

**T.C.**

**SAKARYA ÜNİVERSİTESİ**

**BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ**

BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

KRİPTOLOJİYE GİRİŞ

**ÖDEV**

EAP Exchange

**Hazırlayan:**

**ESRA KIZILELMA 1-A B191210040**

**İçindekiler**

1. EAP Exchange nedir?
2. Gelişim süreci
3. Çerçeve Protokolü Yapısı
4. Yöntemler
5. Kullanım alanları
6. Güçlü zayıf yönleri
7. Kullanılan yöntemlerin karşılaştırılması
8. Kaynakça

**EAP Exchange nedir?**

Genişletilebilir Kimlik Doğrulama Protokolü (EAP), güvenli ağ erişim teknolojileri için farklı kimlik doğrulama yöntemlerinin kullanılmasına izin veren bir kimlik doğrulama çerçevesidir. Bu teknolojilere örnek olarak IEEE 802.1X kullanan kablosuz erişim, IEEE 802.1X kullanan kablolu erişim ve Sanal Özel Ağ (VPN) gibi Noktadan Noktaya Protokol (PPP) bağlantıları verilebilir. EAP, MS-CHAP v2 gibi belirli bir kimlik doğrulama yöntemi değil, ağ satıcılarının erişim istemcisi ve kimlik doğrulama sunucusunda EAP yöntemleri olarak bilinen yeni kimlik doğrulama yöntemleri geliştirip yüklemelerini sağlayan bir çerçevedir. EAP çerçevesi ilk olarak RFC 3748 tarafından tanımlanmış ve çeşitli diğer RFC'ler ve standartlar tarafından genişletilmişti

Genişletilebilir Kimlik Doğrulama Protokolü (EAP), kablosuz ağlarda ve noktadan noktaya bağlantılarda sıklıkla kullanılan, belirli bir kimlik doğrulama mekanizması değil, bir kimlik doğrulama çerçevesidir. Bazı ortak işlevleri ve EAP yöntemleri adı verilen kimlik doğrulama yöntemlerinin müzakeresini sağlar.

EAP protokolü, belirli bir tanesi üzerinde önceden anlaşmaya gerek kalmadan birden fazla kimlik doğrulama mekanizmasını destekleyebilir. Şu anda tanımlanmış yaklaşık 40 farklı yöntem bulunmaktadır.



EAP kimlik doğrulaması sunucu (kimlik doğrulayıcı) tarafından başlatılırken diğer birçok kimlik doğrulama protokolü istemci (eş) tarafından başlatılır. EAP kimlik doğrulama değişimi şu şekilde ilerler:

Kimlik doğrulayıcı (sunucu), eşin (istemci) kimliğini doğrulamak için bir istek gönderir.

Eş, geçerli bir isteğe yanıt olarak bir yanıt paketi gönderir.

Kimlik doğrulayıcı ek bir İstek paketi gönderir ve eş bir yanıt ile yanıt verir. İstek ve yanıt sırası ihtiyaç duyulduğu sürece devam eder. EAP bir 'kilit adımı' protokolüdür, dolayısıyla ilk İstek dışında, geçerli bir yanıt alınmadan yeni bir istek gönderilemez.

Konuşma, kimlik doğrulayıcı eşin kimliğini doğrulayamayana kadar devam eder (yanıtlar bir veya daha fazla isteğe kabul edilemez), bu durumda kimlik doğrulayıcı uygulamasının bir EAP Arızası iletmesi zorunludur. Alternatif olarak kimlik doğrulama konuşması, kimlik doğrulayıcı başarılı kimlik doğrulamanın gerçekleştiğini belirleyene kadar devam edebilir; bu durumda kimlik doğrulayıcının bir EAP Başarısı iletmesi zorunludur.

metin, ekran görüntüsü, yazı tipi, sayı, numara içeren bir resim

Açıklama otomatik olarak oluşturuldu

Genişletilebilir Kimlik Doğrulama Protokolü (EAP), kablosuz ağlara erişimi kontrol etmek için bir kimlik doğrulama çerçevesi olarak yaygın şekilde kullanılır; IEEE 802.11 ve IEEE 802.16 ağlarında. EAP, IKE ve TLS gibi iki taraflı bir protokol olarak diğer kimlik doğrulama çerçevelerinden farklıdır çünkü farklı ortamlara sahip iki iletişim bağlantısı üzerinden üç tarafla yürütülür. EAP'nin bir başka güvenlik sorunu da EAP yöntemlerinin, şifre paketlerinin ve protokol sürümlerinin tartışılabilirliğidir. Bu zorluklar, EAP için bir güven modelinin türetilmesini ve mevcut protokollerin güvenli bir şekilde benimsenmesini zorlaştırmaktadır. Son olarak, daha güvenli EAP uygulamalarına yönelik önerilerle bitiriyoruz.

metin, ekran görüntüsü, yazı tipi, sayı, numara içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Gelişim Süreci**

EAP (Extensible Authentication Protocol), gelişim süreci içinde çeşitli alt protokollerin ortaya çıkması ve geliştirilmesi ile karakterize edilir. EAP'nin evrimi, ağ güvenliği ve kimlik doğrulama gereksinimlerindeki değişikliklere yanıt olarak gerçekleşmiştir. İşte EAP'ın genel gelişim sürecine dair ana hatlar:

1. EAP'ın Temelleri:

- EAP, orijinal olarak RFC 2284 ile 1998 yılında tanıtılmıştır. Bu, EAP'ın temelini atmış ve genişletilebilir bir kimlik doğrulama çerçevesi olarak tasarlanmıştır.

2. İlk Alt Protokoller:

- EAP'nin ilk kullanılan alt protokolleri arasında EAP-MD5 ve EAP-TLS yer almaktadır. EAP-MD5, basit bir mesaj özeti (digest) doğrulamasını sağlar, ancak güvenlik açısından zayıftır. EAP-TLS ise sertifika tabanlı bir kimlik doğrulama sağlar.

