Adı :Halil Durmuş

Numara:150757017

Bölüm :Bilgisayar Mühendisliği(İ.Ö)

**Bölüm 2.2.12 :IP Güvenliğine Giriş**

**İçindekiler Sayfa**

1. **IPSec'e Giriş 2**
2. **Özellikler 2**
   1. **Dönüşüm Bağımsızlığı ile Ayrı Gizlilik 2**

**ve Kimlik Doğrulama İşlevleri**

* 1. **Tek Yönlü Kurulum ile Ağ Katmanı (IP) Uygulaması 3**
  2. **Ana Bilgisayar ve Ağ Geçidi Topolojileri 3**
  3. **Anahtar yönetimi 3-4**

1. **Uygulama ve Yapılar 4**
   1. **Güvenlik Birlikleri (SA) 5-6**
   2. **Güvenlik Parametreleri Endeksi (SPI) 6**
   3. **Kimlik Doğrulama Fonksiyonu 6-7**
   4. **Gizlilik İşlevi 7-8**
   5. **Anahtar Yönetimi 8-9**
   6. **İnternet Güvenliği Birliği ve Anahtar 9-10 Yönetimi Protokolü (ISAKMP) 11**
   7. **Bulgular 12**
2. **Özet 12-13**

**1.1.IPSec'e Giriş**

IP Güvenlik Protokolü Çalışma Grubu (IPSec), 1992 yılında İnternet Mühendisliği Görev Gücü (IETF) tarafından IP sürüm 4 ve ortaya çıkan sürüm 6 protokollerinde gizlilik ve kimlik doğrulama hizmetlerini uygulamak için standart bir yöntem geliştirmek üzere kuruldu. akılda çeşitli özgül hedefleri vardı. Mimarlığın geniş çapta benimsenmesi için esnek olması gerekirdi. Şifreleme teknolojisindeki değişikliklerin yanı sıra şifreleme kullanımına ilişkin uluslararası kısıtlamaları da barındırabilmelidir. İkinci olarak, mimarlık, standart veya yayın (çok noktaya yayın) modlarında tüm istemci IP protokollerini (yani, İletim Kontrol Protokolü veya TCP, Kullanıcı Datagram Protokolü veya UDP) desteklemelidir. Üçüncüsü, iki ana bilgisayar veya birden fazla ana bilgisayar, iki alt ağ veya çoklu alt ağ veya bir ana bilgisayar ve alt ağ kombinasyonu arasındaki iletişimi sağlayabilmelidir. Son olarak, şifreleme anahtarlarını otomatik olarak dağıtmak için bir yöntem olması gerekiyordu. Bu bölüm, IPSec güvenlik mimarisinin temel özelliklerini, ana bileşenlerini ve uyum için asgari zorunlu gereksinimleri kapsayacaktır.

**Amaç:** IPSEC standart ip paketlerine uygulanır. Temel amaç verilerin şifreleme yöntemi ile güvenliğinin sağlanması ve doğrulama mekanizmalarının işletilmesidir.

**METERYAL VE YÖNTEM**

**2.Özellikler**

IPSec'in hedefleri aşağıdaki temel mimari özelliklere dönüştürülmüştür.

**Dönüşüm Bağımsızlığı ile Ayrı Gizlilik ve Kimlik Doğrulama İşlevleri**

IPSec gizlilik ve kimlik doğrulama hizmetleri birbirinden bağımsızdır. Bu, uygulamalarını basitleştirir ve ana bilgisayar sistemi üzerindeki performans etkilerini azaltır. Ayrıca, son kullanıcılara işlemleri için uygun güvenlik seviyesini seçme imkanı verir. Güvenlik işlevleri, şifreleme dönüşümlerinden bağımsızdır. Bu, temel şifrelemeyi değiştirmeden yeni şifreleme teknolojilerinin IPSec'e dahil edilmesine olanak tanır ve yere özgü kullanım ve ihracat kısıtlamalarıyla uyuşmazlığı önler. Ayrıca, son kullanıcıların kendi özel güvenlik gereksinimlerini en iyi şekilde karşılayan dönüşümleri gerçekleştirmesini mümkün kılar.

Kullanıcılar düşük uygulama maliyetleri, minimum performans etkileri ve az sayıda uluslararası kullanım kısıtlaması olan karma şifreleme kullanarak kimlik doğrulama hizmetlerini seçebilirler. Bu uygulamalar geniş çapta dağıtılabilir ve günümüzdeki İnternet işlemlerinin çoğu için güvenlik konusunda önemli bir gelişme sağlar. Veya kullanıcılar, özel anahtar şifrelemesine dayalı gizlilik işlevlerini seçebilir. Bunların uygulanması daha zordur, daha yüksek performans etkilerine sahiptir ve çoğu zaman uluslararası kullanım kısıtlamalarına tabidir, bu nedenle çok daha yüksek bir güvenlik seviyesi sağlasalar da dağıtımları ve kullanımları genellikle sınırlıdır. Veya mümkün olan en yüksek güvenlik seviyesini sağlamak için bu fonksiyonları birleştirebilirler.

**2.1.Tek Yönlü Kurulum ile Ağ Katmanı (IP) Uygulaması**

Ağ katmanında güvenlik işlevinin tanıtılması, tüm istemci IP protokollerinin, bireysel özelleştirmeler olmadan güvenli bir şekilde çalışabileceği anlamına gelir. Dış Ağ Geçidi Protokolü (EGP) ve Sınır Ağ Geçidi Protokolü (BGP) gibi yönlendirme protokollerinin yanı sıra, TCP ve UDP gibi bağlantı ve bağlantısız taşıma protokolleri güvence altına alınabilir. Bu istemci protokollerini kullanan uygulamalar, IPSec güvenlik hizmetlerinden yararlanmak için hiçbir değişiklik gerektirmez. IPSec servislerinin eklenmesi, doğal güvenlik açıklarına (örneğin, açık metin şifresi) sahip uygulamaları, tek bir sistem değişikliği ile güvenli hale getirmeyi mümkün kılar. Ve bu değişiklik, IP hizmetleri ya da kullandıkları taşımalardan bağımsız olarak bu tür bir uygulamayı güvence altına alacaktır.

Bu özellik, hedef adresin belirlenemediği çok noktaya yayın ve tek noktaya yayın paketlerini kullanarak akış hizmetlerini bile genişletir. IPSec bunu, güvenli bağlantılar kurmak için tek yönlü bir başlatma şeması kullanarak mümkün kılar. Gönderen istasyon, bir ayar dizinini alıcı istasyona geçirir. Alıcı istasyon bu dizini, bağlantıyı yöneten güvenlik parametreleri tablosuna başvurmak için kullanır. Alıcı istasyonun güvenli tek yönlü bir bağlantı kurmak için gönderen istasyonla etkileşime girmesi gerekmez. İki yönlü bağlantılar için işlem tersine çevrilir. Alıcı istasyon gönderici olur ve kurulum dizinini göndericiye geri iletir. İstasyon gönderme ve alma, ana bilgisayarlar veya güvenlik ağ geçitleri olabilir.

