Şifreleme Algoritmaları ve Bazı Saldırı Yöntemleri

Prof. Dr. Resul Daş

Kriptosistemler ve Şifreleme Yöntemleri

Kriptosistemler

- Kimlik doğrulama ve şifreleme verinin güvenliğini sağlamaya yarayan birbiriyle bağlantılı iki teknolojidir.
- Kimlik doğrulama, haberleşmede her iki tarafta bulunanların ne söylüyorlar ise onun doğru olmasını sağlama sürecidir.
- Şifreleme ise iletişim sırasında verinin hem güvenliğini sağlamak hem de değiştirilmesini önlemeye yönelik işlemlerdir.

Güvenliğin Geliştirilmesi İhtiyacı

- 1970'li yıllarda IPv4 İnternette kullanılmaya başlandığında ağ güvenliği önemli bir konu değildi.
- Bu nedenle IP tüm veriyi açık metin şeklinde göndermektedir.
- Bunun anlamı gönderilen paketler dinlenirse içeriğinin öğrenilebileceği ve istenilirse değiştirilebileceğidir.
- Ağ analizi yapan bir saldırgan, hem oturumları öğrenebilir hem de veri paketlerinin içeriklerini değiştirebilir.

Güvenliğin Geliştirilmesi İhtiyacı

- Aşağıdaki protokoller açık metin kullanan protokollerdir.
  - FTP (File Transfer Protocol), Telnet, IMAP (Internet Message Access Protocol), SNMP (Simple Network Management Protocol): Doğrulama işlemi açık metin ile yapılır.
  - SMTP (Simple Mail Transfer Protocol): Posta mesajlarının içeriği açık mesaj olarak dağıtılır.
  - http (Hyper Text Transfer Protocol): Sayfa içeriği ve formlardaki bilgilerin içeriği açık metin olarak gönderilir.

Ağ Üzerinden Yapılan Saldırı Türleri

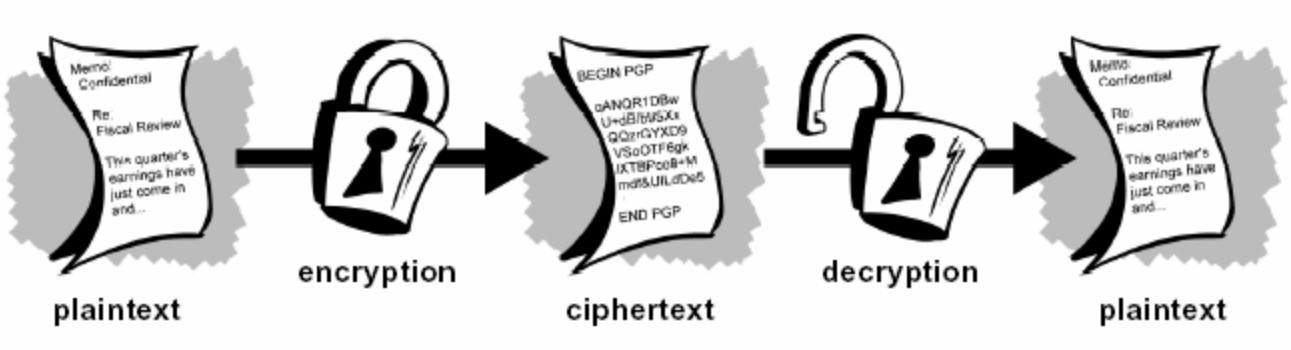
1) **İfşaat-Açığa Çıkarma (Disclosure):** mesaj içeriğinin herhangi birisine verilmesi veya uygun kriptografik anahtara sahip olmama
2) **Trafik Analizi:** ağdaki trafik akışının analiz edilmesi. Bağlantı esaslı uygulamalarda bağlantının sıklığı ve süresi belirlenebilir. Bağlantısız ortamda ise mesajların sayısı ve uzunluğu belirlenebilir.
3) **Gerçeği Gizleme (Masquerade):** hileli bir kaynaktan ağa mesaj ekleme. Bu işlem saldırgan tarafından yetkili bir kullanıcıdan geliyormuş gibi mesaj oluşturulmasını içerir.

Ağ Üzerinden Yapılan Saldırı Türleri

4) **İçerik Değiştirme (Content Modification):** Ekleme, silme, sırasını değiştirme veya içeriğini değiştirme yöntemleri ile mesajın değiştirilmesi
5) **Sıra Değiştirme (Sequence Modification):** Ekleme, silme ve yeniden sıralama ile mesajın sırasında değişiklik yapmak.
6) **Zamanlamayı Değiştirme (Timing Modification):** Mesajları geciktirme veya yeniden yollama. Bir bağlantı temelli uygulamada bütün oturum ve mesajların bir kısmı istendiğinde geciktirilebilir yada yeniden yollanabilir.
7) **İnkarcılık (Repudation):** Alınan mesajın varış tarafından inkarı veya gönderilen mesajın kaynak tarafından inkar edilmesi.

Şifreleme Nedir?

- Bir açık metinin bir şifreleme algoritması yardımıyla anlaşılamaz hale getirilmesi işlemine şifreleme denir.



Şifreleme Nedir?

- Şifrelenecek mesaj plaintext (düz-metin) olarak adlandırılır.
- Şifreleme(encryption); veriyi alıcının haricinde kimse okuyamayacak şekilde kodlamaktır.
- Şifrelenmiş mesaja ciphertext (şifreli-mesaj) denir
- Şifre Çözme(Decryption) ise şifrelenmiş veriyi çözüp eski haline getirme işlemidir.
- Veriyi şifrelerken ve çözerken kullanılan matematiksel metoda ise şifreleme algoritması denilmektedir.
- Şifreleme ve çözme genelde bir anahtar(Key) kullanılarak yapılır

Şifreleme Algoritmalarının Performans Kriterleri

- Kırılabilme süresinin uzunluğu.
- Şifreleme ve çözme işlemlerine harcanan zaman (Zaman Karmaşıklığı).
- Şifreleme ve çözme işleminde ihtiyaç duyulan bellek miktarı (Bellek Karmaşıklığı).
- Bu algoritmaya dayalı şifreleme uygulamalarının esnekliği.
- Bu uygulamaların dağıtımındaki kolaylık yada algoritmaların standart hale getirilebilmesi.
- Algoritmanın kurulacak sisteme uygunluğu.

