem -set_serial 01 -out server-cert.pem
```

(server-cert.pem = public key, server-key.pem = private key)

5.3.3. Sertifikanın testi

```
openssl verify -CAfile ca-cert.pem server-cert.pem
server-cert.pem: OK
```

Oluşturulan sertifika otoritesi sertifikası(ca-cert.pem) client bilgisayarında güvenilir kök sertifikalar dizininin altına kopyalanır.

5.4. Kablosuz Adaptör Kurulumu

Çalışmada, erişim noktası özelliği olan Edimax ew-7711UMn USB adaptör kullanılmıştır.

```
lspci -k | grep -A 3 -i "network"
lsusb : Bus 002 Device 003: ID 7392:7711 Edimax Technology Co. Ltd EW-
7711UTn nLite Wireless Adapter [Ralink RT2870] driver=rt2800usb
```

5.5. Hostapd ve wpa_supplicant

5.5.1. Hostapd kurulumu ve E-PEAP konfigürasyonu

Hostapd [18], Kablosuz usb adaptörün erişim noktası olarak çalışmasını sağlayacak, açık kaynak kodlu yazılımdır. Kimlik doğrulayıcı sistem üzerinde çalışarak istemcilerden gelen erişim isteklerini değerlendirir.

Kurulumu

```
wget http://w1.fi/releases/hostapd-0.7.3.tar.gz
tar -xvzf hostapd-0.7.3.tar.gz
cd hostapd-0.7.3/hostapd
cp defconfig .config
sudo make
sudo install
```

E-PEAP konfigürasyonu (hostapd.conf)

```
interface=wlan1
driver=nl80211
ssid=EnhancedPEAP
ieee8021x=1
channel=6
hw_mode=g
wpa=3
wpa_key_mgmt=WPA-EAP
wpa_pairwise=TKIP CCMP
rsn_pairwise=CCMP
wpa_group_rekey=3600
wpa_gmk_rekey=3600
auth_algs=1
eap_server=1
auth_server_addr= 127.0.0.1
```

auth_server_port= 1812

eap_user_file=/home/cagdas/hostapd-0.7.3/hostapd/hostapd.eap_user

server_cert=/home/cagdas/server-cert.pem

ca_cert=/home/cagdas/ca-cert.pem

private_key=/home/cagdas/server-key.pem

hostapd.eap_user

"deneme" PEAP

"cagdaskurt" PEAP

"sybl" PEAP

"cagdaskurt" MSCHAPV2 "master_tezi2012" [2]

"deneme" MSCHAPV2 "deneme" [2]

"sybl" MSCHAPV2 "gonuer" [2]

5.5.2. wpa_supplicant kurulumu ve E-PEAP konfigürasyonu

WPA_Supplicant [19], Linux işletim sistemlerinde, WPA ve üzeri güvenlik seviyesindeki kablosuz ağlara baglanabilmek icin kullanılan açık kaynak kodlu bu araç, istemcilerin 802.1x denetimi ile kablosuz ağa bağlanabilmelerini sağlar.

Kurulumu

sudo wget http://hostap.epitest.fi/releases/wpa_supplicant-1.0.tar.gz

tar -xvzf wpa_supplicant-1.0.tar.gz

cd wpa_supplicant-1.0/wpa_supplicant

cp defconfig .config

sudo make

sudo install

E-PEAP konfigürasyonu (wpa_supplicant.conf)

networkssid="EnhancedPEAP "

key_mgmt=WPA-EAP

```
eap=PEAP
pairwise=TKIP
group=TKIP
phase1="peapver=0"
phase2="MSCHAPV2"
identity="cagdas"    (real_identity, not anonymous)
password="kurt"
```

PEAP, konfigürasyonlardan da görüldüğü gibi sadece sunucu tarafında sertifika kullanmaktadır. İstenirse istemci tarafında da sertifika kullanılabilmektedir fakat bu durum operasyonel anlamda zorluklara yol açabilmektedir.