3. Geniş Kullanım Alanları ve İlgili Protokoller:

- EAP, kablosuz ağlardan sanal özel ağlara (VPN) kadar geniş bir kullanım alanında kullanılmaya başlandı. Bu dönemde, EAP-TTLS (Tunneled Transport Layer Security) ve EAP-PEAP (Protected Extensible Authentication Protocol) gibi protokoller ortaya çıktı.

4. Mobil Ağ Operatörleri İçin EAP-SIM ve EAP-AKA:

- GSM ve 3G bağlantıları için mobil ağ operatörleri tarafından kullanılmak üzere EAP-SIM ve EAP-AKA gibi alt protokoller geliştirildi. Bu protokoller, abonelerin SIM kartları üzerinden kimlik doğrulama yapmalarına olanak tanır.

5. EAP-FAST ve Diğer İnovasyonlar:

- EAP-FAST (Flexible Authentication via Secure Tunneling), Cisco tarafından önerilen ve EAP-TLS ve EAP-TTLS'nin kullanımını basitleştirmeyi amaçlayan bir protokoldür. Bu dönemde diğer EAP türevleri ve geliştirmeleri de ortaya çıktı.

6. Güncellemeler ve Yenilikler:

- EAP, zaman içinde güncellenmiş ve çeşitli alt protokollerle genişletilmiştir. Güvenlik, performans ve kullanılabilirlik açısından çeşitli geliştirmeler yapılmıştır. Yenilikçi yaklaşımlar, EAP'nin farklı bağlantı türlerinde ve uygulama senaryolarında daha etkili olmasını sağlamıştır.

7. Uygulama ve Standartlaştırma:

- EAP, çeşitli endüstri standardizasyon organları tarafından benimsenmiş ve bir dizi standartlaştırılmış alt protokolle birlikte çeşitli ağ güvenlik uygulamalarında yaygın olarak kullanılmaktadır.

EAP'ın gelişimi, güvenlik endüstrisinin ve ağ teknolojilerinin evrimiyle yakından ilişkilidir. Bu süreç, yeni tehditlere ve güvenlik ihtiyaçlarına yanıt verme amacını taşımaktadır. Bu nedenle, EAP'ın evrimi sürekli olarak devam etmektedir.

**Çerçeve Protokolü Yapısı**

EAP (Extensible Authentication Protocol), ağ güvenliğinde genellikle kullanılan bir kimlik doğrulama protokolüdür. Ancak, EAP'nin bir algoritma olmadığını, genel bir çerçeve veya protokol olduğunu belirtmek önemlidir. EAP, bir ağ kullanıcısının kimlik doğrulama sürecini yöneten genişletilebilir bir çerçeve sunar.

EAP, aşağıdaki temel adımları içeren bir kimlik doğrulama sürecini destekler:

İletişim Başlatma:

İstemci (kullanıcı veya cihaz) ile kimlik doğrulama sunucusu arasında iletişim başlatılır.

Seçenek Sunma (Options Negotiation):

İletişim başladıktan sonra, her iki taraf da destekledikleri ve kullanabilecekleri kimlik doğrulama yöntemlerini ve özelliklerini müzakere ederler.

Kimlik Doğrulama:

İstemci ve sunucu, müzakere edilen yöntemlere uygun olarak kimlik doğrulama sürecini gerçekleştirir.

Onay ve Bağlantı Kurma:

Eğer kimlik doğrulama başarılıysa, taraflar bağlantı kurma sürecine geçerler.

EAP, geniş bir ağ ortamında farklı kimlik doğrulama yöntemlerini destekleyebilen bir çerçeve olduğu için "genişletilebilir" olarak adlandırılır. Örnek olarak, EAP-TLS (Transport Layer Security), EAP-PEAP (Protected Extensible Authentication Protocol) ve EAP-TTLS (Tunneled Transport Layer Security) gibi alt protokoller, EAP çerçevesini kullanarak farklı kimlik doğrulama mekanizmalarını uygular.

Belirli bir EAP alt protokolünün ayrıntıları, o alt protokolün spesifikasyonlarına ve uygulama belgelerine dayanır. Bu alt protokoller, şifreleme, anahtar yönetimi ve diğer güvenlik özellikleriyle birlikte çeşitli kimlik doğrulama yöntemlerini destekler. Bu nedenle, EAP'nin kendisi bir algoritma değil, bir çerçeve veya protokol olduğunu unutmamak önemlidir.

**Yöntemler**

EAP (Extensible Authentication Protocol), geniş bir çerçeve olduğu için bir dizi kimlik doğrulama yöntemini destekler. Bu yöntemler, genellikle EAP ile birlikte kullanılan alt protokoller tarafından uygulanır. İşte bazı yaygın EAP yöntemleri:

1. EAP-TLS (Transport Layer Security):

- EAP-TLS, güvenli bir ulaşım katmanı üzerinde çalışan, genellikle sertifika tabanlı bir kimlik doğrulama yöntemidir. İstemci ve sunucu, birbirlerine karşılıklı olarak sertifikalarını gönderir ve doğrulama işlemi bu sertifikalar üzerinden gerçekleşir.

2. EAP-PEAP (Protected Extensible Authentication Protocol):

- EAP-PEAP, içerideki EAP yöntemini koruyan bir tünelleme protokolüdür. PEAP, tipik olarak EAP-TLS, EAP-MSCHAPv2 veya EAP-GTC gibi içerideki EAP yöntemlerini taşır.

3. EAP-TTLS (Tunneled Transport Layer Security):

- EAP-TTLS, EAP çerçevesi içinde Transport Layer Security (TLS) kullanarak kimlik doğrulama sağlar. Kullanıcı kimliği genellikle içindeki başka bir EAP yöntemiyle doğrulanır.

4. EAP-SIM (Subscriber Identity Module):

- EAP-SIM, GSM veya 3G telefonlarında kullanılan Subscriber Identity Module (SIM) kartlarını temel alarak kimlik doğrulama yapar.