Şifreleme Algoritmaları

- Kriptografide şifreleme için kullanılan anahtarın özellikleri ve çeşidine göre temel olarak iki çeşit şifreleme algoritması bulunmaktadır.
  - Simetrik şifreleme algoritmaları
  - Asimetrik şifreleme algoritmaları

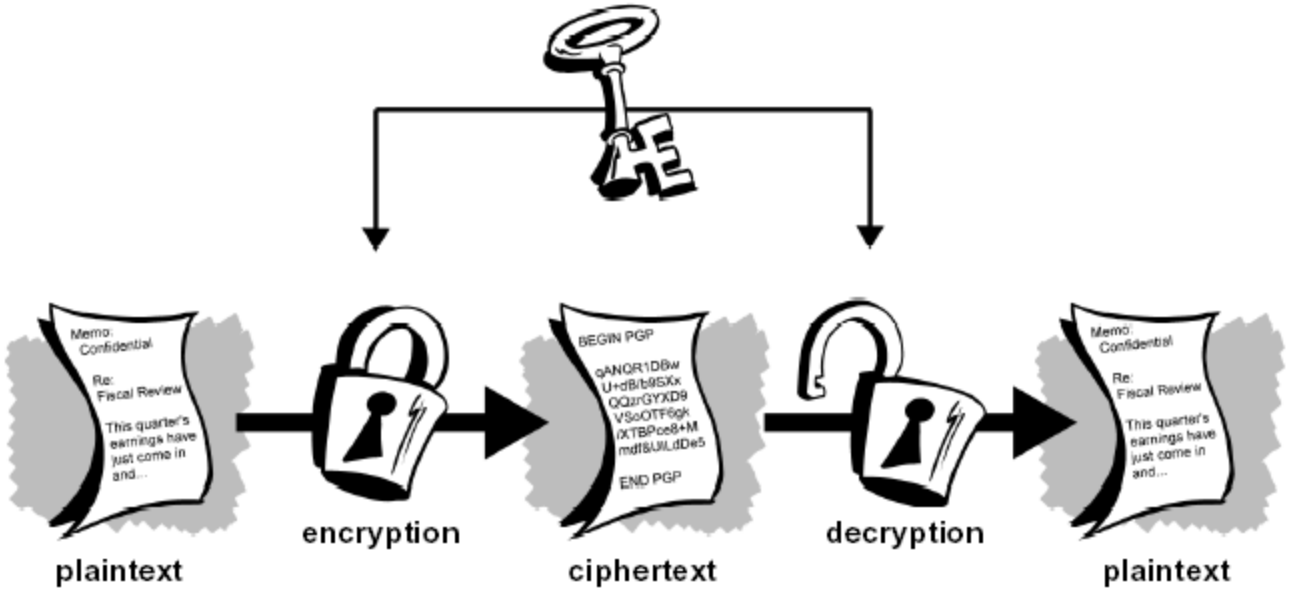
Simetrik Şifreleme Algoritmaları

- Bu algoritmada şifreleme ve şifre çözmek için bir tane gizli anahtar kullanılmaktadır.
- Kullanılan anahtar başkalarından gizlidir ve şifreleme yapan ile şifrelemeyi çözecek kişilerde arasında anlaşılmış ortak bir anahtardır.
- Gönderilecek gizli metinle beraber üstünde anlaşılmış olan gizli anahtar da alıcıya gönderilir ve şifre çözme işlemi gerçekleştirilir.

Simetrik Şifreleme Algoritmaları

- Simetrik şifrelemenin en önemli avantajlarından birisi oldukça hızlı olmasıdır.
- Asimetrik şifrelemeyle karşılaştırıldığında hız konusunda simetrik algoritmalar çok daha başarılıdır.
- Bununla birlikte simetrik algoritmayı içerdiği basit işlemlerden dolayı elektronik cihazlarda uygulamak çok daha kolaydır.
- Ayrıca simetrik algoritmalarda kullanılan anahtarın boyu ve dolayısıyla bit sayısı çok daha küçüktür.

Simetrik Şifreleme Algoritmaları



Simetrik Şifreleme Algoritmaları

- Kuvvetli Yönleri;
  - Algoritmalar olabildiğince hızlıdır.
  - Donanımla birlikte kullanılabilir.
  - Güvenlidir.
- Zayıf Yönleri;
  - Güvenli anahtar dağıtımı zordur.
  - Kapasite sorunu vardır.
  - Kimlik doğrulama ve bütünlük ilkeleri hizmetlerini güvenli bir şekilde gerçekleştirmek zordur.

Simetrik Şifreleme Algoritmaları

- Simetrik algoritmalar blok şifreleme ve dizi şifreleme algoritmaları olarak ikiye ayrılmaktadır.
- Blok Şifreleme Algoritmaları veriyi bloklar halinde işlemektedir.
- Bazen bağımsız bazen birbirine bağlı olarak şifrelemektedir.
- Bu algoritmalarda iç hafıza yoktur, bu yüzden hafızasız şifreleme adını da almıştır.
- Bütünlük kontrolü gerektiren uygulamalarda genellikle blok şifreleme algoritmaları tercih edilir.

Simetrik Şifreleme Algoritmaları

- Dizi şifreleme algoritmaları ise veriyi bir bit dizisi olarak almaktadır.
- Bir üreteç aracılığı ve anahtar yardımıyla istenilen uzunlukta kayan anahtar adı verilen bir dizi üretilir.
- Kayan anahtar üretimi zamana bağlıdır ve bu yüzden bu algoritmalara aynı zamanda hafızalı şifreleme denir.
- Telsiz haberleşmesi gibi gürültülü ortamlarda ses iletimini sağlamak için genellikle dizi şifreleme algoritmaları kullanılır.

Simetrik Şifreleme Algoritmaları - DES

- DES (Data Encryption Standard) : DES yapısı itibari ile blok şifreleme örneğidir.
- Yani basitçe şifrelenecek olan açık metni parçalara bölerek (blok) her parçayı birbirinden bağımsız olarak şifreler ve şifrelenmiş metni açmak içinde aynı işlemi bloklar üzerinde yapar.
- Bu blokların uzunluğu 64 bittir.

Simetrik Şifreleme Algoritmaları - DES

- Dünyada en yaygın kullanılan şifreleme algoritmalarından birisidir.
- DES, IBM tarafından geliştirilmiştir. 1975 yılında "Federal Register" tarafından yayınlanmıştır.
- DES 64 bitlik veriyi 56 bitlik anahtar kullanarak şifreler.
- Ayrıca klasik Feistel Ağı kullanılarak temelde şifreleme işleminin deşifreleme işlemiyle aynı olması sağlanmıştır.
- Kullanılan teknikler yayılma ve karıştırmadır.

Simetrik Şifreleme Algoritmaları - DES

- DES'in en büyük dezavantajı anahtar uzunluğunun 56 bit olmasıdır.
- 1975 yılında yayınlanan bu algoritma günümüzde geliştirilen modern bilgisayarlar tarafından yapılan saldırılar (BruteForce) karşısında yetersiz kalmaktadır.
- Daha güvenli şifreleme ihtiyacından dolayı DES, Triple-DES olarak geliştirilmiştir.
  - Triple -DES algoritması geriye uyumluluğu da desteklemek amacıyla 2 adet 56 bitlik anahtar kullanır.