5.6. DHCP Konfigürasyonu

/etc/dhcpd.conf

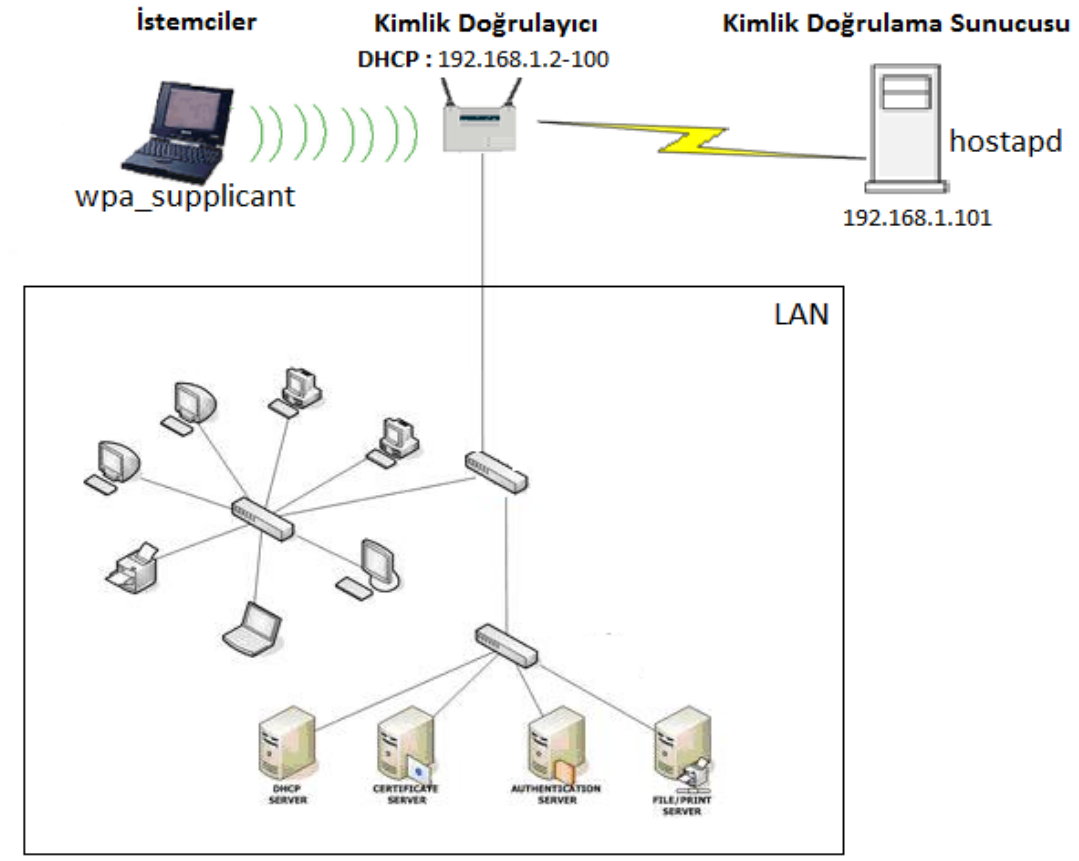
```
subnet 192.168.1.0 netmask 255.255.255.0
{
range 192.168.1.2 192.168.1.100;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.1;
option domain-name-servers 192.168.1.1;
option interface-mtu 1492;
}
```

5.7. Deneysel Sonuçlar ve Güvenlik Analizi

Geliştirilen protokolün testi için Şekil 5.1'deki gibi bir test ortamı kurulmuştur. Ağa bağlanmak isteyen kullanıcı açık kaynak kodlu, PEAP protokolü geliştirilmiş wpa_supplicant kullanır. Kimlik doğrulama sunucusu üzerinde açık kaynak kodlu hostapd-0.7.3 programı çalışmaktadır. Kablosuz Erişim Noktası olarak Edimax EW-

7811Un cihazı kullanılmaktadır. Her iki sistemde de 3.0.0-21 versiyonlu Ubuntu, Linux işletim sistemi çalışmaktadır.