5. EAP-MD5 (Message Digest 5):

- EAP-MD5, basit bir mesaj özeti (digest) doğrulama yöntemidir. Ancak, şu an için güvenli olmayan bir yöntemdir ve genellikle tercih edilmez.

6. EAP-MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2):

- EAP-MSCHAPv2, Microsoft'un geliştirdiği bir kimlik doğrulama protokolüdür. Özellikle Microsoft ağlarında yaygın olarak kullanılır.

7. EAP-GTC (Generic Token Card):

- EAP-GTC, genellikle kullanıcı adı ve şifre ile kimlik doğrulamaya dayanan genel bir token kart (token card) tabanlı yöntemdir.

Bu sadece birkaç örnektir ve birçok başka EAP yöntemi bulunabilir. EAP'nin genişletilebilir yapısı, yeni kimlik doğrulama yöntemlerinin kolayca entegre edilmesine olanak tanır. İlgili güvenlik gereksinimlerine ve kullanım durumlarına bağlı olarak, organizasyonlar belirli bir EAP yöntemini seçebilir veya kombinasyonlarını yapılandırabilirler.

**Kullanım alanları**

EAP (Extensible Authentication Protocol) genellikle ağ güvenliği ve kimlik doğrulama bağlamında kullanılır. EAP'nin kullanım alanları şunları içerir:

1. Kablosuz Ağlarda Kullanımı:

- EAP, özellikle WPA (Wi-Fi Protected Access) ve WPA2 güvenlik protokollerinde kablosuz ağlarda kimlik doğrulama sağlamak için kullanılır. EAP-TLS, EAP-PEAP ve EAP-TTLS, bu bağlamda sıkça kullanılan alt protokollerdir. Kablosuz ağlarda EAP kullanımı, güvenli ağlara erişim sağlamak ve kimlik doğrulama süreçlerini şifreli olarak iletmek için kritiktir.

2. Sanal Özel Ağlarda (VPN'ler) Kullanımı:

- EAP, VPN bağlantılarında da yaygın olarak kullanılır. VPN'ler, uzaktan erişim sağlamak ve güvenli bağlantılar oluşturmak amacıyla kullanıldığında EAP, kullanıcıların güvenli bir şekilde kimlik doğrulamasını sağlar.

3. Kurumsal Ağ Güvenliği:

- İşletmelerde iç ağlarda, özellikle 802.1X tabanlı ağ erişimi kontrolü (NAC) çözümlerinde EAP kullanılır. Bu sayede kullanıcılar ve cihazlar, ağa güvenli bir şekilde erişebilmek için kimlik doğrulama süreçlerinden geçer.

4. Mobil Cihaz Güvenliği:

- Mobil cihazlar, tabletler ve akıllı telefonlar gibi taşınabilir cihazlarda, EAP kullanılarak güvenli bir şekilde kurumsal ağlara erişim sağlanabilir. Bu, işletmelerin BYOD (Bring Your Own Device) politikalarını destekler.

5. İş Uygulamaları ve Sunucu Tabanlı Hizmetler:

- EAP, çeşitli iş uygulamalarında ve sunucu tabanlı hizmetlerde güvenli kimlik doğrulama sağlamak için kullanılabilir. Örneğin, e-posta sunucularına güvenli erişim için EAP kullanılabilir.

6. VoIP Güvenliği:

- Ses üzerinden iletişim sağlayan VoIP uygulamalarında, EAP kimlik doğrulama süreçlerine katkıda bulunabilir. Bu, sesli iletişimin güvenliğini artırmak için kullanılır.

7. 802.1X Tabanlı Ağ Erişimi Kontrolü (NAC):

- EAP, 802.1X standartlarına dayalı ağ erişimi kontrolü (NAC) çözümlerinde kullanılır. Bu, ağa bağlanmak isteyen cihazların ve kullanıcıların güvenli bir kimlik doğrulama sürecinden geçmelerini sağlar.

8. Mobil Ağ Operatörleri:

- EAP-SIM, GSM veya 3G bağlantılarında mobil ağ operatörleri tarafından abonelerin kimlik doğrulaması için kullanılır.

Bu kullanım alanları, EAP'nin genişletilebilir yapısının ve çeşitli alt protokollerinin farklı güvenlik senaryolarına uygun olarak kullanılmasının bir sonucudur. EAP, ağ güvenliği ve kimlik doğrulama açısından çok yönlü bir çözüm sunar ve bu özellikleriyle çeşitli sektörlerde yaygın olarak kullanılmaktadır.

**Güçlü zayıf yönleri?**

EAP'nin güçlü ve zayıf yönleri, kullanılan alt protokollere, uygulama senaryolarına ve spesifik güvenlik gereksinimlerine bağlı olarak değişebilir. Ancak, genel olarak aşağıda, EAP'nin güçlü ve zayıf yönleri hakkında genel bilgiler bulunmaktadır:

Güçlü Yönler:

1. Genişletilebilirlik:

- EAP, genişletilebilir bir çerçeve olduğu için farklı kimlik doğrulama yöntemlerini destekleyebilir. Bu, değişen güvenlik gereksinimlerine uyum sağlamak ve yeni teknolojilere entegre olmak için önemlidir.

2. Kapsamlı Uygulama Alanları:

- EAP, kablosuz ağlardan VPN'lere, iş uygulamalarından mobil cihaz güvenliğine kadar bir dizi uygulama alanında kullanılabilir. Bu, çeşitli senaryolarda geniş bir kullanım olanağı sağlar.

3. Esnek Kimlik Doğrulama Yöntemleri:

- Farklı EAP alt protokolleri, çeşitli kimlik doğrulama yöntemlerini destekler. Örneğin, EAP-TLS, sertifikalı kimlik doğrulama sağlarken, EAP-PEAP kullanıcı adı/şifre tabanlı doğrulama yöntemlerini destekler.