Simetrik Şifreleme Algoritmaları – Triple DES

- Triple-DES, IBM tarafından geliştirilip 1977'de standart olarak kabul edilmiştir.
- Fakat 1997 yılında İsrail'liler tarafından kırılmış bulunmaktadır.
- Şifreleme metodunun çözülmüş olmasına rağmen günümüz bankacılık sistemlerinde kullanılmakta olan şifreleme sistemidir.
- Triple-DES algoritması, DES algoritmasının şifreleme, deşifreleme, şifreleme şeklinde uygulanmasıdır.

Simetrik Şifreleme Algoritmaları – Triple DES

- Standart DES'in 112 veya 168 bitlik iki veya üç anahtar ile artarda çalıştırılması ile oluşturulan bir şifreleme tekniğidir.
- Anahtar alanı 2112 veya 2168 sayısına ulaşınca bugün için veya tahmin edilebilir bir gelecekte çözülmesi mümkün olmayan bir kod olmaktadır

Simetrik Şifreleme Algoritmaları – IDEA

- IDEA (International Data Encryption Algorithm) 1991 yılında geliştirilmiştir.
- 128 bit anahtar uzunluğu kullanır.
- XOR, 16 bit tam sayı toplama ve 16 bit tam sayı çarpma matematik işlemlerini kullanır.
- Alt anahtar üretim algoritması dairesel kaydırma üzerinedir.

Simetrik Şifreleme Algoritmaları – Twofish

- 1993 yılında yayınlanan bu algoritma Bruce Schneier - John Kelsey - Doug Whiting – David Wagner - Chris Hall - Niels Ferguson tarafından oluşturulmuş simetrik blok şifreleme algoritmasıdır.
- AES kadar hızlıdır.
- Aynı DES gibi Feistel yapısını kullanır.
- DES'den farklarından biri anahtar kullanılarak oluşturulan değişken S-box (Substitution box – Değiştirme kutuları)' lara sahip olmasıdır.

Simetrik Şifreleme Algoritmaları – Twofish

- Ayrıca 128 bitlik düz metni 32 bitlik parçalara ayırarak işlemlerin çoğunu 32 bitlik değerler üzerinde gerçekleştirir.
- AES'den farklı olarak eklenen 2 adet 1 bitlik rotasyon, şifreleme ve deşifreleme algoritmalarını birbirinden farklı yapmış, bu ise uygulama maliyetini arttırmış, aynı zamanda yazılım uygulamalarını %5 yavaşlatmıştır

Simetrik Şifreleme Algoritmaları – IRON

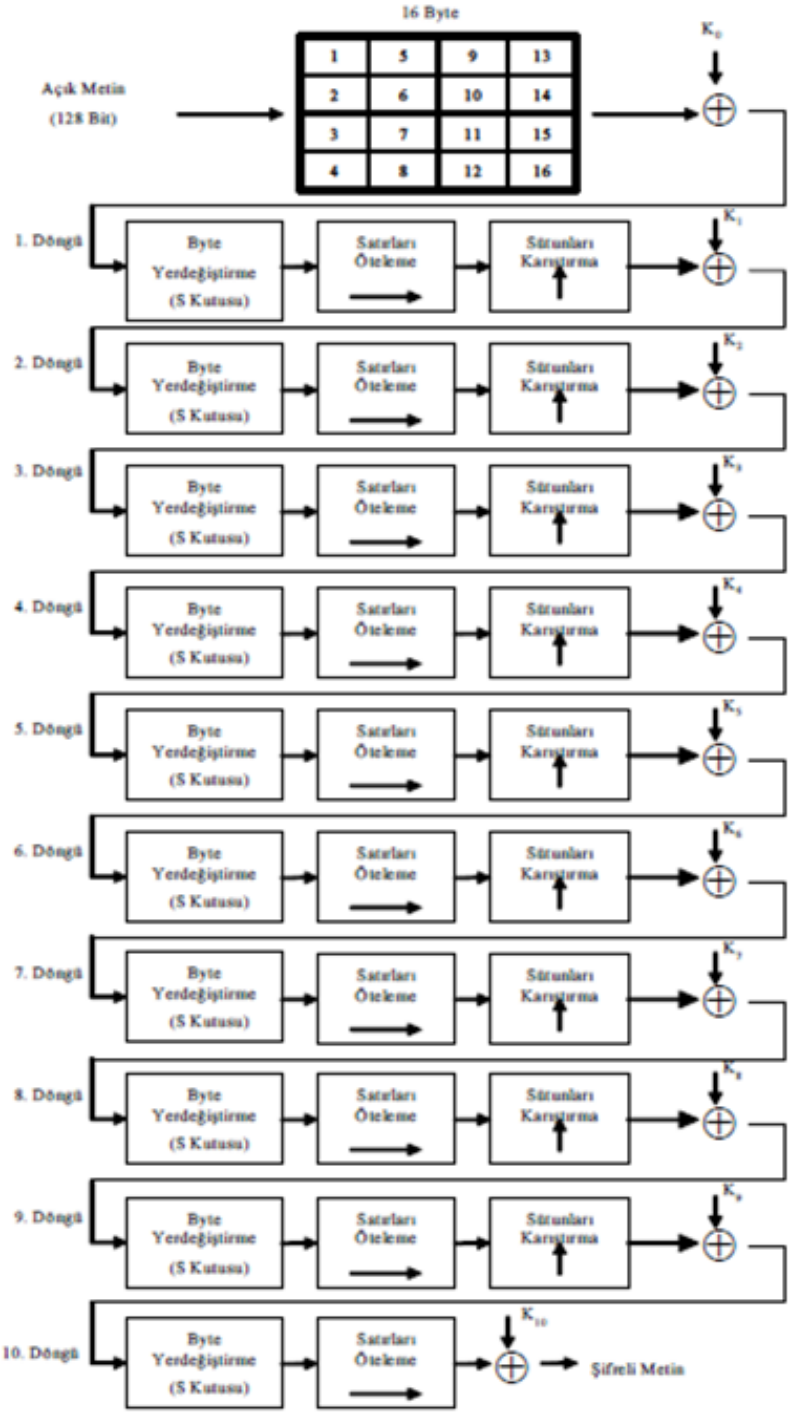
- Diğer iki algoritma gibi Feistel yapısını kullanır.
- IRON, **64 bitlik veri bloklarını 128 bitlik anahtarla** şifrelemede kullanılır.
- Döngü (round) sayısı 16 ile 32 arasındadır.
- Alt anahtarların sayısı döngü sayısına eşittir.
  - Bu nedenden dolayı **algoritma anahtar bağımlıdır.** Var olan algoritmalardan **farkı da** budur.
- Bu algoritmanın avantajı **bitler yerine 16-tabanındaki (hex) sayılar kullanmasıdır, dezavantajı** ise **yazılım için tasarlanmış olmasıdır.**