**2.2.Ana Bilgisayar ve Ağ Geçidi Topolojileri**

IPSec iki temel bağlantı topolojisini destekler: ana bilgisayardan ana bilgisayara ve ağ geçidinden ağ geçidine. Ana bilgisayar (bazen baştan sona denilen) topolojisinde, gönderme ve alma sistemleri, kendi aralarında veri iletmek için güvenli bağlantılar kuran iki veya daha fazla ana bilgisayardır. Ağ geçidi (alt ağdan alt ağa da denir) topolojisinde, gönderme ve alma sistemleri, kendi iç (güvenilir) alt ağlarına bağlı güvenilir ana bilgisayarlar adına dış (güvenilmeyen) sistemlerle bağlantı kuran güvenlik ağ geçitleridir. Güvenilir bir alt ağ çalışması, pasif veya aktif saldırılara girmemesi için birbirlerine güvenen bir veya daha fazla ana bilgisayar içeren bir iletişim kanalı (örneğin, Ethernet) olarak tanımlanır. Bir ağ geçidinden ağ geçidine bağlantı genellikle bir tünel veya sanal bir özel ağ (VPN) olarak adlandırılır. Üçüncü bir senaryo, ev sahibi ağ geçidine de mümkündür. Bu örnekte, güvenlik ağ geçidi, bir harici alt ağlarda harici ana bilgisayarlar ve güvenilir ana bilgisayarlar arasında bağlantı kurmak için kullanılır. Bu senaryo, Internet gibi güvenilmeyen ağlar aracılığıyla iç sistemlerdeki uygulamalara ve verilere erişmesi gereken seyahat eden çalışanlar veya telekomünikasyon cihazları için özellikle yararlıdır.

**2.3.Anahtar yönetimi**

Şifreleme anahtarlarını etkin bir şekilde yönetme ve dağıtma yeteneği, herhangi bir şifreleme sisteminin başarısı için çok önemlidir. IP Güvenlik Mimarisi, genel ve özel anahtar tabanlı sistemleri ve manuel veya otomatik anahtar dağıtımını destekleyen bir uygulama katmanı anahtar yönetimi şeması içerir. Aynı zamanda diğer prensip oturum parametrelerinin dağılımını da destekler. Bu işlevlerin standartlaştırılması, IPSec güvenlik işlevlerinin birden çok güvenlik alanında ve satıcı platformlarında kullanılmasını ve yönetilmesini mümkün kılar. IPSec Güvenlik Mimarisinin diğer iki önemli özelliği, Çok Düzeyli Güvenliği (MLS) olan sistemler ve tüm standart IPSec tipi kodlar için atanmış IANA (İnternet Atanmış Numaralar Otoritesi) kullanan sistemleri desteklemesidir.

**3.Uygulama ve Yapılar**

IPSec Güvenlik Mimarisi iki IP başlık yapısı etrafında toplanmıştır: Kimlik Doğrulama Başlığı (AH) ve Kapsülleme Güvenlik Yükü (ESP) başlığı. Bu mekanizmaların nasıl işlediğini tam olarak anlamak için, güvenlik dernekleri kavramına bakmak gerekir. Algoritma bağımsızlığını elde etmek için, oturum parametrelerini belirlemek için esnek bir yöntem oluşturulmalıdır. Güvenlik dernekleri (SA) bu yöntem haline geldi

**3.1.Güvenlik Birlikleri (SA)**

Güvenlik birliği, bir veya daha fazla ağ bağlantısındaki güvenlik işlemlerini yöneten bir dizi güvenlik parametresinden oluşan bir tablo veya veritabanı kaydıdır. Güvenlik dernekleri yukarıda belirtilen tek yönlü başlatma planının bir parçasıdır. SA tabloları alıcı ana bilgisayara oluşturulur ve gönderen ana bilgisayar tarafından Güvenlik Parametreleri Dizini (SPI) olarak bilinen bir dizin parametresi kullanılarak referans alınır. Bir SA'daki en yaygın girişler:

* Dönüşümün türü ve çalışma modu, örneğin blok zincirleme modunda DES. Bu gerekli bir parametredir. IPSec'in bağımsız olarak dönüştürülmek üzere tasarlandığını unutmayın, bu nedenle anlamlı bir veri alışverişi gerçekleşecekse, bu bilgiler uç noktalar arasında senkronize edilmelidir.
* Dönüşüm algoritması tarafından kullanılan anahtar veya anahtarlar. Bariz nedenlerden dolayı bu da zorunlu bir parametredir. Anahtarların kaynağı değişebilir. SAS ana bilgisayar veya ağ geçidi üzerine tanımlandığında manuel olarak girilebilirler. Anahtar dağıtım sistemi aracılığıyla tedarik edilebilirler veya - asimetrik şifreleme durumunda, ortak anahtar bağlantı kurulumu sırasında kablo üzerinden gönderilir.
* • Şifreleme algoritmasının senkronizasyon veya ilklendirme vektörü. Bazı şifreleme algoritmalarının, özellikle de zincirleme kullananların, şifreleme sırasını senkronize etmek için alıcı sisteme bir ilk veri bloğu sağlaması gerekebilir. Genellikle, şifreli verilerin ilk bloğu bu amaca hizmet eder, ancak bu parametre diğer uygulamalara izin verir. Bu parametre tüm ESP uygulamaları için gereklidir, ancak senkronizasyon gerekli değilse “yok” olarak tanımlanabilir.
* Dönüştürme anahtarlarının ömrü. Parametre bir sürenin ifadesi veya bir anahtar değişikliğinin gerçekleşeceği belirli bir zaman olabilir. Kriptografik anahtarlar için önceden belirlenmiş bir kullanım ömrü yoktur. Anahtarların ne sıklıkta değiştiği sıklığı tamamen güvenlik noktalarının son noktalardaki takdirine bağlıdır. Bu nedenle, bu parametre yalnızca tavsiye edilir, gerekli değildir
* Güvenlik birliğinin ömrü. Bir güvenlik birliği için önceden belirlenmiş bir yaşam süresi yoktur. Bir güvenlik birliğinin yürürlükte kaldığı süre, son nokta uygulayıcılarının takdirindedir. Bu nedenle, bu parametre de önerilir, ancak gerekli değildir.
* Güvenlik birliğinin kaynak adresi. Bir güvenlik birliği normalde sadece bir yönde kurulur. İki uç nokta arasındaki bir iletişim oturumu genellikle iki güvenlik birliğini içerecektir. Birden fazla gönderen ana bilgisayar bu güvenlik ilişkisini kullanırken, parametre bir joker değerine ayarlanabilir. Genellikle bu adres IP başlığındaki kaynak adresle aynıdır; bu nedenle, bu parametre önerilir, ancak gerekli değildir.
* Korunan verilerin hassasiyet seviyesi. Bu parametre, çok düzeyli güvenliği uygulayan ana bilgisayarlar için gereklidir ve diğer tüm sistemler için önerilir. Parametre, uç noktaların doğru yönlendirilmesini ve kullanılmasını sağlamak için güvenlik etiketleri (örneğin, Gizli, Gizli, Sınıflandırılmamış) ekleme yöntemi sağlar.