4. Güvenli Taşıma:

- EAP, kimlik doğrulama süreçlerini şifreli bir şekilde taşıyarak güvenli bir iletişim sağlar. Bu, kimlik bilgilerinin güvende olmasını ve ortadaki saldırılara karşı direnci artırır.

5. Uyumluluk:

- EAP, geniş bir cihaz ve yazılım yelpazesinde kullanılabilir. Bu, çeşitli platformlarda ve ağ cihazlarında uyumluluk sağlar.

Zayıf Yönler:

1. EAP-MD5 Zayıf Güvenlik:

- EAP-MD5, şu an için güvenli olmayan bir yöntemdir. MD5 kullanılarak yapılan basit bir mesaj özeti (digest) doğrulaması sağlar ve saldırılara karşı dirençsizdir.

2. Protokol Yenilikleri Yavaş:

- EAP protokolü, tarih boyunca pek çok alt protokolün eklenmesine rağmen, protokolün kendisi zaman içinde sınırlı yeniliklere sahiptir. Bu, bazı yeni güvenlik tehditlerine karşı hızlı bir şekilde adapte olmayı zorlaştırabilir.

3. Kimlik Sızıntı Riski:

- Bazı EAP alt protokolleri, kullanıcı kimlik bilgilerini ağa iletmek için kullanılır. Bu, ortadaki saldırılara ve kimlik bilgilerinin sızdırılma riskine yol açabilir, ancak bu durum alt protokole ve yapılandırmaya bağlıdır.

4. Alt Protokol Seçimi Karmaşıklığı:

- EAP'nin genişletilebilirliği aynı zamanda kullanıcılar ve uygulama geliştiricileri için alt protokol seçimini karmaşık hale getirebilir. Yanlış yapılandırma, güvenlik zafiyetlerine yol açabilir.

5. Denetim Sorunları:

- EAP alt protokollerinden bazıları, güvenlik denetimleri ve yönetim zorlukları gibi sorunlarla karşılaşabilir. Bu, büyük ölçekli ağlarda yönetim zorluklarına neden olabilir.

Bu güçlü ve zayıf yönler, EAP'nin genel özellikleri ve kullanım durumlarına bağlı olarak değişebilir. Güvenlik ve uyumluluk gereksinimleri göz önüne alınarak, en uygun EAP alt protokolünün seçilmesi önemlidir.

**Kullanılan yöntemlerin karşılaştırılması**

EAP, belirli bir kimlik doğrulama mekanizması değil, bir kimlik doğrulama çerçevesidir. Bazı ortak işlevler ve EAP yöntemleri adı verilen kimlik doğrulama yöntemlerinin müzakere edilmesini sağlar. Şu anda yaklaşık 40 farklı yöntem tanımlanmıştır. Tanımlanan yöntemler IETF RFC'ler arasında EAP-MD5, EAP-POTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, EAP-AKA ve EAP-AKA bulunur. Ayrıca, satıcıya özgü bir dizi yöntem ve yeni teklif bulunmaktadır. Kablosuz ağlarda çalışabilen yaygın olarak kullanılan modern yöntemler arasında EAP-TLS, EAP-SIM, EAP-AKA, LEAP ve EAP-TTLS. Kablosuz LAN kimlik doğrulamasında kullanılan EAP yöntemleri için gereksinimler RFC4017. EAP'de kullanılan tür ve paket kodlarının listesi IANA EAP Kayıt Defterinden edinilebilir.

**Hafif Genişletilebilir Kimlik Doğrulama Protokolü (LEAP)**

Hafif Genişletilebilir Kimlik Doğrulama Protokolü (LEAP) yöntemi Cisco Sistemleri önce IEEE onaylaması 802.11’i güvenlik standardı. Cisco, 802.1X ve dinamik elde etmenin bir parçası olarak protokolü CCX (Cisco Sertifikalı Uzantılar) üzerinden dağıttı WEP bir standardın yokluğunda sektöre benimsenmesi. Hiçbirinde LEAP için yerel destek yoktur Windows işletim sistemi, ancak WLAN (kablosuz LAN) cihazlarında en yaygın olarak bulunan üçüncü taraf istemci yazılımı tarafından yaygın olarak desteklenmektedir. LEAP Microsoft Windows 7 ve Microsoft Windows Vista desteği hem LEAP hem de EAP-FAST için destek sağlayan Cisco'dan bir istemci eklentisi indirilerek eklenebilir.

LEAP MS-CHAP, bir kimlik doğrulama kullanıcı kimlik bilgilerinin güçlü bir şekilde korunmadığı ve kolayca tehlikeye atıldığı protokol; ASLEAP adlı bir istismar aracı 2004'ün başlarında Joshua Wright tarafından piyasaya sürüldü. Cisco, LEAP'ı kesinlikle kullanması gereken müşterilerin bunu yalnızca yeterince karmaşık şifrelerle yapmasını önerir, ancak karmaşık şifrelerin yönetilmesi ve uygulanması zordur. Cisco'nun mevcut önerisi, EAP-FAST gibi daha yeni ve daha güçlü EAP protokollerini kullanmaktır.

**EAP Taşıma Katmanı Güvenliği (EAP-TLS)**

EAP-TLS (Extensible Authentication Protocol - Transport Layer Security), kablosuz ağ kimlik doğrulama protokollerinden biridir ve RFC5216 standardını kullanır. TLS protokolü üzerine kurulmuş olan EAP-TLS, kablosuz LANlarda güvenli kimlik doğrulama sağlayan orijinal bir EAP protokolüdür.

EAP-TLS, güvenliği açısından hala en güvenli EAP standartlarından biri olarak kabul edilir. TLS, kullanıcı yanlış kimlik bilgileri hakkında uyarılar sağlamak şartıyla güçlü güvenlik sağlar. Nisan 2005'e kadar, WPA veya WPA2 sertifikasyonu için EAP-TLS, diğer tüm EAP tiplerinden önce gelmekteydi.