Simetrik Şifreleme Algoritmaları – AES

- AES, John Daemen ve Vincent Rijmen tarafından **Rijndael adıyla geliştirilmiş ve 2002 yılında standart** haline gelmiştir.
- AES uzunluğu **128 bitte sabit olan blok** ile uzunluğu **128, 192 ya da 256 bit olan anahtar** kullanır.
- Kullanılan tekniklerden bazıları baytların yer değiştirmesi, **4x4' lük matrisler üzerine yayılmış metin** parçalarının satırlarına uygulanan kaydırma işlemleridir.
- **2010 yılı itibariyle en popüler simetrik algoritmalardan biridir.**

AES Döngü Yapısı

	Kelime Uzunluğu	Tur Sayısı
AES-128	4	10
AES-192	6	12
AES-256	8	14



AES Döngü Yapısı

- Her döngü tersi alınabilir dönüşümler kullanır.
- Her döngü, son döngü hariç, 4 dönüşüm kullanır: SubBytes, ShiftRows, MixColumns ve AddRoundKey.
- Son döngüde MixColumns dönüşümü göz ardı edilir.
- Her döngüde farklı anahtar materyali kullanılır.
- Farklı anahtar materyalleri anahtar planlama evresinde gelen anahtarlardır. Master anahtardan farklı anahtarlar elde edilerek şifrede kullanılır.
- Deşifreleme kısmında ters dönüşümler kullanılır: InvSubByte, InvShiftRows, InvMixColumns ve AddRounKey (tersi kendisidir- XOR işlemi).

Simetrik Şifreleme Algoritmaları – RC4

- **RC4 algoritması şifrelenecek veriyi akan bir bit dizisi** olarak algılar.
- RC4 belirlenen anahtar ile veriyi şifreleyen bir algoritmadır.
- Genellikle hız gerektiren uygulamalarda kullanılır.
- **Şifreleme hızı yüksektir ve MB/sn seviyesindedir.**
- Güvenliği **rastgele bir anahtar kullanımına bağlıdır.**
- Anahtar uzunluğu değişkendir.
- **128 bitlik bir RC4 şifrelemesi sağlam bir şifreleme** olarak kabul edilir.
- **Bankacılık ve Dökümantasyon (PDF) şifrelemelerinde** yaygın olarak kullanılır.

Simetrik Şifreleme Algoritmaları – MD5

- MD5 (Message-Digest algorithm 5) Ron Rivest tarafından 1991 yılında geliştirilmiş bir tek yönlü şifreleme algoritmasıdır
- Veri bütünlüğünü test etmek için kullanılan, bir şifreleme algoritmasıdır.
- Bu algoritma girdinin büyüklüğünden bağımsız olarak 128-bit'lik bir çıktı üretir ve girdideki en ufak bir bit değişikliği bile çıktının tamamen değişmesine sebep olur.
- MD5'ın en çok kullanıldığı yerlerden biri, bir verinin (dosyanın) doğru transfer edilip edilmediği veya değiştirilip değiştirilmediğinin kontrol edilmesidir.

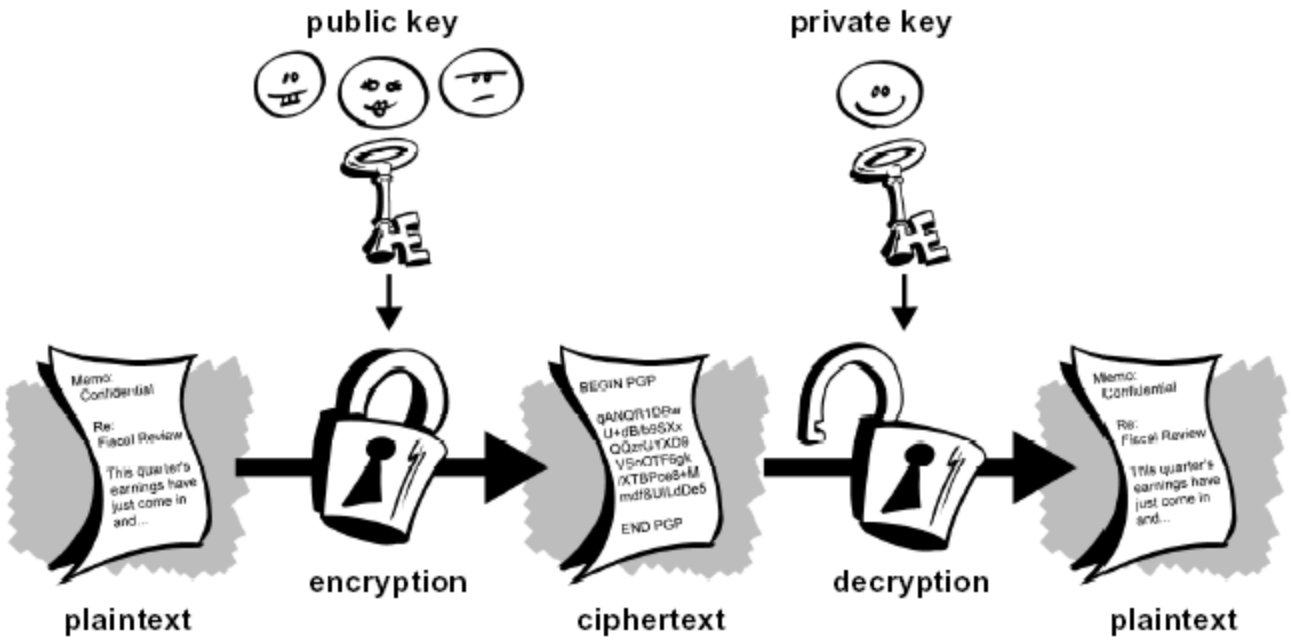
Simetrik Şifreleme Algoritmaları – SHA

- SHA (Secure Hash Algorithm – Güvenli Özetleme Algoritması), Amerika'nın ulusal güvenlik kurumu olan NSA tarafından tasarlanmıştır.
- SHA-1, uzunluğu en fazla 264 bit olan mesajları girdi olarak kullanır ve 160 bitlik mesaj özeti üretir.
- Bu işlem sırasında, ilk önce mesajı 512 bitlik bloklara ayırır ve gerekirse son bloğun uzunluğunu 512 bite tamamlar.
- SHA-1 çalışma prensibi olarak R. Rivest tarafından tasarlanan MD5 özet fonksiyonuna benzer.
- 160 bitlik mesaj özeti üreten SHA-1 çakışmalara karşı 80 bitlik güvenlik sağlar.

Asimetrik Şifreleme Algoritmaları

- 1976 yılında Stanford Universitesinden Diffie ve Hellman adlı araştırmacılar iki farklı anahtara dayalı şifreleme sistemi önermiştir.
- Bu sistemde bir tane şifreleme için (public key) ve bundan farklı olarak bir tanede şifre çözmek için(private key) anahtar bulunur.
- private key, public key' den elde edilemez.
- Asimetrik şifreleme algoritmalarında çok büyük asal sayılar kullanılmaktadır.

