SAKARYA ÜNİVERSİTESİ BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİ

2023 KRİPTOLOJİ ÖDEVİ
KEY EXCHANGE (IKE-IKEv2)

İSİM SOYİSİM: FATMA GÜNER

ÖĞRENCİ NUMARASI: B201210373

SINIF: 1. ÖĞRETİM A GRUBU

İÇİNDEKİLER

İki bilgisayar arasında güvenlik anlaşması oluşturmak için IETF tarafından geliştirilen Internet Anahtar Değişimi (IKE), standart bir güvenlik ilişkisi ve anahtar değişim çözümü sunmaktadır. Bu yöntem, güvenlik ilişkisi yönetimini merkezileştirerek bağlantı süresini azaltma avantajına sahiptir. Aynı zamanda, bilginin güvenliğini sağlamak için kullanılan paylaşılan, gizli anahtarları oluşturup yönetir.

IKE (Internet Key Exchange), IKEv1 ve IKEv2 olarak iki ana versiyona ayrılan, IPsec (Internet Protocol Security) protokol suitinin bir parçası olan bir anahtar değişim protokolüdür. Temel olarak, iki iletişim kuruluşu arasında güvenli bir iletişim kanalı oluşturmak için kullanılır.

IKE'NİN DOĞUŞU:

1998 yılında, IETF (Internet Engineering Task Force) IKE protokolünü tanıtmıştır. Temel amacı, IPsec güvenlik kurallarını müzakere etmek ve anahtar değişimini yönetmekti. IKE, IPsec'in temelini oluşturarak, ağ üzerinden güvenli bir iletişim kanalı kurmayı mümkün kıldı.

IKEv1:

- IKEv1, orijinal IKE protokolünün evrimleşmiş bir versiyonudur.
- 1998 yılında IETF tarafından RFC 2409 ile standartlaştırılmıştır.
- IKEv1, Diffie-Hellman anahtar değişimi ve özel anahtar algoritmalarını içerir.
- Farklı aşamalarda (Phase 1 ve Phase 2) güvenlik birliği kurma konseptini getirir.
- Ancak, bazı güvenlik zayıflıkları ve performans kısıtlamaları vardı.

İhtiyaçlar ve Gelişmeler:

- Zamanla, internet üzerindeki tehditler ve güvenlik ihtiyaçları değişti.
- Mobil cihazların ve çoklu ağ bağlantılarının yaygınlaşması, IKE'nin geliştirilmiş bir versiyonunu zorunlu kıldı.
- Gelişen teknoloji ve güvenlik standartları, IKEv1'in bazı eksikliklerini giderme ihtiyacını ortaya çıkardı.

IKEv2'nin Ortaya Çıkışı:

- IKEv2, IKEv1'in yerini alacak şekilde tasarlanmıştır.
- 2005 yılında IETF tarafından RFC 4306 ile standartlaştırılmıştır.
- Single Exchange Mode özelliği, performansı artırmak için öne çıkar.
- NAT traversal konusundaki sorunları daha etkili bir şekilde çözer.
- MOBIKE (Mobility and Multihoming) desteği, mobil cihazlar için daha iyi uyumluluk sağlar.

Güncel ve Güvenli:

- IKEv2, modern güvenlik standartlarına uyum sağlar.

- EAP (Extensible Authentication Protocol) desteği ile çeşitli kimlik doğrulama yöntemlerini destekler.
- Header minimization özelliği, daha düşük bant genişliği kullanımını mümkün kılar.

Tabii ki, aşağıda IKE ve IKEv2'de kullanılan anahtar değişim algoritmaları hakkında detaylı bir yazı bulabilirsiniz:

IKE VE IKEv2 ANAHTAR DEĞİŞİM ALGORİTMALARI

İnternet Key Exchange (IKE) ve IKEv2, güvenli iletişim sağlamak amacıyla kullanılan anahtar değişim protokolleridir. Bu protokoller, anahtar değişimini yönetmek ve güvenlik parametrelerini müzakere etmek için çeşitli algoritmaları kullanır

IKE ve IKEv2'de Kullanılan Temel Algoritmalar:

1. **Diffie-Hellman Anahtar Değişimi:**
    - **Amaç:** İki taraf arasında güvenli bir şekilde anahtar malzemesi paylaşmak.
    - **İşleyiş:** İki taraf, açıkça iletilmeyen bir ortak anahtar oluşturmak için matematiksel bir protokol kullanır.
    - **Önemi:** Güvenli bir anahtar değişimi sağlar.
2. **Symmetric Key Algoritmaları:**
    - **Amaç:** Gerçek veri trafiği için kullanılan anahtarları şifrelemek.
    - **Örnekler:** DES (Data Encryption Standard), 3DES, AES (Advanced Encryption Standard).
    - **Gelişmeler:** Güvenlik standartlarına uygun olarak zaman içinde evrimleşir.
3. **Hash Fonksiyonları:**
    - **Amaç:** Veri bütünlüğünü sağlamak ve doğrulamak için kullanılır.
    - **Örnekler:** SHA-1, SHA-256, SHA-3.
    - **Gelişmeler:** Güvenlik endişeleri nedeniyle zamanla daha güçlü hash fonksiyonlarına doğru evrilmiştir.

IKEv2'nin Getirdiği Yenilikler:

4. **EAP (Extensible Authentication Protocol):**
    - **Amaç:** Çeşitli kimlik doğrulama yöntemlerini desteklemek.
    - **Örnekler:** EAP-TLS, EAP-MSCHAPv2.
    - **Avantaj:** Esnek kimlik doğrulama seçenekleri sunar.
5. **MOBIKE (Mobility and Multihoming):**

- **Amaç:** Mobil cihazlar ve çoklu ağ bağlantıları için destek sağlamak.
- **Önem:** İnternet üzerindeki hareketlilik ve çoklu bağlantı senaryolarına uyum sağlar.

6. **Header Minimization:**
    - **Amaç:** İletişim başlıklarının boyutunu minimize etmek.
    - **Avantaj:** Daha düşük bant genişliği kullanımını sağlar.

IKE VE IKEv2 KEY EXCHANGE YÖNTEMLERİ

İnternet Key Exchange (IKE) ve IKEv2, bilgisayar ağları arasında güvenli iletişim kurmak için kullanılan protokollerdir. Bu protokoller, anahtar değişimi sürecinde kullanılan yöntemlerle güvenli bir bağlantı kurarlar. İşte IKE ve IKEv2'nin temel key exchange yöntemleri:

IKE Key Exchange Yöntemleri:

1. **Main Mode:**
    - **Açıklama:** Main Mode, anahtar değişimi sürecinin ilk aşamasını temsil eder.
    - **Diffie-Hellman Anahtar Değişimi:** Anahtar materyali müzakere edilir.
    - **Authentications:** İki taraf arasında kimlik doğrulaması yapılır.
2. **Aggressive Mode:**
    - **Açıklama:** Aggressive Mode, Main Mode'a kıyasla daha hızlı bir anahtar değişimi sağlar.
    - **Fazladan Trafik:** Daha az paket ile daha hızlı bir müzakere süreci sunar.
    - **Güvenlik: **Main Mode'a göre daha az güvenli olabilir.
3. **Quick Mode:**
    - **Açıklama:** Veri trafiğinin anahtarlarını güncellemek için kullanılır.
    - **Anahtar Refresh:** Veri trafiği için kullanılan anahtarlar sürekli olarak yenilenir.
    - **Güvenlik İlişkileri:** İki taraf arasındaki güvenlik ilişkilerini yönetir.

IKEv2 Key Exchange Yöntemleri:

1. **Initiator and Responder:**
    - **Açıklama:** IKEv2'de anahtar müzakeresi, başlatıcı (initiator) ve yanıtlayıcı (responder) arasında gerçekleşir.
    - **Diffie-Hellman:** İki taraf arasında güvenli bir anahtar oluşturmak için kullanılır.
    - **Exchange Types:** IKEv2, çeşitli anahtar değişim türlerini destekler.