EAP-TLS, birçok büyük şirket ve açık kaynak işletim sistemleri tarafından desteklenir, örneğin 3Com, Apple, Cisco, Microsoft gibi. Çoğu TLS uygulamasının aksine, EAP-TLS istemci tarafı kullanarak karşılıklı kimlik doğrulamasını gerektirir ve X.509 standart sertifikalar kullanır.

EAP-TLS'nin istemci tarafı sertifikası, güvenli bir kimlik doğrulama sağlar. İstemci tarafı sertifikasına sahip olmadan, şifreyi bilmek yeterli değildir. Özel anahtarların akıllı kartlarda depolanması, ek bir güvenlik katmanı ekler, çünkü kartın çalınması, şifre hırsızlığından daha fark edilebilir ve kart hemen iptal edilebilir. Akıllı karttaki özel anahtar genellikle PIN ile korunduğu için güvenliği daha da artar.

**EAP-MD5**

EAP-MD5, orijinal RFC2284'te tanımlandığında IETF Standartları Parçası tabanlı bir EAP yöntemiydi. Ancak, MD5 karması kullanarak minimum güvenlik sağladığı için savunmasızdır ve sözlük saldırılarına açıktır. Ayrıca, dinamik WEP veya WPA/WPA2 anahtar üretimi için uygun değildir.

EAP-MD5, diğer EAP yöntemlerinden farklıdır çünkü EAP eşi ile EAP sunucusu arasında kimlik doğrulamasını sağlar, ancak karşılıklı kimlik doğrulamasını desteklemez. EAP sunucusunun kimlik doğrulamasını sağlaması, bu EAP yöntemini ortadaki adam saldırılarına karşı savunmasız kılar.

EAP-MD5, başlangıçta Windows 2000 tarafından destekleniyordu ancak Windows Vista ile kullanımdan kaldırıldı. Bu, EAP-MD5'in güvenlik açıklarından dolayı tercih edilmeyen bir yöntem olduğunu ve daha güvenli alternatiflerin benimsenmesi gerektiğini gösterir.

**EAP Korumalı Tek Kez Şifre (EAP-POTP)**

EAP Korumalı Tek Kez Parola (EAP-POTP), RFC4793 tarafından tanımlanan bir EAP yöntemidir ve RSA Laboratories tarafından geliştirilmiştir. Bu yöntem, elde taşınabilir donanım cihazları veya kişisel bilgisayarlarda çalışan bir donanım veya yazılım modülü kullanarak tek seferlik (OTP) belirteçleriyle kimlik doğrulama anahtarları oluşturmayı amaçlar. EAP-POTP, EAP tabanlı protokollerde tek taraflı veya karşılıklı kimlik doğrulama ve anahtar malzemesi sağlamak için kullanılabilir.

EAP-POTP yöntemi, iki faktörlü kullanıcı kimlik doğrulamasını destekler. Bu, kullanıcının fiziksel bir belirtece ve kişisel kimlik numarasına (PIN) erişimi olduğu anlamına gelir. Bu iki faktör, güvenli bir kimlik doğrulama süreci sağlar.

Özetle, EAP-POTP, tek seferlik belirteçler kullanarak güvenli kimlik doğrulama sağlayan ve iki faktörlü kimlik doğrulamasını destekleyen bir EAP yöntemidir.

**EAP Önceden Paylaşılan Anahtar (EAP-PSK)**

EAP Önceden Paylaşılan Anahtar (EAP-PSK), RFC4764 tarafından tanımlanan bir EAP yöntemidir ve önceden paylaşılan anahtarları (PSK) kullanarak karşılıklı kimlik doğrulama ve oturum anahtarı türetme işlemleri gerçekleştirir. Bu yöntem, başarılı bir karşılıklı kimlik doğrulama durumunda, her iki tarafla da korumalı bir iletişim kanalı sağlar ve özellikle güvensiz ağlar üzerinden kimlik doğrulaması için tasarlanmıştır, örneğin IEEE 802.11 gibi.

EAP-PSK, hafif ve genişletilebilir bir EAP yöntemi olarak belgelenmiştir, aynı zamanda ortak anahtar şifrelemesi gerektirmez. Bu yöntem, protokol değişimini en az dört mesajla gerçekleştirir.

Diğer bir EAP yöntemi olan EAP Parolası (EAP-PWD), RFC5931'de tanımlanmıştır ve kimlik doğrulaması için paylaşılan bir şifre kullanır. Parolanın düşük entropiye sahip olma olasılığı vardır ve saldırganın kullanabileceği bir sözlük saldırısına maruz kalabilir. Ancak, temel anahtar değişimi, aktif saldırılara, pasif saldırılara ve sözlük saldırılarına karşı dirençlidir..

**EAP Tüneli Taşıma Katmanı Güvenliği (EAP-TTLS)**

EAP Tüneli Taşıma Katmanı Güvenliği (EAP-TTLS), EAP protokolünü genişleten bir protokoldür ve TLS (Taşıma Katmanı Güvenliği) ile entegre çalışır. Bu protokol, Funk Yazılımı ve Certicom tarafından ortaklaşa geliştirilmiş olup, çeşitli platformlarda geniş destek bulmaktadır. Microsoft, EAP-TTLS protokolüne yerel destek sağlamıştır, özellikle Windows XP, Vista ve 7 işletim sistemlerinde. Windows 8'de ve Windows Phone 8.1'de EAP-TTLS desteği ortaya çıkmıştır.

EAP-TTLS, istemcilerin bir CA-imzalı PKI (Kamu Anahtar Altyapısı) sunucu sertifikası ile kimlik doğrulamasını sağlayabilir. Bu, her istemcinin kendi sertifikasına ihtiyaç duymadığından kurulum sürecini basitleştirir. Sunucunun CA sertifikası ve isteğe bağlı olarak istemcinin kimliğinin doğrulanmasından sonra, sunucu güvenli bir "tünel" oluşturarak istemcinin kimliğini doğrulayabilir. Bu sayede, eski kimlik doğrulama mekanizmalarını kullanırken bile güvenli tünel oluşturulur ve gizli dinleme ve orta adam saldırılarına karşı koruma sağlanır.