Asimetrik Şifreleme Algoritmaları



Asimetrik Şifreleme Algoritmaları

- Kuvvetli Yönleri;
  - Kriptografinin ana ilkeleri olarak sayılan; bütünlük, kimlik doğrulama ve gizlilik hizmeti güvenli bir şekilde sağlanabilir.
  - Anahtarı kullanıcı belirleyebilir.
- Zayıf Yönleri;
  - Şifrelerin uzunluğundan kaynaklanan algoritmaların yavaş çalışması.
  - Anahtar uzunlukları bazen sorun çıkarabiliyor olması.

Asimetrik Şifreleme Algoritmalarının Avantajları

- Asimetrik şifrelemenin kırılması simetrik şifrelemeye göre daha zordur.
- Bu yöntem private-key' lerin karşılıklı aktarılmasını gerektirmez.
  - Böylece simetrik şifrelemedeki anahtar dağıtım problemi çözülmüş olur.
- Public Keylerin bize şifreli mesaj göndermek isteyenler tarafından bilinmesi gerektiğinden bu anahtarlar internette bir sunucu ile rahatça dağıtılmaktadır.
- İki anahtarla şifrelemeden dolayı inkar edememeyi sağlayan sayısal imza gibi yeni yöntemler geliştirilmiştir.

Asimetrik Şifreleme Algoritmalarının Dezavantajları

- Anahtarları kullanarak bilgileri çözme işlemlerinde CPU zamanının çok fazla olması.
- Bu zaman ileti uzunluğu ile üssel olarak artmaktadır.

Asimetrik Şifreleme Algoritmaları – Diffie Helman

- 1976 yılında Diffie ve Helman tarafından bulunmuş ilk asimetrik şifreleme algoritmasıdır.
- DH iki katılımcının öncesinde herhangi bir bilgi alışverişi yapmadan güvenli olmayan bir kanal vasıtasıyla (güvenli bir şekilde) ortak bir şifrede karar kılmalarına yarayan bir protokoldür.
- Algoritma anahtar değişimi ile asıl amacı, iki kullanıcının bir anahtarı güvenli bir şekilde birbirlerine iletmeleri ve daha sonrasında da bu anahtar yardımı ile şifreli mesajları birbirlerine gönderebilmelerini sağlamaktır.
- Diffie–Hellman algoritması oluşturularak simetrik şifreleme algoritmaları için büyük problemi olan gizli anahtarı koruma ve dağıtım büyük ölçüde aşılmıştır.
- Bununla birlikte Diffie-hellman algoritması sadece ortak gizli anahtarı belirlemekte kullanılmaktadır.

Asimetrik Şifreleme Algoritmaları - RSA

- Dünyada en yaygın biçimde kullanılan asimetrik algoritma, ismini mucitlerinin baş harflerinden (Ronald L.Rivest, Adi Shamir ve Leonard Adleman) almıştır.
- Büyük sayıların moduler aritmetiğine dayalı çok basit bir prensibi vardır.
- Anahtarlar, iki büyük asal sayıdan üretilir.
- Dolayısıyla, algoritmanın güvenliği büyük sayı üretme problemine dayalıdır

Asimetrik Şifreleme Algoritmaları - DSA

- DSA (Digital Signature Algorithm) , NIST tarafından sayısal imza standardı olarak yayınlanmıştır.
- Amerika Birleşik Devletleri tarafından kullanılan dijital doğrulama standartlarının bir parçasıdır.
- DSA “discrete logarithm” problemine dayanır ve Schnorr ve ElGamar tarafından geliştirilen algoritmalarla benzer yapıdadır.
- RSA’dan farkı sadece imzalama amaçlı kullanılabilmesi, şifreleme yapılamamasıdır.

Asimetrik Şifreleme Algoritmaları – Eliptik Eğri Algoritması (ECC)

- ECC şifreleme algoritmasının en büyük özelliği diğer açık anahtar şifreleme sitemlerinin güvenliğini daha düşük anahtar değerleriyle sağlayabilmesidir.
- 1024-bitlik anahtar kullanan RSA şifreleme algoritmasının sağladığı güvenlik gücünü, 160-bit anahtar kullanan ECC sağlayabilmektedir.
- Bu açık anahtarlı algoritmalar içinde çok önemli bir avantajdır.
- Yeni gelişen teknolojiyle birlikte kablosuz ağların kullanımı geniş anahtar değerlerine sahip şifreleme algoritmalarının kullanımını zorlaştırmıştır.
- ECC daha düşük anahtar değerlerini kullanması ve aynı güvenlik seviyesini sağlaması sayesinde kablosuz ağlarda kullanımına çok uygundur.

Şifreleme Algoritmaları

- Günümüzde simetrik ve asimetrik şifreleme algoritmalarını birlikte kullanarak hem yüksek derecede güvenlik hem de yüksek hızlı sistemler şifrelenebilmektedir.
- Bu gibi sistemlere melez sistem adı verilir.
- Anahtar şifreleme, anahtar anlaşma ve sayısal imza işlemleri genellikle asimetrik şifrelemeyle, yığın veri işlemleri ve imzasız veri bütünlüğü korumaysa simetriklerle gerçekleştirilir.

İletişim Protokollerini Kullanan Saldırılar

IP Adresi- Internet Protocol Adress

- IP adresi (internet protokol adresi), TCP/IP(iletişim kontrol protokolü/internet protokolü) standardını kullanan bir ağdaki cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve veri haberleşmesinde bulunmak için kullandıkları noktalarla ayrılan 4 sayıdan oluşmaktadır.
- İnternette trafiğin işlemesi bu IP adreslerine bağlıdır.
- Çoğu kullanıcının IP adresi dinamiktir, yani servis sağlayıcınızda o an boş bulunan IP adresi atanır. Bu yüzden her bağlantıda IP adresinizin son numarası değişir.

IP Protokol Türleri

- Bugün halen kullanılmakta ve test edilmekte olan 2 tür internet protokolü bulunmaktadır.
  - IPv4:Günümüzde kullanılmakta olan standart internet protokolüdür ve 32 bitten oluşur.
  - IPv6:Artan ağ kullanıcısı sayısına bağlı olarak daha büyük bir ip adresine ihtiyaç duyulmuştur.Bu ihtiyacı karşılamak ve IPv4'ün eksikliklerini gidermek amacıyla 128 bitten oluşan IPv6 geliştirilmiştir.