2. **Child SA Negotiation:**
    - **Açıklama:** IKEv2, anahtar değişimini daha spesifik alt sistemler (Child Security Associations - Child SA) üzerinde yönetir.
    - **Traffic Selector:** Hangi trafiğin güvenli bir şekilde iletilmesi gerektiğini belirler.
    - **SA (Security Association) Parameters:** İletişim kurulan cihazlar arasındaki güvenlik parametrelerini belirler.
3. **EAP (Extensible Authentication Protocol):**
    - **Açıklama:** Kimlik doğrulama için esnek bir yöntem sağlar.
    - **Çeşitli Yöntemler:** EAP-TLS, EAP-MSCHAPv2 gibi çeşitli kimlik doğrulama yöntemlerini destekler.
    - **Esneklik:** Farklı kimlik doğrulama yöntemlerini kullanarak daha geniş bir kullanıcı tabanını destekler.

İşleyiş ve Güvenlik:

- IKE ve IKEv2, Diffie-Hellman anahtar değişimi ile güvenli anahtar materyali oluştururlar.
- Güvenlik parametreleri, karşılıklı kimlik doğrulama ve trafik seçicileri üzerinden müzakere edilir.
- Algoritmalar, güvenlik standartlarına uyum sağlamak ve sürekli güncellenmek üzere tasarlanmıştır.

IKE VE IKEv2 KULLANIM ALANLARI

İnternet Key Exchange (IKE) ve IKEv2, bilgisayar ağları arasında güvenli iletişim kurmak için temel protokollerdir. Bu protokoller, anahtar değişimini yönetir ve güvenlik parametrelerini müzakere ederek birbirleriyle güvenli bir iletişim kanalı oluştururlar. İşte IKE ve IKEv2'nin kullanım alanları:

1. Sanal Özel Ağlar (VPN) Kurulumu:

- IKE ve IKEv2, en yaygın olarak sanal özel ağlar (VPN) kurulumunda kullanılır.
- Uzaktan erişim, site-to-site ve çoklu kullanıcı VPN bağlantıları için güvenli bir bağlantı sağlamak amacıyla kullanılır.
- Diffie-Hellman anahtar değişimi ve güçlü şifreleme algoritmaları, VPN trafiğini korumak için temel unsurları oluşturur.

2. Mobil Cihaz Güvenliği:

- IKEv2'nin getirdiği özellikler, mobil cihazlarda kullanımı kolaylaştırır.
- MOBIKE (Mobility and Multihoming) desteği, kullanıcıların mobil cihazları üzerinden güvenli bir şekilde iletişim kurmasını sağlar.

- Esnek kimlik doğrulama yöntemleri, çeşitli mobil cihazlar ve platformlar üzerinde güvenli bağlantılar kurulmasına olanak tanır.

3. Şirket İçi İletişim Güvenliği:

- İşletmeler, şirket içi iletişimlerinde güvenlik önlemleri almak için IKE ve IKEv2'yi kullanabilirler.
- Özellikle uzaktan çalışma ortamlarında, güvenli anahtar değişimi ve şifreleme, hassas verilerin korunmasına yardımcı olur.
- VPN bağlantıları, ofis şubeleri arasında güvenli iletişimi destekler.

4. Güvenli Veri Transferi:

- IKE ve IKEv2, güvenli anahtar değişimi ve müzakere yetenekleri ile genel veri transferi için de kullanılabilir.
- İnternet üzerindeki hassas verilerin, örneğin finansal bilgiler veya sağlık verileri, güvenli bir şekilde iletilmesini sağlar.
- Anahtar materyali ve güvenlik parametreleri, iletişimdeki taraflar arasında güvenli bir şekilde paylaşılır.

5. Çoklu Güvenlik Protokollerini Destekleme:

- IKE ve IKEv2, çeşitli güvenlik protokollerini destekleme yeteneğine sahiptir.
- EAP (Extensible Authentication Protocol) desteği sayesinde farklı kimlik doğrulama yöntemlerini entegre etmek mümkündür.
- Bu, protokollerin esneklik açısından zengin ve farklı kullanım senaryolarına uygun olmalarını sağlar.

6. Endüstriyel ve Askeri Uygulamalar:

- Güvenlik endişeleri yüksek olan endüstriyel ve askeri uygulamalarda, IKE ve IKEv2 kullanımı yaygındır.
- Stratejik veri iletimi, siber tehditlere karşı dirençli bir bağlantı gerektirir, bu nedenle güvenli anahtar değişimi hayati önem taşır.