Güvenlik ilişkileri normalde sadece bir yönde kurulur. Güvenli bir iletim kurulmadan önce, gönderme ve alma ana bilgisayarlarında SA'lar oluşturulmalıdır. Bu güvenlik ilişkileri anahtar yönetim protokolü aracılığıyla manuel veya otomatik olarak yapılandırılabilir. Bir (güvenli) alıcı ana bilgisayara yönelik bir datagram gönderilmeye hazır olduğunda, gönderme sistemi uygun güvenlik ilişkisini arar ve ortaya çıkan endeks değerini alıcı ana bilgisayara iletir. Alıcı ana sistemde ilgili SA'yı aramak için SPI ve hedef adresini kullanır. Çok seviyeli güvenlik durumunda, güvenlik etiketi de SA seçim sürecinin bir parçası haline gelir. Alıcı sistem daha sonra gönderen ana bilgisayardan sonraki tüm paketleri işlemek için bu SA parametrelerini kullanır. Tam kimliği doğrulanmış bir iletişim oturumu oluşturmak için, gönderme ve alıcı ana bilgisayarlar rolleri tersine çevirir ve ters yönde ikinci bir SA kurar. Bu tek yönlü SA seçim şemasının bir avantajı, trafo yayın türlerini desteklemesidir. Güvenlik dernekleri, yalnızca bu alıcı senaryosunda bile, alıcı ana bilgisayarın SPI'yi seçmesini sağlayarak kurulabilir. Tek noktaya yayın paketlerine tek bir SPI değeri atanabilir ve çok noktaya yayın paketlerine her çok noktaya yayın grubu için bir SPI atanabilir. Ancak, IPSec'in yayın trafiği için kullanımı bazı ciddi sınırlamalara sahiptir. Anahtar yönetimi ve dağıtımı çok zordur ve kriptografinin değeri azalır çünkü paketin kaynağı pozitif olarak kurulamaz.

Güvenlik ilişkileri normalde sadece bir yönde kurulur. Güvenli bir iletim kurulmadan önce, gönderme ve alma ana bilgisayarlarında SA'lar oluşturulmalıdır. Bu güvenlik ilişkileri anahtar yönetim protokolü aracılığıyla manuel veya otomatik olarak yapılandırılabilir. Bir (güvenli) alıcı ana bilgisayara yönelik bir datagram gönderilmeye hazır olduğunda, gönderme sistemi uygun güvenlik ilişkisini arar ve ortaya çıkan endeks değerini alıcı ana bilgisayara iletir. Alıcı ana sistemde ilgili SA'yı aramak için SPI ve hedef adresini kullanır. Çok seviyeli güvenlik durumunda, güvenlik etiketi de SA seçim sürecinin bir parçası haline gelir. Alıcı sistem daha sonra gönderen ana bilgisayardan sonraki tüm paketleri işlemek için bu SA parametrelerini kullanır. Tam kimliği doğrulanmış bir iletişim oturumu oluşturmak için, gönderme ve alıcı ana bilgisayarlar rolleri tersine çevirir ve ters yönde ikinci bir SA kurar. Bu tek yönlü SA seçim şemasının bir avantajı, trafo yayın türlerini desteklemesidir. Güvenlik dernekleri, yalnızca bu alıcı senaryosunda bile, alıcı ana bilgisayarın SPI'yi seçmesini sağlayarak kurulabilir. Tek noktaya yayın paketlerine tek bir SPI değeri atanabilir ve çok noktaya yayın paketlerine her çok noktaya yayın grubu için bir SPI atanabilir. Ancak, IPSec'in yayın trafiği için kullanımı bazı ciddi sınırlamalara sahiptir. Anahtar yönetimi ve dağıtımı çok zordur ve kriptografinin değeri azalır çünkü paketin kaynağı pozitif olarak kurulamaz.

**3.2.Güvenlik Parametreleri Endeksi (SPI)**

Güvenlik Parametreleri Dizini, bir güvenlik ilişkisini (SA) benzersiz şekilde tanımlamak için kullanılan 32 bit sözde rasgele bir sayıdır. Bir SPI'nin kaynağı değişebilir. SA ana bilgisayar veya ağ geçidi üzerine tanımlandığında manuel olarak girilebilir veya bir SA dağıtım sistemi aracılığıyla sağlanabilir. Açıkçası, güvenlik fonksiyonunun düzgün çalışması için, SPI'ların bitiş noktaları arasında senkronize edilmesi gerekir. 1 ile 255 arasındaki SPI değerleri, açıkça belirtilmiş (diğer bir deyişle standart) uygulamalarda kullanılmak üzere IANA tarafından ayrılmıştır. SPI'ler minimum yönetim gerektirir ancak önceden atanmış SPI'lerin ilişkili SA'ları silindikten sonra çok hızlı bir şekilde tekrar kullanılmamasını sağlamak için bazı önlemler alınmalıdır. SPI değeri sıfır (0), bu işlem için bir güvenlik ilişkisinin bulunmadığını belirtir. Ana bilgisayardan ana bilgisayara bağlantılarda, SPI alıcı ana bilgisayar tarafından güvenlik ilişkisini aramak için kullanılır. Bir ağ geçidinden ağ geçidine, tek noktaya yayın veya çok noktaya yayın işleminde alıcı sistem, uygun SA'yı belirlemek için SPI'yı hedef adresle (ve bir MLS sisteminde, güvenlik etiketiyle) birleştirir. Şimdi, IPSec kimlik doğrulama ve gizlilik işlevlerinin SA ve SPI'leri nasıl kullandığına bakacağız.

**3.3.Kimlik Doğrulama Fonksiyonu**

IPSec kimlik doğrulaması (IPSec). Varsayılan algoritma, yeniden değerlendirme yapılmayan Message Digest sürüm 5 (MD5) olarak anahtarlanmıştır. Reddedilmeme için kullanılabilir. IPSec kimlik doğrulama fonksiyonu, gizlilik veya trafik fonksiyonu c analiz koruması sağlamaz.

İşlev, güvenlik ilişkisinde (SA) belirtilen algoritma ve tuşları kullanarak tüm datagram üzerinde hesaplanır. Hesaplama, fragmantasyondan önce yapılır ve taşıma sırasında değişen alanlar (örneğin, ttl veya hop sayısı) hariç tutulur. Ortaya çıkan kimlik doğrulama verileri, SA'ya atanan Güvenlik Parametre Dizini (SPI) ile birlikte Kimlik Doğrulama Başlığına (AH) yerleştirilir. Kimlik doğrulama verilerini orijinal veri programına eklemek yerine kendi yük kapasitesi yapısına (AH) yerleştirmek, kullanıcı datagramının orijinal biçimini koruduğu ve kimlik doğrulamaya katılmamış sistemler tarafından okunup işlenebileceği anlamına gelir. Açıkçası, hiçbir gizlilik yoktur, ancak IPSec kimlik doğrulama işlevini desteklemek için İnternet altyapısını değiştirmeye de gerek yoktur. Doğrulamaya katılmayan sistemler hala normal olarak datagramları işleyebilir.

Kimlik Doğrulama Başlığı (AH), IP başlığından (IPv4) veya Hop-Hop Başlığından (IPv6) hemen sonra ve görüldüğü gibi gizlilik işleviyle kullanıldığında ESP başlığından hemen önce datagrama eklenir.

Başlık tipi, IANA atanan sayı 51'dir ve bir sonraki başlıkta veya önceki başlık yapısının protokol alanında tanımlanır. Bir kimlik doğrulama başlığında, şu anda dördü kullanımda olan beş adet parametre alanı vardır.