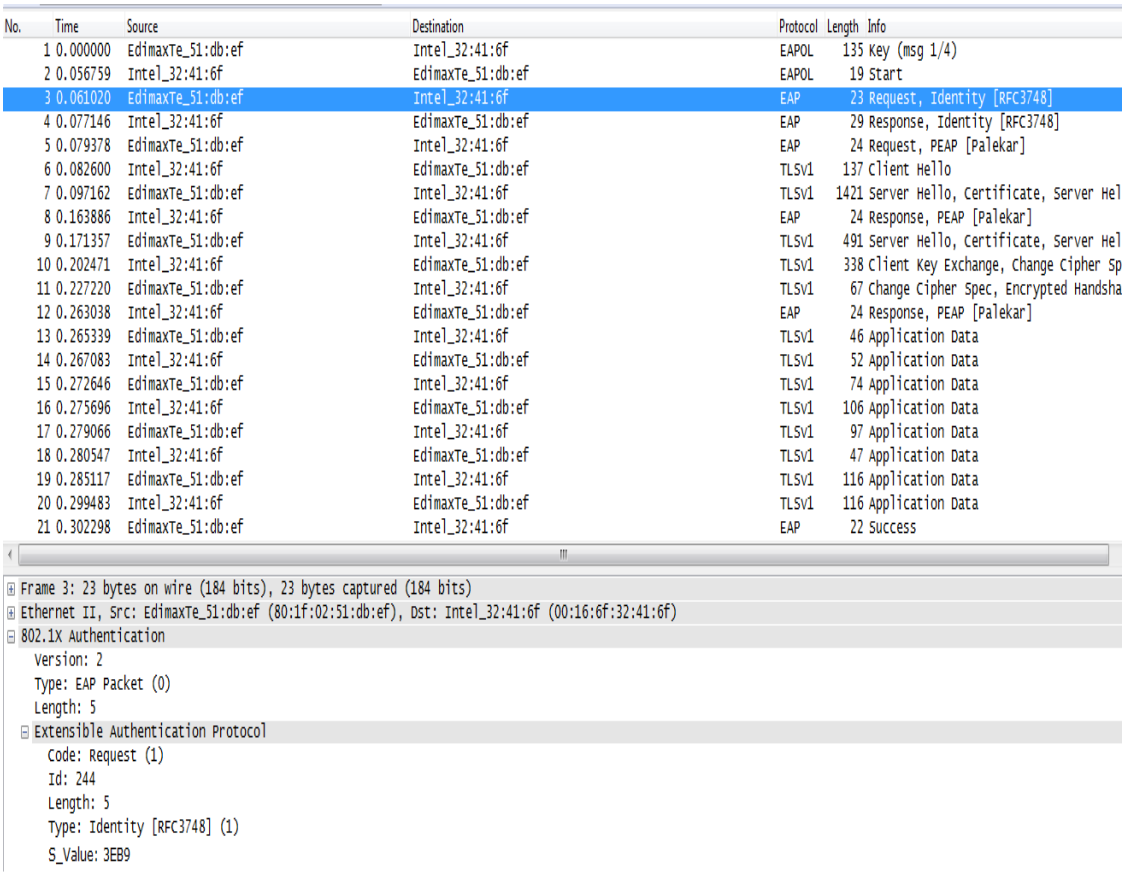
Testin amacı, PEAP protokolü optimize edilmiş istemcinin kimliğinin doğrulanmasını, Faz-1 kimlik bilgilerinin yukarıda anlatıldığı şekilde dinamik anahtarlama yöntemi ile şifrelendiğini göstermek, protokolün gerçeklemesini yapmaktır.



Şekil 5.1. Test topolojisi

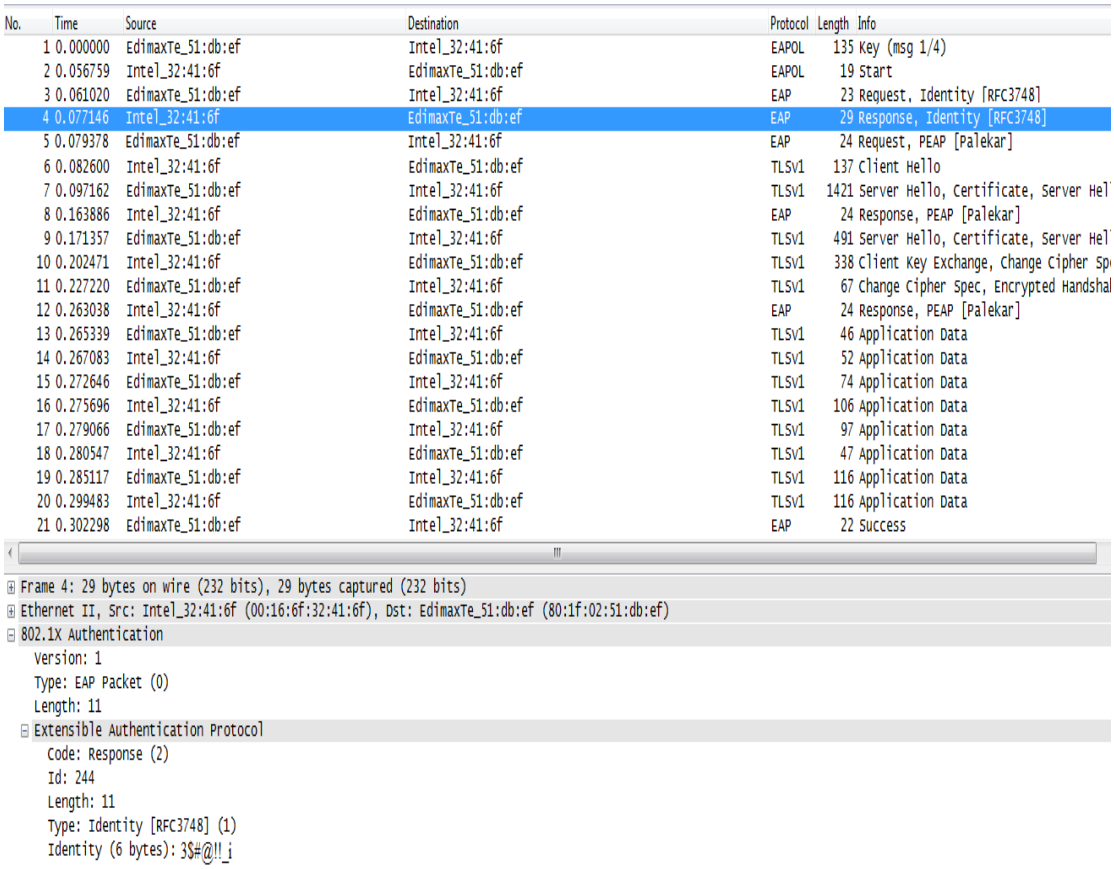
Paket izleyici araç olarak Wireshark [20] (versiyon: 1.5.1) kullanılarak kablosuz ortamda istemci ve sunucu arasında gidip gelen kimlik doğrulama mesajları incelenmiştir. Yakalanan paketlerde yapılan incelemelerde geliştirilen protokolün istendiği gibi çalıştığı görülmüştür.

Şekil 5.2'de sunucunun gönderdiği EAP-İstek mesajlarına 2 byte'lık 3EB9 değerinin enjekte edildiği, Şekil 5.3'te ise istemcinin EAP-Cevap mesajında, kimlik bilgisini EAP-İstek mesajında gelen S değeri ile şifrelediği görülmektedir.