IKE (Internet Key Exchange) Güçlü ve Zayıf Yönleri:

Güçlü Yönler:

1. **Güvenlik:** IKE, güvenli bir anahtar değişimi sağlamak amacıyla tasarlanmıştır. Diffie-Hellman anahtar değişimi ve güçlü şifreleme algoritmaları kullanarak, iletişimi korumak için etkili bir temel oluşturur.
2. **Esnek Kimlik Doğrulama:** IKE, çeşitli kimlik doğrulama yöntemlerini destekler. Bu esneklik, farklı kullanım senaryolarına ve güvenlik politikalarına uyum sağlamak için önemlidir.

3. **Çoklu Fazlar:** IKE'nin üç aşamalı bir yapısı vardır. Bu fazlar, güvenli bir anahtar değişimi sürecini adım adım sağlar ve iletişim başlamadan önce bir güvenlik birliği oluşturur.

Zayıf Yönler:

1. **Performans:** Özellikle Aggressive Mode kullanıldığında, IKE'nin performansı azalabilir. Çünkü bu mod, daha hızlı bir anahtar değişimi sağlamak amacıyla daha az güvenlik içerebilir.
2. **Esnek Olmayan Header Boyutları:** IKE'nin başlık boyutları genellikle sabittir. Bu durum, bazı durumlarda başlık boyutlarının daha esnek olmasını isteyen uygulamalarda sorunlara neden olabilir.

IKEv2 Güçlü ve Zayıf Yönleri:

Güçlü Yönler:

1. **Gelişmiş Performans:** IKEv2, önceki sürüm olan IKE'ye kıyasla daha hızlı bir anahtar değişimi sağlar. Single Exchange Mode özelliği, müzakere sürecini tek bir aşamaya indirir, bu da performansı artırır.
2. **Esnek ve Güçlü Kimlik Doğrulama:** EAP (Extensible Authentication Protocol) desteği sayesinde IKEv2, çeşitli kimlik doğrulama yöntemlerini destekler, bu da daha fazla esneklik sağlar.

Zayıf Yönler:

1. **Uyum Sorunları:** IKEv2'nin bazı uygulama ve cihazlarla uyumsuzluk sorunları olabilir. Bu, özellikle karışık ağ ortamlarında sorunlara yol açabilir.
2. **Kurulum Karmaşıklığı:** IKEv2, IKE'ye göre daha karmaşık bir yapıya sahiptir. Bu nedenle, doğru şekilde yapılandırılması ve yönetilmesi daha fazla dikkat gerektirebilir.

IKE VE IKEV2 KULLANILAN YÖNTEMLERİ KARŞILAŞTIRMA

1. Performans:
    - IKE: Aggressive Mode, hızlı bir anahtar değişimi sağlar ancak daha az güvenlik olabilir.
    - IKEv2: Single Exchange Mode, daha hızlı bir anahtar değişimini destekler.
2. Esneklik:
    - IKE: Belirli bir esneklik seviyesine sahiptir ancak EAP desteği sınırlıdır.
    - IKEv2: EAP desteği ile daha geniş bir kimlik doğrulama yelpazesi sunar.
3. Güvenlik ve Karmaşıklık:
    - IKE: Main Mode ve Quick Mode'un ayrı aşamaları, belirli güvenlik seviyelerini sağlar ancak karmaşık bir yapıya sahiptir.
    - IKEv2: Tek bir Exchange Type kullanarak daha hızlı ve güvenli bir anahtar değişimine olanak tanır.

KAYNAKÇA:

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc784994(v=ws.10)?redirectedfrom=MSDN

https://www.rfc-editor.org/rfc/rfc2409.html

https://networkengineering.stackexchange.com/questions/1/whats-the-difference-between-ike-and-isakmp/30397#30397

https://datatracker.ietf.org/doc/html/rfc7296

https://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ikevpn/configuration/15-1mt/Configuring_Internet_Key_Exchange_Version_2.html

https://www.techradar.com/features/what-is-ikev

https://nordvpn.com/tr/blog/ikev2ipsec/

https://dl.acm.org/doi/abs/10.17487/RFC4306

https://www.cloudflare.com/learning/network-layer/ipsec-vs-ssl-vpn/

https://www.expressvpn.com/what-is-vpn/protocols/ikev2#:~:text=IKEv2%20is%20one%20of%20the%20most%20secure%20VPN%20protocols.,Camellia%2C%20AES%2C%20and%20Blowfish.