* Bir sonraki başlık alanı - bir sonraki başlık yapısında kullanılan IP protokolünü (IANA atanan numara) tanımlamak için kullanılır.
* Yük taşıma uzunluğu - kimlik doğrulama veri alanında bulunan 32 bit kelimelerin sayısı.
* Ayrılmış alan - gelecekteki genişleme için tasarlanmıştır. Bu alan şu anda sıfıra ayarlanmış
* SPI alanı - bu datagram için kullanılan güvenlik birliğini (SA) benzersiz şekilde tanımlayan değer.
* Doğrulama verileri alanı - bir sonraki 32 bit sınırına kadar doldurulmuş kriptografik dönüşümün verileri.

**3.4.Gizlilik İşlevi**

IPSec gizliliği, IP datagramları için güçlü bir bütünlük ve gizlilik sağlamak için anahtarlı şifreleme kullanır. Varsayılan algoritma, kimlik doğrulama veya reddetme sağlamayan ABD Veri Şifreleme Standardı'nın (DES CBC) Şifreleme Blok Zincirleme modunu kullanır. Kimlik doğrulamayı, onu destekleyen bir şifreleme dönüşümü kullanarak sağlamak mümkündür. Bununla birlikte, kimlik doğrulama veya reddetme gerektiren uygulamaların bu amaçla IP Kimlik Doğrulama Başlığını kullanmaları önerilir. IPSec gizlilik fonksiyonu, trafik analizi saldırılarına karşı koruma sağlamaz. İki çalışma modu vardır: tünel ve taşıma. Tünel modunda, orijinal IP datagramının tüm içeriği, güvenlik ilişkisinde (SA) belirtilen algoritma ve anahtar (lar) kullanılarak Encapsulation Security Payload (ESP) içinde saklanır. Bu SA'ya atanan Güvenlik Parametre Dizini (SPI) ile birlikte ortaya çıkan şifrelenmiş ESP, ikinci bir datagramın açık metin IP başlığına sahip bir veri yükü kısmı haline gelir. Bu açık metin başlığı genellikle, ana bilgisayardan ana bilgisayara aktarımlar için orijinal başlığın kopyasıdır, ancak güvenlik ağ geçitleri içeren uygulamalarda açık metin başlığı genellikle ağ geçidine yöneliktir, şifreli başlığın adres noktası ise bir iç alt ağdaki uç nokta ana bilgisayarıdır. Aktarım modunda, çerçevenin sadece aktarım katmanı (yani, TCP, UDP) kısmı ESP içine yerleştirilir, böylece IP başlığının açık metin bölümleri orijinal değerlerini korur. “Aktarım modu” terimi, TCP ve UDP protokolleriyle sınırlı bir kullanım anlamına gelse de, bu bir yanlış isimdir. Aktarım modu ESP, tüm IP istemci protokollerini destekler. Her iki mod için de işleme, çıktıda parçalanma öncesinde ve girdide tekrar bir araya getirme işleminden sonra gerçekleşir.

Kapsülleme Güvenlik Yükü (ESP) başlığı, IP Başlığından sonra ve taşıma katmanı protokolünden önce datagramın herhangi bir yerine yerleştirilebilir. Kimlik doğrulama işleviyle kullanıldığında, AH başlığından sonra görünmelidir (bkz. Ek 39.3). Başlık tipi IANA tarafından atanan numara 50'dir ve bir sonraki başlıkta veya önceki başlık yapısının protokol alanında tanımlanır. ESP başlığı üç alan içeriyor

* SPI alanı - bu datagramı işlemek için kullanılan SA için benzersiz tanımlayıcı. Bu tek zorunlu ESP alanıdır.
* Opak dönüşüm verileri alanı - bu SA tarafından kullanılan şifreleme dönüşümünü desteklemek için gereken ek parametreler (örneğin, bir başlangıç ​​vektörü). Bu alandaki veriler spesifik bir dönüşümdür ve bu nedenle uzunlukları değişir. Tek IPSec gereksinimi, alanın yastıklı olması, böylece 32-bit sınırda bitmesidir.
* Şifreli veri alanı - kriptografik dönüşümün verdiği veri.

ESP uyumluluğunu iddia eden IP sürüm 4 veya sürüm 6 sistemleri, DES CBC dönüşümünün kullanımını destekleyen Enkapsülasyon Güvenlik Protokolünü uygulamalıdır. Tüm ESP uygulamalarının diğer şifreleme algoritmalarını destekleme seçeneği vardır. Örneğin, gelen bir datagram için geçerli bir SA mevcut değilse (örneğin, alıcının anahtarı yoktur), alıcı şifreli ESP'yi atmalı ve arızayı bir sistem veya denetim günlüğüne kaydetmelidir. Kaydedilmesi önerilen değerler SPI değeri, tarih / saat, gönderen ve hedef adresleri ve akış kimliğidir. Günlük girişi, diğer uygulamaya özel verileri içerebilir. Alıcı sistemin, kullanımı kolay hizmet reddi saldırıları için güçlü bir potansiyel olması nedeniyle, gönderim sistemine arıza bildirimi göndermemesi önerilir. Şifrelenmiş verilerin ESP kullanan sistemler tarafından hesaplanması, işlem maliyetlerini ve iletişim gecikmesini artırır. Genel etki şifreleme algoritmasına ve uygulamaya bağlıdır. Gizli anahtar algoritmaları, genel anahtar algoritmalarından çok daha az işlem süresi gerektirir ve donanım tabanlı uygulamalar çok az sistem etkisiyle daha hızlı olma eğilimindedir. Kapsülleme Güvenlik Yükü fonksiyonu, bazı uluslararası ihracat ve kullanım kısıtlamalarını uygulamak ve bunlara tabi olmak için daha zordur, ancak esnek yapısı, VPN özellikleri ve güçlü gizliliği, güvenilmez ağlar arasında güvenli iletişim gerektiren işletmeler için idealdir.

**3.5.Anahtar Yönetimi**

Anahtar yönetimi işlevleri, güvenli iletişim kurmak için gereken şifreleme anahtarlarının oluşturulmasını, onaylanmasını ve dağıtımını içerir. İşlevler, destekledikleri kriptografik algoritmalara yakından bağlıdır, ancak genel olarak, üretim, anahtarları yaratan ve yaşam süreleri ve konumlarını yöneten işlevdir; kimlik doğrulama, anahtar hizmetleri talep eden ana bilgisayarları veya ağ geçitlerini doğrulamak için kullanılan işlemdir; ve dağıtım, anahtarları talep eden sistemlere güvenli bir şekilde aktaran işlemdir.

IP anahtarlamaya iki genel yaklaşım vardır: ana bilgisayar odaklı ve kullanıcı odaklı. Ana bilgisayar odaklı anahtarlar, tüm kullanıcıların uç nokta (yani ana bilgisayarlar ve ağ geçitleri) arasında veri aktarırken aynı anahtarı paylaşmasını sağlar. Kullanıcı odaklı anahtarlama, her bir kullanıcı oturumu için uç noktalar arasında veri aktaran ayrı bir anahtar oluşturur. Anahtarlar kullanıcılar veya uygulamalar arasında paylaşılmaz. Kullanıcıların Telnet ve FTP oturumları için farklı anahtarları vardır. Çok seviyeli güvenlik (MLS) sistemleri, farklı hassasiyet seviyeleri arasındaki gizliliği korumak için kullanıcı odaklı anahtarlama gerektirir. Ancak, MLS olmayan sistemlerde birbirine güvenmeyen kullanıcıların, grupların veya işlemlerin olması nadir değildir. Bu nedenle, IETF Güvenlik Çalışma Grubu, tüm IPSec anahtar yönetimi uygulamaları için kullanıcı odaklı anahtarlamanın kullanılmasını şiddetle tavsiye eder.