EAP-TTLS'nin iki versiyonu bulunmaktadır: orijinal EAP-TTLS (EAP-TTLSv0 olarak da bilinir) ve EAP-TTLSv1. EAP-TTLSv0 RFC5281 standardında belgelenmişken, EAP-TTLSv1 şu anda bir İnternet taslağı olarak mevcuttur.

**EAP İnternet Anahtar Değişimi v. 2 (EAP-IKEv2)**

EAP İnternet Anahtar Değişimi v. 2 (EAP-IKEv2), İnternet Anahtar Değişimi protokolünün ikinci sürümü (IKEv2) ile çalışan bir EAP (Genişletilebilir Yetkilendirme Protokolü) yöntemidir. EAP-IKEv2, bir EAP akranı (client) ile bir EAP sunucusu arasında karşılıklı kimlik doğrulama ve oturum anahtarı oluşturma yeteneği sağlar.

Bu protokol, farklı kimlik doğrulama tekniklerini destekler ve kimlik doğrulaması için çeşitli yöntemlere izin verir. Örneğin, EAP sunucusu genel/özel anahtar çiftini kullanabilir ve EAP eşini simetrik anahtarlarla doğrulayabilir. Ancak, teorik olarak mümkün olan tüm dokuz kombinasyonun uygulanması pratikte beklenmemektedir.

RFC5106 standardı, dört farklı kullanım durumunu listeler. İstemci üç farklı yöntemi kullanırken, sunucu asimetrik anahtar çiftiyle kimlik doğrulaması yapabilir ve her iki taraf da simetrik anahtar kullanabilir. Bu durumlar, EAP-IKEv2'nin kullanımını tanımlar ve uygulamada yaygın olarak karşılaşılan senaryolara odaklanır.**Güvenli Tünel ile EAP Esnek**

**Kimlik Doğrulaması (EAP-FAST)**

Güvenli Tünel ile Esnek Kimlik Doğrulama (EAP-FAST; RFC4851), Cisco Sistemleri'nin LEAP protokolü yerine geliştirdiği bir protokol önerisidir. Bu protokol, LEAP'ın zayıf yönlerini ele alarak "hafif" bir uygulamayı korumayı amaçlar. EAP-FAST, sunucu sertifikalarının kullanımını isteğe bağlı kılar.

EAP-FAST, TLS tüneli kullanarak istemci kimlik bilgilerini doğrulayan Korumalı Erişim Kimlik Bilgisi (PAC) kullanır. Otomatik PAC provizyonu etkinleştirildiğinde, güvenlik açığı potansiyeli ortaya çıkar; bir saldırgan PAC'yi kesip kullanıcı kimlik bilgilerini ele geçirebilir. Bu güvenlik açığı, manuel PAC sağlama veya sunucu sertifikalarını kullanarak PAC sağlama aşaması ile azaltılabilir.

Her kullanıcı için PAC dosyasının ayrı ayrı yayınlanması gerektiği unutulmamalıdır. Bu, RFC4851'in 7.4.4 bölümünde belirtilen bir gerekliliktir. Bu nedenle, yeni bir kullanıcı ağa bağlandığında, önce yeni bir PAC dosyası sağlanmalıdır. EAP-FAST'ın güvensiz anonim sağlama modunda çalıştırılmamasının zor olmasının bir nedeni budur. Alternatif olarak, cihaz şifrelerinin kullanılması düşünülebilir, ancak bu durumda cihaz, kullanıcı değil ağ tarafından doğrulanır.

EAP-FAST, Apple'ın OS X 10.4.8 ve daha yeni sürümlerinde yerel olarak desteklenir. Cisco, Windows Vista ve sonraki işletim sistemleri için genişletilebilir bir EAPHost mimarisi sağlayarak EAP-FAST modülü sunmaktadır, böylece yeni kimlik doğrulama yöntemleri ve eklemeleri entegre edilebilir.

**Tünel Genişletilebilir Kimlik Doğrulama Protokolü (TEAP)**

Tünel Genişletilebilir Kimlik Doğrulama Protokolü (TEAP; RFC7170), bir eş ve bir sunucu arasında güvenli iletişimi sağlamak için Aktarım Katmanı Güvenliği (TLS) protokolünü kullanan bir tünel tabanlı bir EAP yöntemidir. Bu protokol, karşılıklı doğrulanmış bir tünel oluşturmak amacıyla tasarlanmıştır.

TEAP, tünel içinde Tip-Uzunluk-Değer (TLV) nesnelerini kullanarak, EAP eşi ile EAP sunucusu arasında kimlik doğrulamasıyla ilgili verileri iletmek için kullanılır.

Bu protokol, eş kimlik doğrulamasının yanı sıra eşin sunucudan sertifika talep etmesine ve sunucunun eşe PKCS #7 biçiminde bir sertifika sağlamasına izin verir. Aynı zamanda sunucu, güvenilir kök sertifikalarını eşe PKCS #7 biçiminde dağıtabilir. Bu işlemler, önceden kurulmuş olan TLS tüneli içinde güvenli bir şekilde gerçekleşir ve karşılık gelen TLV'ler aracılığıyla iletilir.

**EAP Abone Kimlik Modülü (EAP-SIM)**

EAP Abone Kimlik Modülü (EAP-SIM), Global Mobil İletişim Sistemi (GSM) abone kimlik modülü (SIM) kartları aracılığıyla kimlik doğrulama ve oturum anahtarı dağıtımı için kullanılan bir EAP (Genişletilebilir Yetkilendirme Protokolü) yöntemidir.