Şekil 5.2. Rastgele S değeri içeren EAP-İstek paketi

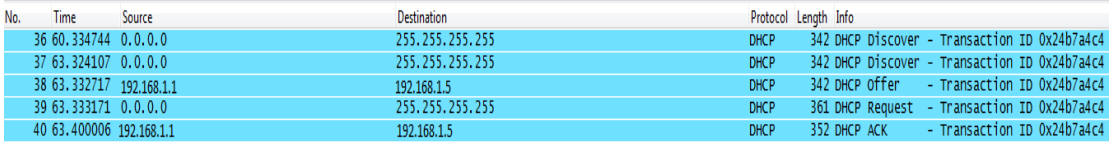
Şekil 5.2'de EAPOL paketleri ile kimlik doğrulama sürecine hazırlanan istemciye Erişim Noktası EAP-Sorgu/Kimlik mesajı yollayarak EAP sürecini başlatmaktadır. EAP paket yapısına istendiği gibi 10.000 değer arasından rasgele seçilen bir S değeri enjekte edilmiştir. Ağa bağlanmak isteyen istemcinin, kimlik bilgisini bu S değerine karşılık gelen şifreleme anahtarı ile şifreleyerek göndermesi beklenmektedir.



Şekil 5.3. Şifreli kimlik bilgisi taşıyan EAP-Cevap paketi

Şekil 5.3'te kimlik bilgisinin istenen şifreleme anahtarıyla şifrelendiği görülmektedir. Şifreleme anahtarı kabul edildiği için kimlik doğrulama süreci devam etmekte ve en sonunda erişim noktası EAP-Success mesajı ile istemcinin kimliğinin doğrulandığını, ağa bağlanabileceğini bildirir.