Şimdiye kadar sadece geleneksel şifreleme anahtar yönetiminden bahsettik. Bununla birlikte, geleneksel anahtar yönetimi işlevleri tam bir IPSec uygulamasını destekleyemez. IPSec’in dönüşüm bağımsızlığı, güvenlik birliğinin tüm öğelerinin, yalnızca şifreleme anahtarlarının değil, katılımcı uç noktalara dağıtılmasını gerektirir. Tüm güvenlik ilişkilendirme parametreleri olmadan, uç noktalar şifreleme anahtarının nasıl uygulandığını belirleyemez. Bu gereklilik, İnternet Güvenlik Birliği ve Anahtar Yönetimi Protokolü'nün (ISAKMP) geliştirilmesine yol açmıştır. ISAKMP standart anahtar yönetimi işlevlerini destekler ve güvenlik ilişkilerini ve özniteliklerini görüşmek, kurmak, değiştirmek ve silmek için mekanizmalar içerir. Bu bölümün geri kalanında, tüm SA yapısının (kriptografik anahtarlar dahil) yönetimine ve bir anahtarın yalnızca kriptografik anahtar parametrelerine atıfta bulunmak için anahtar yönetimine değinmek için “SA yönetimi” terimini kullanacağız. Kilit yönetimin SA yönetiminden ayrı olarak yapılabileceğini not etmek önemlidir. Örneğin, ana bilgisayar odaklı anahtarlama, hem oturum parametrelerini hem de kriptografik anahtarları oluşturmak için SA yönetimini kullanırken, kullanıcı odaklı anahtarlama, ilk oturum parametrelerini oluşturmak için SA yönetim işlevini ve bireysel kullanım oturum anahtarlarını sağlamak için anahtar yönetim işlevini kullanır. .

SA veya anahtar yönetiminin en basit şekli manuel yönetimdir. Sistem güvenliği yöneticisi kendi sistemleri ve iletişim kurdukları sistemler için SA parametrelerini ve şifreleme anahtarlarını manuel olarak girer. IPSec'in tüm IPv4 ve IPv6 uygulamaları, güvenlik ilişkilerinin ve anahtarların el ile yapılandırılmasını desteklemek için gereklidir. Manuel konfigürasyon küçük, statik ortamlarda iyi çalışır ancak daha büyük ortamlara, özellikle de birden fazla idari alan içerenlere ölçeklendirmek için çok zor. Bu ortamlarda, SA ve kilit yönetim fonksiyonları etkin olması için otomatikleştirilmeli ve merkezileştirilmelidir. Bu, ISAKMP'nin sağlamak için tasarlandığı bir işlevdir.

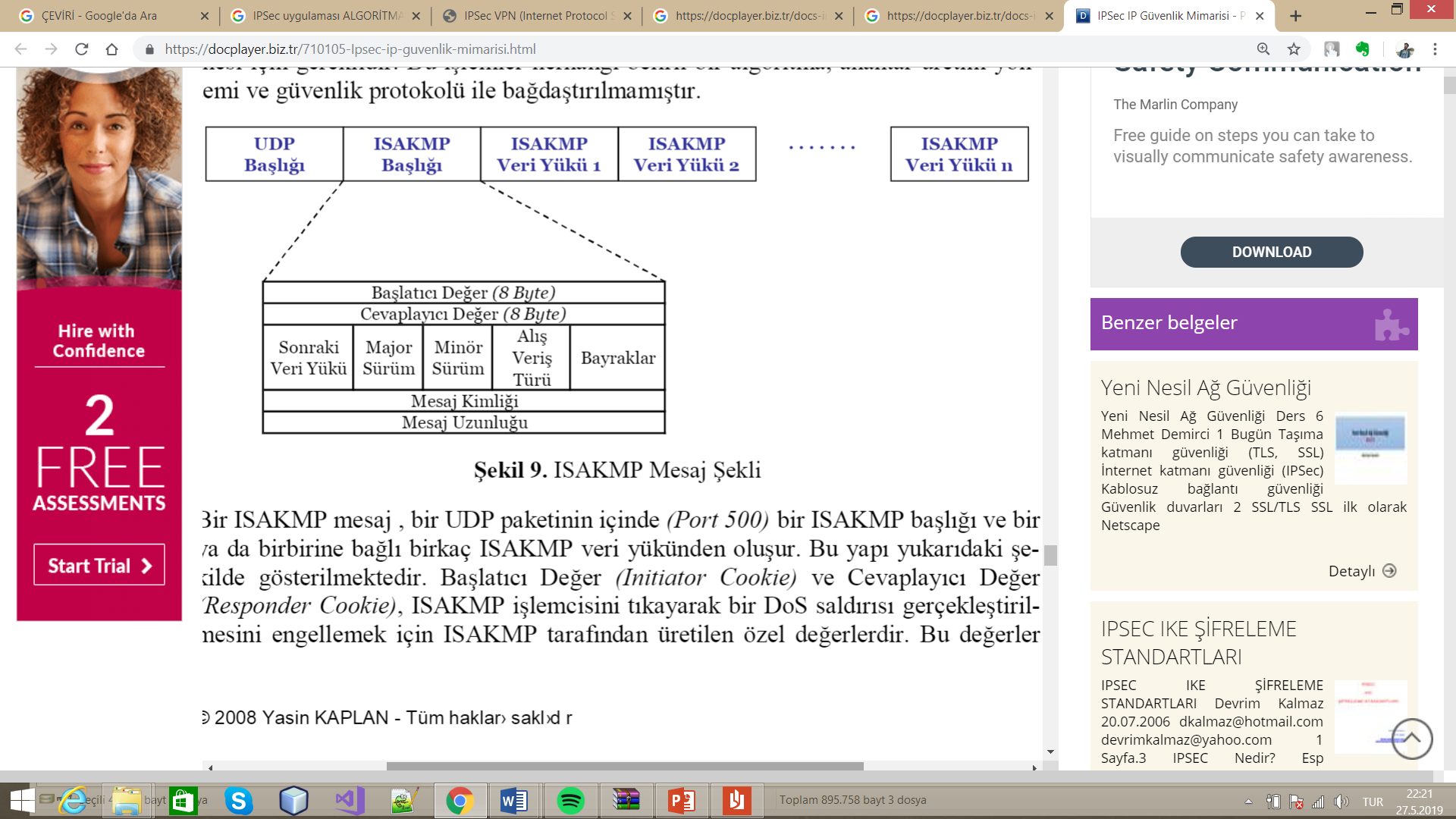
**3.6.İnternet Güvenliği Birliği ve Anahtar Yönetimi Protokolü (ISAKMP)**

ISAKMP, güvenlik ilişkilerini ve şifreleme anahtarlarını dağıtmak için standart, esnek ve ölçeklenebilir bir metodoloji sunmaktadır. Protokol, iletişim kuranın kimliğini doğrulamak, güvenlik birlikleri oluşturmak ve yönetmek, anahtarlar ve güvenlik birlikleri oluşturmak ve yönetmek için kullanılan teknikler ve tekrarlama ve hizmet reddi saldırıları gibi tehditleri hafifletme yöntemlerini tanımlar. ISAKMP, IPSec AH ve ESP servislerini destekleyecek şekilde tasarlanmıştır, ancak bunun ötesine geçer.