IP Adreslerinin Dağıtımı

- IP adresleri IANA başkanlığında RIR(Regional Internet Registry) olarak adlandırılan organizasyonlar tarafından dağıtılır.
- Tüm dünyaya IP dağıtan beş farklı RIR vardır.
- Bunlar bölgelere göre IP dağıtım işlemlerini üstlenmişlerdir.
- Sıradan Internet kullanıcılarına (son kullanıcılara) IP dağıtım işlemi hizmet aldıkları ISS(Internet servis sağlayıcısı) tarafından yapılır.
- Bazı ISS'ler sabit IP adresi verebilirken bazı ISS'ler değişken IP adresi ataması yapar.

IP Sahteciliği (IP Spoofing)

- Internetin çalışmasını sağlayan TCP/IP protokol ailesi geliştirilirken güvenlik temel amaç olmadığı için olabildiğince esnek davranılmıştır.
- Bu esneklik IP adreslerinin aldatılabilir(spoofed) olmasını sağlamıştır.
- Spoofing IP paketlerinin yanlış kaynak adres kullanılarak gönderilmesidir.
- Bu işlem:
  - Saldırıda bulunan kişinin IP adresini gizlemesi, başka bir taraf ya da kişiyi saldırı yapan olarak göstermesi.
  - Güvenilir bir kullanıcı gibi görünmesi yanında network trafiğini dinleme ya da ele geçirme
  - Ortadaki adam saldırısı gibi saldırıları gerçekleştirmek için kullanılır.

IP Sahteciliği (IP Spoofing)

- Genel korunma yöntemleri şu şekilde sayılabilir.
  - Kaynak IP yanında Hedef IP ve MAC kontrolünün yapılması
  - Yönlendiricilerde, kaynak yönlendirme fonksiyonunu pasif hale alınması
  - İç ağın İnternete açıldığı yerde güvenlik duvarı kurulması
  - Paket Filtreleme
  - Şifreleme Yöntemleri

TCP SYN Paketi Akışı Saldırıları

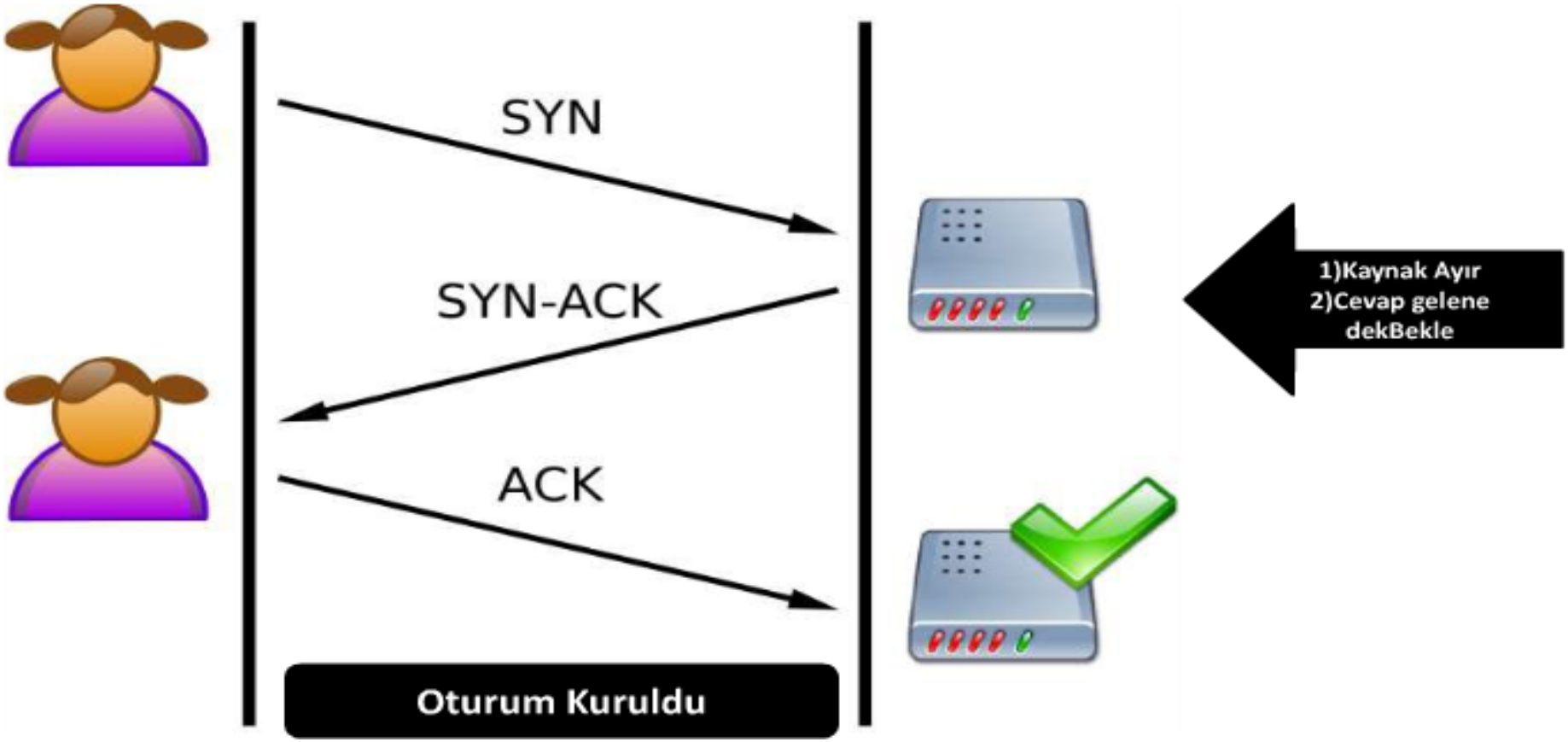
- Genelde TCP/IP servislerini devre dışı bırakmak için kullanılan bir saldırı türüdür.
- TCP bağlantı temelli bir protokoldür.
- Birbiriyle iletişim kuran iki bilgisayar, paketlerini önceden kurulmuş bir hat üzerinden aktarırlar.
- Bunun için iletişimin başlaması esnasında 3 yönlü el sıkışma kuralıyla hat kurulur.

TCP SYN Paketi Akışı Saldırıları

- Bir TCP bağlantısının başında istekte bulunan uygulama SYN paketi gönderir.
- Buna cevaben alıcı site SYN-ACK paketi göndererek isteği aldığını onaylar.
- Son olarak istekte bulunan uygulama ACK göndererek hattın kurulmasını sağlar.