Kimlik doğrulaması sağlanan istemcinin ağa bağlanabilmesi için DHCP-Sunucusunda tanımlanan ip bloğundan ip verilir



Şekil 5.4. Kimliği doğrulanan istemciye otomatik IP atanması

5.7.1. Güvenlik analizi

Bu bölüm, protokolümüzün ataklara karşı direncini ve özelliklerini göstermektedir. EAP metoduna yönelik saldırılar, şifresiz paket içersindeki verilerin okunarak kullanıcı bilgilerinin elde edilmesini, yaygın kullanılan kelimelerin denendiği sözlük saldırılarını, tekrar ataklarını içermektedir [22,23].

Kimlik gizliliği

Kimlik gizliliği daha önce belirtildiği gibi, kullanıcının kullanıcı ad, eposta adresi, domain bilgisi gibi bilgilerinin ağı dinleyen saldırganlar tarafından elde edilmesinin önüne geçilmesidir. Güvenli tünel kurmak için gerekli olan Faz-1 kimlik bilgileri normal şartlarda şifrelenmeden gönderilmektedir. Bu fonksiyon için anonymous kullanıcı ad özelliği olsa da uygulamada bu özellik kullanılmamakta, kullanıcılar Faz-1 ve Faz-2 için aynı kullanıcı adı kullanmaktalar. Ayrıca, ağ güvenliğini kullanıcıların eğilimlerine bağlamak çok geçerli bir tutum değildir. Bu ihtiyaçlardan dolayı çalışmada Faz-1 kullanıcı bilgilerin (credentials) değişimi kablosuz ortamda dinamik anahtarlar tarafından şifrelenerek yapılmaktadır. Kullanıcının girdiği bilgiler, 3 saniyede bir farklı bir anahtar ile şifrelenerek anahtarın tespiti oldukça zorlaştırılmıştır. Çok güçlü bilgisayarlar kullanılarak anahtar tespit edilmiş olsa dahi, dinamik şifre anahtar veritabanı sayesinde daha önce kullanılan S değeri sonraki kullanımda başka bir anahtar ile eşleşeceğinden saldırganın 3 saniye içerisinde bu dinamik yapıda şifrelenmiş verileri tespit edemeyeceği yapılan testlerde görülmüştür.

Tekrar atağı

Tekrar atağı, saldırganın geçerli kimlik doğrulama paketlerini biriktirerek, daha sonraki kimlik doğrulama sürecinde tekrar kullanmaktır. Bu saldırıyı önleyebilmek için her oturumda farklı anahtarlar kullanmak gerekmektedir. Geliştirilen protokolde Faz-1 kimlik bilgilerinin tekrar atağında kullanılmasını engelleyecek dinamik şifreleme anahtarı mekanizması kullanılmaktadır. Her başarılı kimlik doğrulama işlemi sonucu şifreleme

anahtarı değişmekte, bu da tekrar ataklarına karşı güçlü bir direnç sağlamaktadır.

Semantik güvenlik

Semantik güvenlik özelliği, ele geçirilen yeterli sayıda şifrelenen verinin şifreleme örüntüsünü ve kullanılan şifreleme anahtarını saptayabilmektir. Şifreleme örüntüsünün saptanmaması, dinamik anahtarlama yöntemiyle çözülebilecek bir sorundur. E-PEAP'ta bir önceki oturumda kullanılmış olan S değeri ve ona karşılık gelen şifreleme anahtarı arasındaki ilişki sunucu ve istemci tarafında kırılarak veritabanında bulunan farklı değerlerle eşleşmeleri sağlanır. Bu şekilde, ağı dinleyen bir saldırganın şifrelenmiş paketleri toplayarak şifreleme örüntüsünü ve şifreleme anahtarını bulması engellenmektedir.

Sözlük atağı

Ağda dolaşan şifreli kullanıcı ad bilgisi her seferinde farklı şifreleme anahtarı ile şifrelendiği için sözlük atağının başarılı olması mümkün olmamaktadır.

Çizelge 5.1'de protokollerin güvenlik özelliklerine göre karşılaştırmasına yer verilmiştir. E-PEAP sayesinde Faz-1'de kullanıcı kimliğinin saklanması mümkün olmuştur.