ISAKMP, çeşitli güvenlik mekanizmaları için nakliye ve uygulama katmanlarında güvenlik hizmetlerini destekleme kabiliyetine sahiptir. Bu mümkündür, çünkü ISAKMP güvenlik birliği yönetimi fonksiyonunu anahtar değişim mekanizmasından ayırır. ISAKMP, anahtar değişim protokolünün bağımsızlığına sahiptir. Birbirine benzemeyen sistemler arasında SA'ları pazarlamak, değiştirmek, değiştirmek ve silmek için ortak bir çerçeve sağlar. ISAKMP ile güvenlik birliklerinin yönetimini merkezileştirmek, her güvenlik protokolündeki çoğaltılan işlevlerin çoğunu azaltır ve bağlantı kurulum süresini önemli ölçüde azaltır çünkü ISAKMP bir seferde tüm hizmetleri pazarlık edebilir.

ISAKMP'nin ayrıntılı bir tartışması bu bölümün kapsamı dışındadır, bu nedenle yalnızca bir güvenlik birliğinin ve kilit yönetim sisteminin operasyonları ve işlevsel gereksinimleri ele alınacaktır. Bir güvenlik birliği ve anahtar yönetim sistemi, güvenli bağlantılar kuran sistemler arasında aracılık eden bir hizmet uygulamasıdır. Bu sistemler arasında veri transferine aktif olarak katılmamaktadır. Yalnızca gerekli güvenlik ilişkilerini ve şifreleme anahtarlarını üreterek, doğrulayarak ve dağıtarak güvenli bir bağlantı kurulmasına yardımcı olur.

Sistemin düzgün çalışması için iki parametre üzerinde anlaşmaya varılmalıdır. İlk olarak, uç nokta sistemleri ve SA yöneticisi arasında bir güven ilişkisi kurulmalıdır. SA yöneticisi, bir Kerberos Anahtar Dağıtım Merkezi'ne (KDC) benzeyen veya uç noktadaki IPSec uygulamasına entegre olan üçüncü taraf bir sistem olabilir. Her yaklaşım, her yönetici ve iletişim kurduğu bitiş noktaları için el ile yapılandırılmış bir SA gerektirir. Bunun avantajı, bu birkaç manuel SA'nın çok sayıda güvenli bağlantı kurmak için kullanılabiliyor olmasıdır. Çoğu satıcı, ISAKMP'yi uç nokta sistemlerine entegre etmeyi ve başlangıçtaki güven ilişkisini doğrulamak için üçüncü taraf (örneğin, belirli bir Otorite) sistemini kullanmayı seçti. İkinci şart, bitiş noktalarının ortak bir güvenilen üçüncü tarafa sahip olmalarıdır. Başka bir deyişle, her iki uç noktanın da her ikisine de güvendiği bir SA yönetim sistemine veya belirli bir Otorite'ye sahip olması gerekir.



**Şekil 1:ISAKMP Mesaj Şekli**

Operasyon oldukça basit. Bu senaryo için entegre SA'lara sahip sistemleri kullanacağız. Sistem A, Sistem B ile güvenli bir iletişim oturumu kurmak istiyor ve aralarında geçerli bir güvenlik birliği yok. Sistem A, Sistem B'deki SA yönetim işleviyle bağlantı kurar. İşlem B, Sistem A'ya güvenli bir dönüş yolu belirlediğinden, işlem kendini tersine çevirir (SA'ların yalnızca bir yönde oluşturulduğunu unutmayın). ISAKMP, bir çift yönlü SA'ları müzakere etme yeteneğine sahiptir. tek bir işlem, bu nedenle ayrı bir dönüş yolu anlaşması genellikle gerekli değildir.

ISAKMP dört ana işlevsel bileşene sahiptir. Onlar:

1. İletişim meslektaşlarının kimlik doğrulaması

2. Şifreleme anahtarı oluşturulması ve yönetimi

3. Güvenlik birliği oluşturma ve yönetimi

4. Tehdit azaltma

İletişimin diğer ucunda varlığın kimliğini doğrulamak, güvenli bir iletişim oturumu kurmanın ilk adımıdır. Kimlik doğrulama olmadan, bir işletmenin kimliğine güvenmek mümkün değildir ve geçerli bir ID erişim kontrolü olmadan anlamsızdır. İzinsiz bir sistemle iletişimi güvenceye almak için ne değer var? ISAKMP, tüm ISAKMP değişimleri için güçlü bir kimlik doğrulama oluşturmak için ortak anahtar dijital imzaların kullanılmasını zorunlu kılar (örneğin, DSS, RSA). Standart belirli bir algoritma belirtmez. Genel anahtar şifrelemesi, paylaşılan sırları ve oturum anahtarlarını dağıtmanın çok etkili, esnek ve ölçeklenebilir bir yoludur. Ancak, tamamen etkili olması için, açık anahtarların belirli bir işletmeye bağlanmasının bir yolu olmalıdır. Daha büyük uygulamalarda, bu işlev bir Sertifika Yetkilisi (CA) gibi güvenilir bir üçüncü taraf (TTP) tarafından sağlanır. Küçük uygulamalar manuel olarak yapılandırılmış tuşları kullanmayı seçebilir. ISAKMP, güvenilir üçüncü şahıslarla iletişim kurmak için kullanılan protokolleri tanımlamaz.

Anahtar teslimi, rastgele anahtarların oluşturulmasını ve bu anahtarların katılımcı kuruluşlara taşınmasını kapsar. Bir RSA açık anahtar sisteminde, anahtar aktarımı, oturum anahtarını alıcının açık anahtarıyla şifreleyerek gerçekleştirilir. Şifreli oturum anahtarı daha sonra, özel anahtarla şifresini çözen alıcı sistemine gönderilir. Dif Hell e – Hellman sisteminde, alıcının genel anahtarı, paylaşılan bir gizli anahtar oluşturmak için gönderenin özel anahtar bilgileriyle birleştirilir. Bu anahtar, oturum anahtarı olarak veya rastgele oluşturulmuş ikinci bir oturum anahtarının taşınması için kullanılabilir. ISAKMP kapsamında bu anahtar değişimlerinin güçlü kimlik doğrulaması kullanılarak yapılması gerekir. ISAKMP belirli bir anahtar değişim protokolü belirtmemektedir, ancak Oakley’nin standart olacağı anlaşılmaktadır. Güvenlik birliği oluşturma ve yönetme, bağlantı görüşmesinin iki aşamasına yayılmıştır. İlk aşama, iki uç nokta SA yöneticisi arasında bir güvenlik ilişkisi kurar. İkinci aşama, o oturum için seçilen güvenlik protokolleri için güvenlik ilişkilerini kurar. Birinci aşama, yöneticiler ve bitiş noktaları arasındaki güveni oluşturur; ikinci aşama, iki son nokta arasındaki güvendir. İkinci aşama tamamlandığında, SA yöneticisinin bağlantıya başka bir katkısı yoktur.