SYN Flood Saldırıları

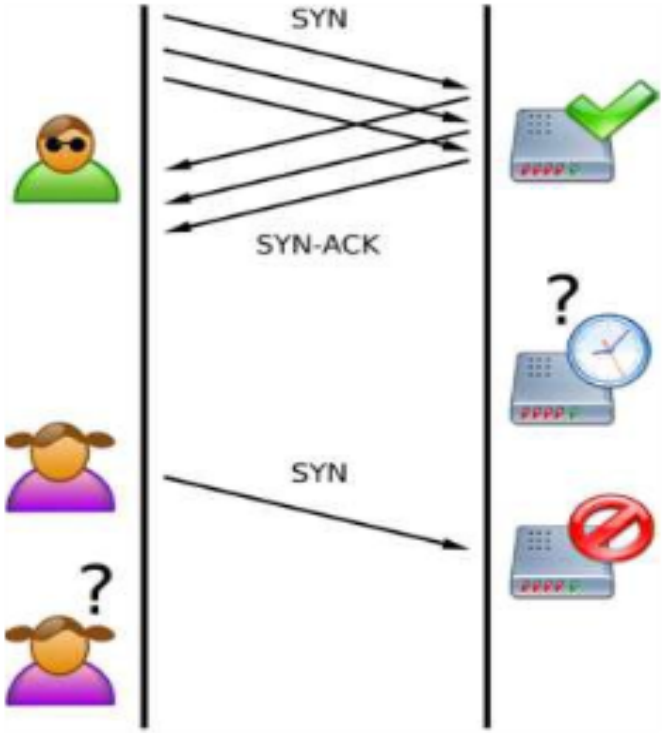
- Normal TCP İşleyişi



TCP SYN Paketi Akışı Saldırıları

- Flood kısa zamanda fazla sayıda bağlantı kurarak siteye zarar verme demektir.
- Bu saldırı türünde saldırgan, internet üzerinde kullanılmayan IP adreslerini kullanarak birçok SYN paketini hedef makineye yollar.
- Hedef makine, alınan her SYN paketi için kaynak ayırır ve bir onay paketini(SYN-ACK), SYN paketinin geldiği IP adresine yollar.
- Hedef makine, kullanılmayan IP adresinden yanıt alamayacağı için SYN-ACK paketini defalarca tekrarlar. Saldırgan bu yöntemi üst üste uyguladığında hedef makine ayırdığı kaynaklardan ötürü yeni bir bağlantıyı kaldıramaz duruma gelir ve bu sebepten makineye bağlanılamaz.

SYN Flood



120 saniye bekler

- Bir SYN paketi ortalama 65 Byte
- 8Mb ADSL sahibi bir kullanıcı saniyede 16.000/4 SYN paketi üretebilir, 100 ADSL kullanıcısı?

IP Servis Durdurma Saldırıları

- Bu saldırı türünde (smurf), saldırgan hedef bilgisayardan ping isteğinde bulunur.
- Ancak ping paketi, hedef makinenin IP'sinden geliyormuş gibi görünecek şekilde hazırlanmıştır.
- Bu durumda ağ üzerindeki bütün makineler, hedef makineye ping atar.
- Hedef makine bu trafiği karşılayamaz ve bağlantı kesilir.

IP Parçalama Saldırıları

- MTU (Maximum Transfer Unit) Nedir?
  - MTU değeri bir ağa girişteki maksimum kapasiteyi belirmektedir.
    - Örneğin Ethernet ağları için MTU değeri 1500 byte, FDDI için 4500 byte'dır. Bu da ethernet ağa giren bir paketin boyutunun maksimum 1500 byte, FDDI ağa giren bir paketin boyutu en fazla 4500 byte olabileceğini gösterir.
  - MTU değerleri farklı iki ağ arasında geçişlerde eğer ilk ortamın MTU değeri daha büyükse IP paketlerinde yeni girilecek ortama göre parçalama işlemi yapılır.

IP Parçalama Saldırıları

- Parçalanmış paketlerin hedefe ulaştığında doğru sırada birleştirilmesi gerekir.
- Paketler hedefe ulaştığında tekrar birleştirilip orijinalinin elde edilmesi için her pakette bulunması gereken bazı alanlar vardır.
  - Fragmentation ID (IP ID): Bir IP datagramına ait parçalanmış tüm paketlerde bu değer aynı olmalıdır.
  - Parçalanmıs her paket datagramın hangi kısmını taşıdığını (Offset Değeri ve Sırasını) bilmelidir. Kendisinden sonra ek parça paket varsa bu alan **flags[+]**, paketin kendisi son paket ise değer **flags[none]** olur.
  - Parçalanmış her paket taşıdığı veri boyutunu ve hangi byte'dan itibaren taşıdığını bilmelidir.

IP Parçalama Saldırıları

- Öncelikle paket parçalamanın olağan bir durumdur. İyi niyetlerle düşünülmüş bu özellik bugüne kadar çeşitli ciddi güvenlik sorunlarına sebep olmuştur.
- Parçalanmış paketlerin sadece birincisinde protokol bilgisi bulunmaktadır. Güvenlik duvarları protokole göre paketleri alır ya da reddeder. Bu durumda sadece ilk paket alınacak yada reddedilecek ama diğer paketler sisteme girebilecektir.

UDP Portlarından Saldırılar

- UDP, TCP / IP protokol grubunun iki aktarım katmanı protokolünden birisidir.
- TCP/IP ailesinin iletim katmanında yer alır.
- UDP güvenilir olmayan bir aktarım protokolüdür. UDP protokolü ağ üzerinden paketi gönderir, gidip gitmediğini takip etmez ve paketin yerine ulaşıp ulaşmayacağına onay verme yetkisi yoktur.

UDP Portlarından Saldırılar

- Bir bilgisayar üzerinde veya birkaç bilgisayar arasında,UDP portlarına yöneltilecek yoğun paket akışıyla gerçekleştirilen bu saldırılar, tek bir bilgisayar üzerinde gerçekleştiriliyorken bu bilgisayarın performansının düşmesine, birden fazla bilgisayar arasında gerçekleştiriliyorken ise, ağın performansının düşmesine sebep olacaktır.
- Birbiriyle haberleşmekte olan iki UDP servisinden birisi veya her ikisi üreteceği yoğun paket akışıyla, karşısındaki bilgisayarın servisini kilitlemeyi, bilgisayarın performansını kötüleştirmeyi başarabilir.
- UDP servisleri bağlantı temelli olmadıklarından, herhangi bir el sıkışma mekanizması ya da bazı kontrol bilgilerinin karşılıklı değerlendirilmesi gerekmediğinden, bu tür saldırılara açıktır.

UDP Portlarından Saldırılar

- Örneğin 7 numaralı portu kullanan UDP echo servisi, karşısındaki bilgisayardan (istemci) aldığı bilgileri olduğu gibi geri gönderir.
- 19 numaralı port üzerinden servis veren UDP chargen servisi ise, istemci bilgisayardan her paket alışında, rastgele sayıdaki verilerden oluşan paketi geri gönderir.
- Bu iki servise ilişkin UDP portlarının aynı bilgisayar üzerinde veya değişik bilgisayarlar arasında birbirine bağlanması, sonsuz bir trafiğin oluşmasına sebep olacaktır.
- Bu hem servisi veren bilgisayarı hem de trafiğin aktığı ağı etkileyecektir.