Çizelge 5.1. Protokollerin güvenlik incelemesi

Gereklilikler	EAP-MD5	EAP-TLS	EAP-TTLS	EAP-LEAP	EAP-PEAP	EAP-SPEKE
Anahtarlama materyalinin oluşturulması	Hayır	Gerekli değil	Evet	Evet	Evet	Evet
Karşılıklı yetkilendirme	Hayır	Evet	Evet	Evet	Evet	Evet
Kendini koruma	Evet	Evet	Evet	Evet	Evet	Evet
Sözlük saldırısına direnme	Sadece daha uzun şifrelerde	Evet	Evet	Hayır	Evet	Evet
MITM saldırısına karşı korunma	Hayır	Evet	Evet	Evet	Evet	Evet
Korunmuş Uzlaşılı Şifre Demeti	Hayır	Gerekli değil	Evet	Evet	Evet	Evet
Kullanıcı Kimlik saklanması	Hayır	Hayır	Evet	Hayır	Sadece Faz-2'de	Hayır
Daha hızlı yeniden bağlanma	Hayır	Hayır	Evet	Hayır	Evet	Hayır

6. SONUÇ VE ÖNERİLER

Kablosuz ağların son yıllarda hızla yayılması ve kullanımlarının artmasıyla kimlik doğrulama yöntemlerini geliştirmek için birçok çalışma yapılmaktadır.

Bu tezde kablosuz ağlarda kimlik bilgisini gizliliğini sağlamak için E-PEAP geliştirilmiştir. Geliştirilen protokol açık kaynak kod kullanılarak uygulanmış, test edilmiş ve sonuçlar güvenlik riskleri ve saldırılar yönünden incelenmiştir.

Kablosuz ağlarda kimlik doğrulama için sağladığı güvenlik seviyesi sayesinde yaygın olarak PEAP kullanılmaktadır. Ancak Faz-1 kimlik bilgisi gizliliği açısından bakıldığında Faz-2'deki gibi güvenlik ve gizlilik sağlayamamakta, bu gizliliği kullanıcı inisiyatifine bırakmaktadır. Geliştirilen E-PEAP kimlik doğrulama protokolü bu kullanıcı bağımlılığını ortadan kaldırmakta, tam bir kimlik bilgisi gizliliği sağlayabilmektedir.

Güçlü oturum anahtarların oluşturulması, karşılıklı kimlik doğrulama ve yetkilendirme, sözlük, MITM, hızlı yeniden bağlanma, güvenli tünel ile veri bütünlüğü, gizliliği sağlama özelliklerinden dolayı oldukça güçlü kimlik doğrulama protokolü olan PEAP'ın, geliştirilen yeni yöntem ile Faz-1'de kullanıcı bilgilerinin dinamik şifreleme anahtarı yöntemi ile gizliliği sağlanmıştır.

Deneysel çalışmaların sonucunda önerilen protokolün sözlük, tekrar ataklarına karşı güçlü direnç sağladığı, kimlik gizliliği ve semantik güvenlik ile güvenlik seviyesini arttırdığı görülmüştür. Gerçek dünya uygulamaları ve güvenlik analizleri geliştirilen E-PEAP'ın orijinal PEAP'tan daha uygulanabilir ve daha iyi güvenlik sağladığını göstermiştir.