ISAKMP, hizmet reddi, kaçırma ve themine man saldırıları gibi tehditlerle mücadele mekanizmalarını bütünleştirir. Yönetici servisi, CPU-yoğun herhangi bir işlem yapmadan önce talep eden sisteme tıkanma önleyici bir simge (çerez) gönderir. Yönetici bu tanımlama bilgisine bir cevap alamazsa, isteğin geçersiz olduğunu ve reddettiğini varsayar. Bu kesinlikle kapsamlı bir tıkanma önleme koruması olmasa da, en yaygın baskın saldırılara karşı oldukça etkilidir. Tıkanmayı önleyici mekanizma, yeniden yönlendirme saldırılarını tespit etmek için de kullanışlıdır. Her oturum kurulumu sırasında birden fazla çerez gönderildiği için, veri akışını farklı bir uç noktaya yönlendirmeye yönelik herhangi bir girişim algılanır. ISAKMP, kimlik doğrulama işlemini ve SA / anahtar değiştirme işlemini tek bir veri akışına bağlar. Bu, veri akışının engellenmesine veya değiştirilmesine dayanan saldırıları (örneğin, kaçırma, them-iniddle) tamamen etkisiz hale getirir. Veri akışındaki herhangi bir kesinti veya değişiklik yönetici tarafından algılanacak ve işlem devam edecektir. ISAKMP ayrıca veri silme işlemlerini tespit etmek için dahili bir durum makinesi kullanır, böylece kısmi değiş tokuşlara dayalı SA'ların kurulmamasını sağlar. Son bir anti-tehdit olarak, ISAKMP tüm anormal işlemler için günlük kaydı ve bildirim gereklilikleri belirtmekte ve on-line hata bildiriminin kullanımını sınırlamaktadır.

**BULGULAR**

Güvenlik İlişkilendirmesi (Security Associattion, SA)kavram , IP güvenlik mimari-sinin temelidir. Bir SA, paketleri kimin gönderdiği, paketlerin nereye gittiği ve yük

olarak ne taşındığı hakkında veri paketlerine uygulanması gereken güvenlik tedbirle-

rini tan mlar. Bir SA taraf ndan sunulan güvenlik hizmetleri kümesi, güvenlik proto-

kolüne, bu protokolün seçeneklerine ve SA’nın hangi çalışma şeklinde işletildiğine

dayanIr. SA’lar için, güvenlik yöneticisi taraf ndan verilen güvenlik politikalarna dayalı olarak, IPSec’in bir ya da daha fazla güvenlik hizmeti kullanılacağı zaman,

haberleşen uçlar arasında dinamik uzlaşı gerçekleştirilebilir. Başka bir yaklaşım,

nadir olarak kullanılsa da, SA’lar statik olarak tanImlanmasıdır.

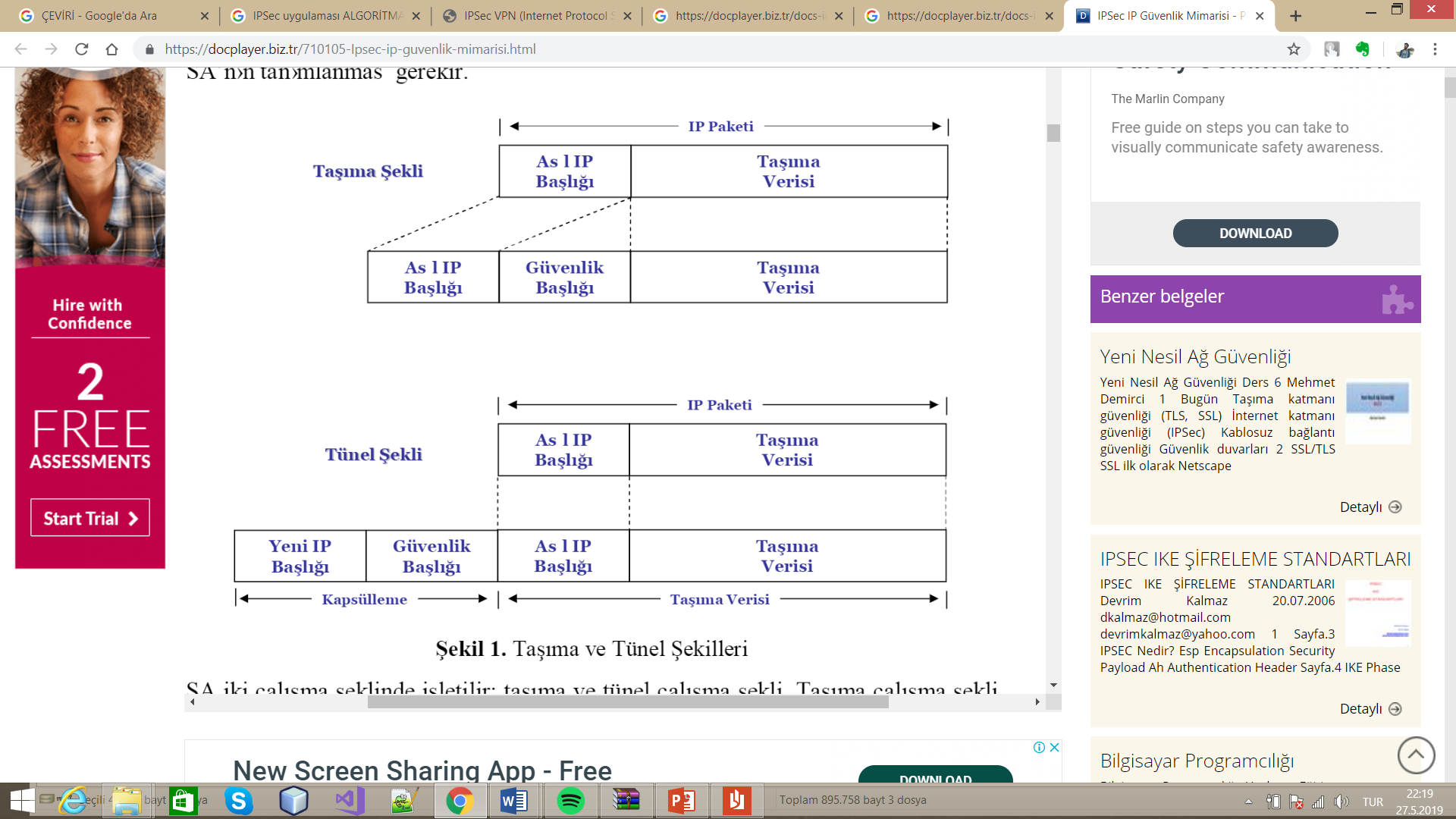
Kaynak IP adresinin SA’yı tanımlamak için kullanılmadığına dikkat edilmelidir. Bu,

SA’n n, iki uç veya geçit arasında tek bir yönde veri iletimi için yapılmış bir hizmet

anlaşması olmasından kaynaklanır. Bunun sonucu olarak eğer iki uç arasında IPSec

kullanılarak iki yönlü veri iletimi gerçekleştirilecekse, her biri bir yön için, iki adet

SA’nın tanımlanması gerekir.