GSM hücresel ağları, kullanıcı kimlik doğrulamasını gerçekleştirmek için bir abone kimlik modülü kartı kullanır. EAP-SIM, istemci ile Authentication, Authorization, and Accounting (AAA) istemcisi ve sunucusu arasında karşılıklı kimlik doğrulaması sağlayan bir SIM kimlik doğrulama algoritması kullanır.

EAP-SIM'de, SIM kart ile Kimlik Doğrulama Merkezi (AuC) arasındaki iletişim, istemci ile AAA sunucusu arasında önceden belirlenmiş bir parola ihtiyacının yerini alır. A3/A8 algoritmaları, farklı 128 bit zorluklarla çalıştırılır ve birleştirilerek 64 bit Kc-s oluşturulur (Kc-s doğrudan kullanılmaz), böylece daha güçlü anahtarlar elde edilir. Bu sayede GSM'de karşılıklı kimlik doğrulama eksikliği aşılmış olur.

**EAP Kimlik Doğrulaması ve Anahtar Sözleşmesi (EAP-AKA)**

Genişletilebilir Kimlik Doğrulama Protokolü Yöntemi Evrensel Mobil Telekomünikasyon Sistemi (UMTS) Kimlik Doğrulama ve Anahtar Sözleşmesi (EAP-AKA), UMTS Abone Kimlik Modülü (USIM) kartları üzerinden kimlik doğrulama ve anahtar sözleşmesi için kullanılan bir EAP (Genişletilebilir Yetkilendirme Protokolü) yöntemidir. Bu yöntem, EAP-AKA olarak RFC4187 standardında belgelenmiştir.

GSM (Global System for Mobile Communications) ve UMTS (Universal Mobile Telecommunications System) gibi hücresel ağlar, abonelerin kimlik doğrulamasını ve güvenli iletişimi sağlamak amacıyla özel kimlik modülü kartlarını kullanır. EAP-AKA, bu bağlamda UMTS ağlarında kullanılan USIM kartlarıyla etkileşimde bulunarak güvenli bir kimlik doğrulama ve anahtar sözleşmesi oluşturur.

EAP-AKA, RFC4187 standardına uygun olarak belirli güvenlik protokollerini ve iletişim adımlarını tanımlar. Bu yöntem, abone kimlik modülü ile ağ arasında güvenli bir iletişim kanalı kurarak, abonenin kimlik doğrulamasını ve güvenli anahtarların paylaşılmasını mümkün kılar.

**EAP Jenerik Jeton Kartı (EAP-GTC)**

EAP Jenerik Jeton Kartı veya EAP-GTC, Cisco tarafından PEAPv0/EAP-MSCHAPv2'ye alternatif olarak geliştirilen bir EAP (Genişletilebilir Yetkilendirme Protokolü) yöntemidir. Bu yöntem, RFC2284 ve RFC3748 standartlarına uygun olarak tanımlanmıştır. PEAP-GTC kimlik doğrulama mekanizması, kimlik doğrulama sunucusundan bir metin zorluğu ve bu zorluktan oluşturulan bir yanıt içeren güvenlik belirteci taşır.

EAP-GTC, genel kimlik doğrulamasına izin veren bir dizi veri tabanını destekler, örneğin Novell Dizin Hizmeti (NDS) ve Hafif Dizin Erişim Protokolü (LDAP) gibi. Ayrıca, bir defalık şifre gibi farklı kimlik doğrulama yöntemlerini de destekleyebilir.

Bu protokol, kullanıcının kimlik doğrulamasını gerçekleştirmek için sunucuya bir metin zorluğu göndermesi ve ardından sunucunun bu zorluğa dayalı olarak bir güvenlik belirteci oluşturması temeline dayanır. EAP-GTC, özellikle PEAP-GTC olarak adlandırılan PEAP türevlerinde kullanılır ve kablosuz ağlarda güvenli kimlik doğrulama sağlamak için tercih edilebilir.

**EAP Şifreli Anahtar Değişimi (EAP-EKE)**

EAP Şifreli Anahtar Değişimi ya da EAP-EKE, güvenli karşılıklı kimlik doğrulamasını kısa şifreler kullanarak sağlayan ve ortak anahtar sertifikalarına gerek duymayan birkaç EAP yönteminden biridir. Bu protokol, Diffie-Hellman'ın üç aşamalı bir değişimi olan ve iyi bilinen EKE (Encrypted Key Exchange) protokolünün bir varyantıdır.

**EAP (EAP-NOOB) için çevik bant dışı kimlik doğrulama**

EAP için Çevik Bant Dışı Kimlik Doğrulama (EAP-NOOB), önceden yapılandırılmış kimlik doğrulama bilgisine sahip olmayan ve henüz herhangi bir sunucuda kayıtlı olmayan cihazlar için genel bir önyükleme çözümüdür. Özellikle Nesnelerin İnterneti (IoT) cihazları ve oyuncaklar gibi herhangi bir sahip, ağ veya sunucu hakkında bilgi içermeyen durumlar için yararlıdır. Bu EAP yönteminin kimlik doğrulaması, sunucu ve cihaz arasındaki kullanıcı destekli bant dışı (OOB) bir kanala dayanmaktadır. EAP-NOOB, QR kodları, NFC etiketleri, ses gibi birçok OOB kanalını destekler ve diğer EAP yöntemlerinden farklı olarak, protokol güvenliği, ProVerif ve MCRL2 Araçları ile resmi bir modelleme ile doğrulanmıştır.

EAP-NOOB, bant içi EAP kanalı üzerinde Ephemeral Eliptik Eğri Diffie-Hellman (ECDHE) kullanarak bir değişim gerçekleştirir. Kullanıcı daha sonra bu değişimi onaylamak için OOB mesajını aktarır. Örneğin, cihazın bir QR kodu gösterebilen bir akıllı TV olduğu durumda, kullanıcı OOB mesajını eşten sunucuya iletebilir. Alternatif olarak, kullanıcılar OOB mesajını sunucudan eşe aktarabilir; örneğin, önyüklenen cihaz yalnızca QR kodunu okuyabilen bir kamera olabilir.