KAYNAKLAR

1. IEEE. (IEEE 802.1X), "Wireless LAN media access local and metropolitan area networks: port-based network access control" ***Tech. Rep, IEEE***; (2001)

2. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H., "Extensible Authentication Protocol (EAP)", RFC 3748, (2004)

3. Baek, K., Smith, S. W., Kotz, D., "A Survey of WPA and 802.11i RSN Authentication Protocols", (2004)

4. Simon, D., Aboba, B., Hurst, R., "The EAP-TLS Authentication Protocol, EAP-TLS" http://www.ietf.org/rfc/rfc5216.txt

5. Dierks, T., Rescorla, E., "The Transport Layer Security(TLS) Protocol", http://tools.ieft.org/html/rfc5246

6. Funk, P. Blake-Wilson, S., "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)", RFC 5281, (2002)

7. Cam-Winget, N., McGrew, D., Salowey, J., Zhou, H., "The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Metot (EAP-FAST)", RFC 4851, (2007)

8. Zhou, S., Setia, S., Jajodia, S., "LEAP: effcient security mechanism for large-scale distributed sensor networks**,"** ***Proceedings of the 10th ACM Conference on Computer and Communications Security*** **(CCS'03)**, Washington, DC, SY. 62-72. (2003)

9. Andersson, H., Josefsson, S., Zorn, G., Simon, D., Palekar A., "Protected EAP Protocol (PEAP)", IETF draft draft-josefsson-pppext-eap-tls-eap-05.txt, (2002)

10. Calder, A., "Nine Steps to Success: An ISO 27001 Implementation Overview", ***IT Governence Institute Conference, (***2006)

11. Höne, H., Eloff, J.H.P. "Information Security Policy- What do international security standards say?", ***Computer and Security***, Vol.21 No.5.1, 402-409 (8), (2002)

12. İnternet : Cisco. "Dictionary Attack on Cisco LEAP. Tech Note", http://www.cisco.com/warp/public/707/cisco-sn-20030802-leap.shtml (2012)

13. Simpson, W.E., "The Point-to-Point Protocol (PPP)", RFC 1661, (1994)

14. Stallings, W., *"*Cryptography and Network Security: Principles and Practices*"* ***Pearson Education, Inc.***, NJ, Third Edition, (2003)

15. Stanley, J., Walker, B., Aboba, "Extensible Authentication Protocol Metot Requirements for Wireless LANs", RFC 4017, (2005)

16. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H., "Extensible Authentication Protocol (EAP)", RFC 3748, (2004)

17. Merkle, R.C., "Secure communications over insecure channels", ***Communications of the ACM,*** 21(4):294–299, (1978)

18. İnternet : Linux WPA/WPA2/IEEE 802.1X Hostapd http://hostap.epitest.fi/hostapd/ (2012)

19. İnternet : Linux WPA/WPA2/IEEE 802.1X Supplicant. http://hostap.epitest.fi/wpa_supplicant/ (2012)

20. İnternet : Wireshark Packet Sniffer Aracı: http://www.wireshark.org/ (2012)

21. İnternet : OpenSSL: "The Open Source toolkit for SSL/TLS", http://www.openssl.org (2012)

22. Dantu, R., Clothier, G. Atri, A., "EAP metots for wireless networks", ***Computer Standards Interfaces***, 29-3, 289–301, (2007)

23. Hwang, H., Jung, G., Sohn, K., Park, S., "A Study on Man in the Middle Vulnerability in Wireless Network Using 802.1X and EAP", ***International Conference on Information Science and Security*** , Seoul, Korea, 164-170, (2008)

24. İnternet : http://www.wifiplanet.com/tutorials/article.php/3075481 (2012)

25. İnternet : http://wireless.utk.edu/documentation/papers/802.1x-chris.pdf (2012)

26. İnternet:http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/networking_solutions_white_paper09186a008009c8b3.shtml (2012)

27. Arbaugh, W.A., "Wireless security is different", ***Computer Science***, Volume: 36, Issue: 8

28. Diffie, W., Hellman, M.E., "New directions in cryptography," ***IEEE Transactions on Information Theory,*** vol. IT-22, no. 6, 644-654, (1976)

29. Rivest, R.L., Shamir, A., Adleman, L.,"A metot for obtaining digital signatures and public-key cryptosystems," ***Communications of the ACM,*** **vol**. 21, no. 2, 120-126, (1978)

30. Congdon, P., Aboba, B., Smith, A., Zorn, G., Roese, J., “IEEE 802.1X Remote Authentication Dial In User Service (RADIUS)”, RFC 3580, (2003)

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: KURT, Çağdaş
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 06.07.1988 İzmir
Medeni hali	: Bekar
Telefon	: -
Faks	: -
e-mail	: cagdas.kurt@hotmail.com

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Lisans	Gazi Üniversitesi / Bilgisayar Sistemleri B.	2011
Lise	Alsancak Cumhuriyer A.M.L / Bilgisayar.	2006

İş Deneyimi

Yıl	Yer	Görev
2011 - 2012	Servus Bilişim A.Ş.	Ağ Mühendisi
2012 - …	Türksat A.Ş.	Ağ Mühendisi

Yabancı Dil

İngilizce, Almanca

Hobiler

Bilgisayar ağları ve güvenlik, Telekomünikasyon, Yapay zeka, Tenis, Basketbol