UDP Portlarından Saldırılar

- Böyle bir saldırı sonucunda doğabilecek sonuçlar şunlardır:
  - Saldırının yöneltildiği servisler kilitlenebilir.
  - Bu servisleri veren bilgisayarların performansı düşebilir
  - Servisleri veren bilgisayarların bulunduğu ağın trafiğini arttırır.
- Bu saldırı tipinden korunmak için alınabilecek önlemlerin başında saldırıda kullanılan servisleri bilgisayarın üzerinden kaldırmak gelir.

UDP Portlarından Saldırılar

- Bu yaklaşımı kullanırken iptal edilecek servislerin ne kadar gerekli olduğu da önemlidir.
- Bu saldırılarda en çok kullanılan UDP servisleri chargen ve echo servisleridir. Bu servisler neredeyse hiç kullanılmazlar. Dolayısıyla bu servislerin iptal edilmesi ya da güvenlik duvarı üzerinden filtrelenmesi, normal çalışmayı etkilemeyecektir.
- Saldırıların daha çok hangi servislere yapıldığının tespiti için ağa saldırıları kontrol edip raporlayan programların kurulması faydalı olacaktır.

ARP Saldırıları

- ARP (Address Resolution Protocol- Adres Çözümleme Protokolü) IP adreslerini fiziksel adrese dönüştürmek için kullanılır.
- Bir paketin bir bilgisayardan çıktığında nereye gideceğini IP numarası değil gideceği bilgisayarın fiziksel adresi (MAC) belirler.
- Bu adres de paketin gideceği IP numarası kullanılarak elde edilir.

ARP Saldırıları

- Ardından paket yönlendirilir.
- ARP adres çözümlemek istediği zaman tüm ağa bir ARP istek mesajı gönderir ve bu IP adresini gören yada bu IP adresine giden yol üzerinde bulunan makine bu isteğe cevap verir ve kendi fiziksel adresini gönderir.
- ARP isteğinde bulunan makine bu adresi alarak verileri bu makineye gönderir.

ARP Saldırıları

- Protokol adreslerinin fiziksel adreslere çevrilmesi işine adres çözümleme (address resolution) denilir.
- Çevrilen adres “çözülen” (resolved) olarak adlandırılır.
- Bir bilgisayar diğer bir bilgisayarın adresini ancak ikisi de fiziksel olarak aynı ağ üzerinde ise bulacaktır.
- Farlı ağlardaki bilgisayarlar birbirlerinin adreslerini çözemezler.

ARP Saldırıları

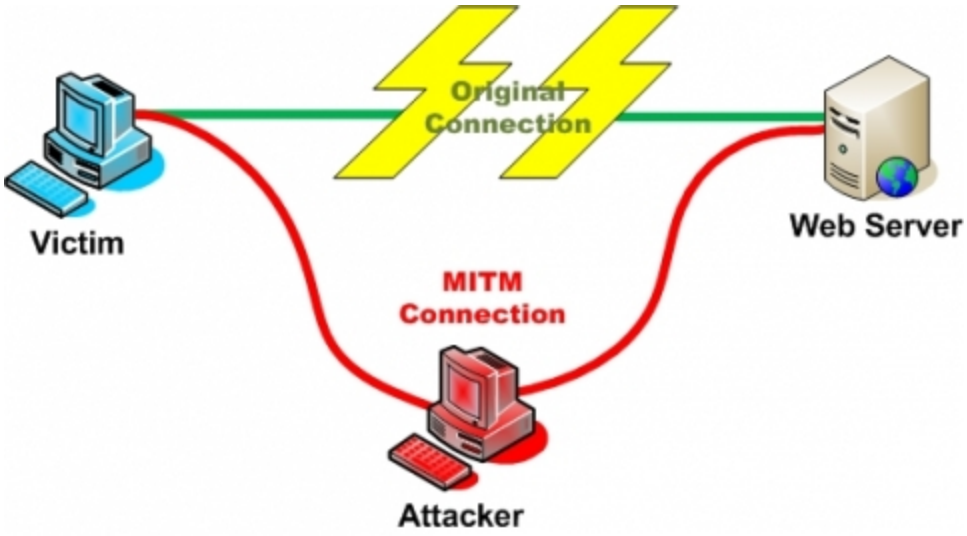
- ARP'de iki temel mesaj vardır. Birisi istek (request) diğeri cevap (response) mesajlarıdır.
- İstek mesajı IP adresi içerir ve karşılık gelen fiziksel adresi ister.
- Cevap ise hem IP hem de aranan fiziksel adresi içerir.
- ARP istekleri broadcast mesajlardır. Cevaplar ise broadcast değil unicasttir.
- Sonuç olarak
  - Ağ üzerinde iki bilgisayarın veri iletişiminde bulunabilmesi için hedef bilgisayar MAC adresini bilmesi gerekir.
  - Veriyi göndermek isteyen bilgisayar hedef bilgisayarın MAC adresini öğrenmek amacıyla adres çözümleme protokolünü (ARP) kullanır.

ARP Saldırıları

- ARP sahtekarlığı (ARP spoofing, ARP flooding, ARP poisoning) saldırısı lokal ağlarda gerçekleştirilebilen bir saldırıdır. Bu saldırı, üç şekilde gerçekleştirilmektedir:
  - **MAC Flooding:** Hedef bilgisayarın ARP tablosunun yanlış bilgilerle dolmasını sağlayarak, hedef bilgisayarın göndereceği paketlerin saldırganın istediği adreslere gitmesini sağlamaktır.

ARP Saldırıları

- **Man in the Middle:** Bu saldırıda saldırgan, sahte ARP (spoofed ARP) çerçevelerinin içerisine kendi bilgisayarının MAC adresini yazmak suretiyle hedef bilgisayardan çıkan tüm paketlerin kendi bilgisayarı üzerinden geçmesini sağlar.
- Böylece kullanıcının hangi sitelere girdiğinden tutunda, gönderdiği aldığı maillere, şifrelere vs. kadar bilgileri alabilir.



ARP Saldırıları

- **Denial of Service:** Bu saldırı türünde saldırganın amacı, hedef bilgisayardan dışarı çıkacak olan paketleri dinlemek değil, hedef bilgisayara servis dışı bırakma (DoS) saldırısı yapmaktır.
- Saldırgan tüm ağda yer alan bilgisayarlara sahte ARP mesajları yollar.
- Bu mesajların içerisine de hedef bilgisayarın MAC adresini yazar.
- Böylece ağda yer alan tüm bilgisayarlar paketlerini hedef bilgisayara yollar. Bu da hedef bilgisayarın ethernet bağlantısının limitinin dolmasına sebep olur.

ARP Saldırıları

- ARP saldırılarından korunabilmek için alınabilecek önlemler şunlardır.
  - Statik veya Dinamik ARP koruması kullanımı
  - ARP sınırlama