**Güçlü ve Zayıf Yönlerinin Karşılaştırılması**

Farklı EAP (Extensible Authentication Protocol) alt protokollerinin karşılaştırılması, kullanım senaryolarına, güvenlik gereksinimlerine ve uygulama ihtiyaçlarına bağlı olarak değişebilir. İşte yaygın olarak kullanılan bazı EAP alt protokollerinin kısa bir karşılaştırması:

1. EAP-TLS (Transport Layer Security):

Güçlü Yönler:

- Sertifika tabanlı kimlik doğrulama.

- Güçlü şifreleme ve anahtar yönetimi.

- Ortadaki saldırılara karşı dayanıklılık.

Zayıf Yönler:

- Sertifika yönetimi karmaşıklığı.

- Yüksek hesaplama gücü gereksinimleri.

2. EAP-PEAP (Protected Extensible Authentication Protocol):

Güçlü Yönler:

- Şifre tabanlı ve sertifika tabanlı kimlik doğrulama.

- Güvenli tünelleme.

- Kullanımı daha basit.

Zayıf Yönler:

- Güvenli tünelin sertifika tabanlı olması durumunda sertifika yönetimi.

3. EAP-TTLS (Tunneled Transport Layer Security):

Güçlü Yönler:

- Şifre tabanlı ve sertifika tabanlı kimlik doğrulama.

- Güvenli tünelleme.

- Sertifika yönetimindeki esneklik.

Zayıf Yönler:

- Yüksek hesaplama gücü gereksinimleri.

4. EAP-SIM (Subscriber Identity Module):

Güçlü Yönler:

- GSM ve 3G bağlantıları için uygun.

- GSM SIM kartları üzerinden kimlik doğrulama.

Zayıf Yönler:

- GSM SIM kartlarına bağımlılık.

- Yetersiz güvenlik seviyeleri.

5. EAP-MD5 (Message Digest 5):

Güçlü Yönler:

- Basit uygulama ve düşük hesaplama gücü gereksinimleri.

Zayıf Yönler:

- Güvenlik zafiyetleri (örneğin, ortadaki saldırılara karşı dirençsiz).

- Güçlü şifreleme veya güvenlik katmanları içermez.

6. EAP-MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2):

Güçlü Yönler:

- Microsoft altyapısına uygun.

- Kullanımı basit.

Zayıf Yönler:

- Ortadaki saldırılara karşı daha zayıf.

- Güvenli tünelleme eksikliği.

7. EAP-GTC (Generic Token Card):

Güçlü Yönler:

- Genel token kartlar üzerinden kimlik doğrulama.

Zayıf Yönler:

- Sertifika tabanlı kimlik doğrulama seviyelerine ulaşamaz.

- Güvenli tünelleme eksikliği.

Bu karşılaştırma, her EAP alt protokolünün belirli avantajları ve zayıf yönleri olduğunu göstermektedir. Seçim, kullanım senaryolarına, ağ yapılarına ve güvenlik gereksinimlerine bağlı olarak yapılmalıdır. İdeal olarak, belirli bir uygulama veya ortam için en uygun olanı seçilir.

**Kaynakça**

“The Extensible Authentication Protocol-Internet Key Exchange Protocol version 2 (EAP-IKEv2) Method”, erişim: 13 Aralık 2023, https://www.rfc-editor.org/rfc/rfc6124

“Extensible Authentication Protocol (EAP)”, erişim: 13 Aralık 2023, https://www.techtarget.com/searchsecurity/definition/Extensible-Authentication-Protocol-EAP

“Extensible Authentication Protocol (EAP) for network access”, erişim: 13 Aralık 2023, https://learn.microsoft.com/en-us/windows-server/networking/technologies/extensible-authentication-protocol/network-access?tabs=eap-tls%2Cserveruserprompt-eap-tls%2Ceap-sim.

“Extensible authentication protocol (EAP) and IEEE 802.1x: tutorial and empirical experience”, erişim: 13 Aralık 2023, https://ieeexplore.ieee.org/abstract/document/1561920?casa\_token=X1gQld1vuIcAAAAA:HwyyBxpkZ\_WeRxfyx0pZMhsPF4MDuhuAv6rnCumwpUqY0B660rFOvhEyyeDHPR2VTSvyFy6fD5HN

“An EAP Authentication Method Based on the Encrypted Key Exchange (EKE) Protocol”, erişim: 13 Aralık 2023, https://www.rfc-editor.org/rfc/rfc6124

“Where EAP security claims fail”, erişim: 13 Aralık 2023, https://dl.acm.org/doi/abs/10.1145/1577222.1577285

“How to use EAP-TLS authentication in PWLAN environment”, erişim: 13 Aralık 2023, https://ieeexplore.ieee.org/abstract/document/1281206?casa\_token=-\_C9hSwYiBcAAAAA:s1mGZ4HXUB5eAyj6yUk\_W5cXWFibPT12rmBfJu5pCNnfcFGcFbImpsit933KeA6e0DF5lPnHDJ6N

“Complete EAP Method: User Efficient and Forward Secure Authentication Protocol for IEEE 802.11 Wireless LANs”, erişim: 13 Aralık 2023, https://ieeexplore.ieee.org/abstract/document/6205749

“Extensible Authentication Protocol (EAP)”, erişim: 13 Aralık 2023, https://www.ietf.org/rfc/rfc3748.txt

“EAP Authenticationerişim” 13 Aralık 2023, https://networkradius.com/doc/FreeRADIUS-Implementation-Ch6.pdf

“Extensible Authentication Protocol (EAP) Key Management Framework” 13 Aralık 2023, https://www.rfc-editor.org/rfc/rfc5247.txt

“Extensible Authentication Protocol” 13 Aralık 2023, https://en.wikipedia.org/wiki/Extensible\_Authentication\_Protocol

EAP Overview "https://mrncciew.com/2013/03/03/eap-overview/”