**Şekil 2.Taşıma ve Tünel Şekilleri**

SA iki çalışma şeklinde işletilir; taşıma ve tünel çalışma şekli. Taşıma çalışma şekli

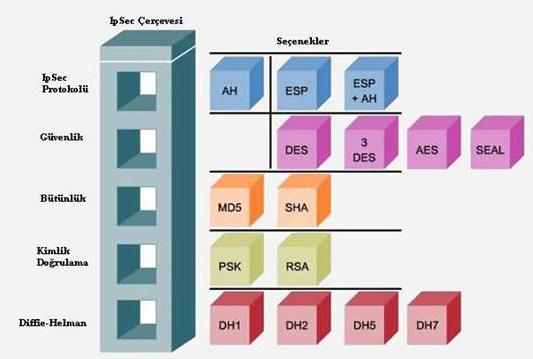
birincil olarak üst katman (TCP ve UDP gibi) protokollerinin korunmas için tasarlanmıştır. Tünel çalışma şeklinde ise bir IP paketi başka bir IP paketinin taşıma verisi olmaktadır. Bu yöntemde içerdeki IP paketi, başlığı ile birlikte kriptolanmakta, dış başlık ise bu kriptolanmış paketin ağ üzerinde, yönlendirilmiş olduğu ağa ulaştırıl-masını sağlamaktadır. Uçlar hem taşıma ve hem detünel çalışma şekillerinde işlenilebilirken, güvenlik geçitleri sadece tünel çalışma şeklindeyapılandırılabilirler (*Geçit uç rolünü üstlendiğinde her iki çalışma şeklini de destekleyebilir*)

**IPSec Çatısı Altında Kullanılan Şifreleme Algoritmaları**

“Güçlü” olarak tanımlanan birçok şifreleme algoritması mevcuttur fakat IPSec çatısı altında kullanılmak üzere bunlardan sadece birkaçı resmen deklare edilmiştir:

* DES,
* Digital Encryption Standard,
* 3DES,
* Triple-pass DES

IPSec uygulaması aşağıda örnekleri verilen diğer bilinen şifreleme algoritmalarını da kullanmaktadır.



**Şekil 3:IpSec te kullanılan Algoritmalar**

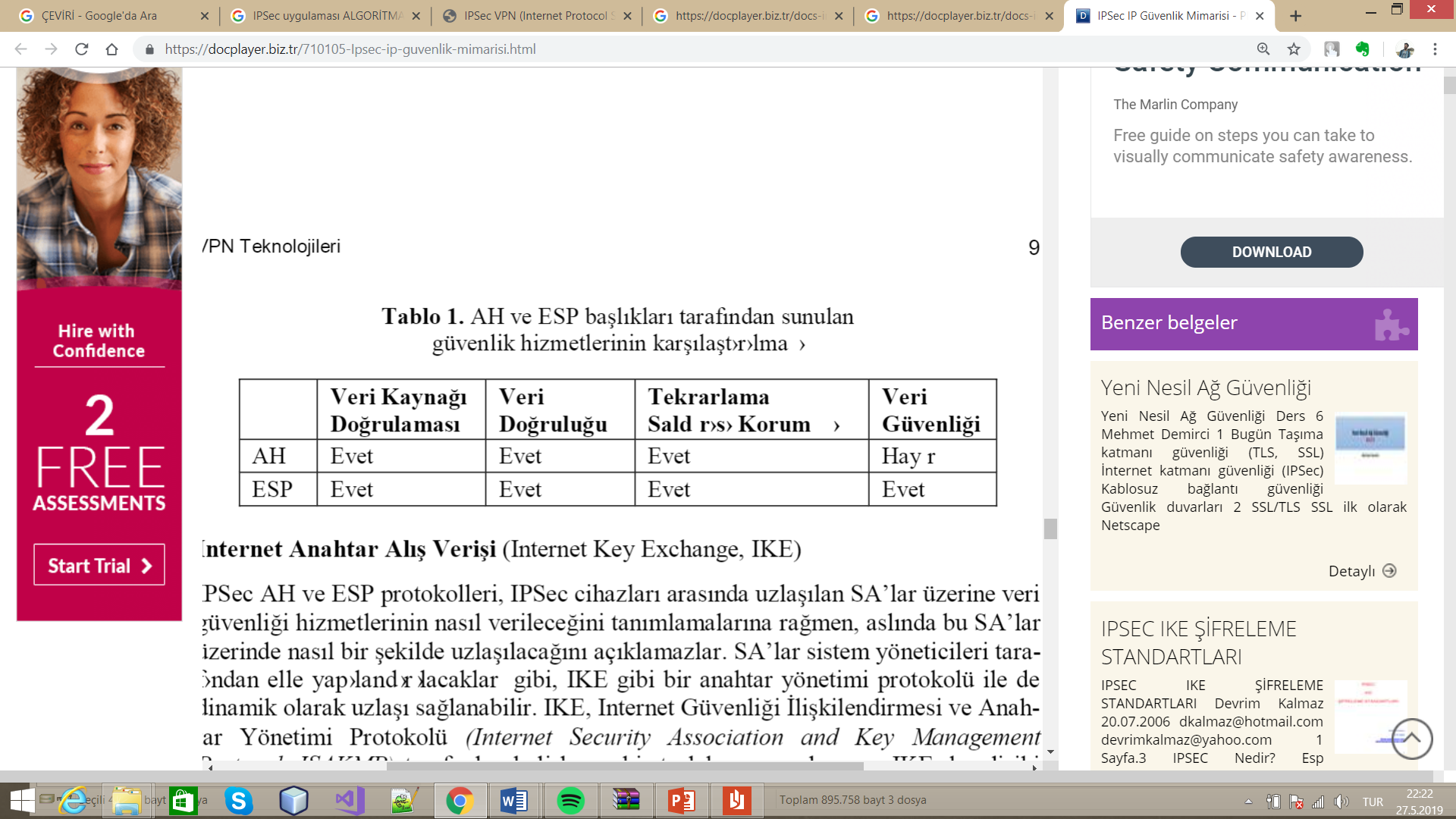
**Asimetrik Şifreler:**

* RSAEl
* Gamal
* DSA
* DiffieHellman

**Simetrik Şifreler:**

* DES (56 bits)
* 3DES (168 bits in theory)
* Blowfish ( bits)
* CAST-12
* (128 bits)
* AES ( bits)

Simetrik şifreler hızlı olduklarından Ipsec tarafından **en fazla** kullanılanlardır.



Farkı:AH protokolünden farkı; ESP IP paketinin şifrelenmesini sağlamaktadır.

**Özet**

Standart olarak, IPSec hızla TCP / IP ağlarında güvenli iletişim için tercih edilen yöntem haline geliyor. Birden fazla şifreleme ve kimlik doğrulama şemasını ve çok satıcılı birlikte çalışabilirliği desteklemek üzere tasarlanan IPSec, hem büyük hem de küçük kuruluşların güvenlik gereksinimlerine uyarlanabilir. İş ortaklarıyla iletişim kurmak için extranet teknolojilerine dayanan endüstriler, IPSec’in esnek şifreleme ve kimlik doğrulama şemalarından faydalanacaktır; büyük işletmeler IPSec’in ölçeklenebilirliğinden ve merkezi yönetiminden faydalanacaktır; ve her şirket, mobil çalışanlara, telekomünikasyon şirketlerine veya şirket kaynaklarına Internet üzerinden erişen şirket şubelerine destek vermek için IPSec’in sanal özel ağ (VPN) yeteneklerinden faydalanabilir. İnternet Güvenlik Protokolü Mimarisi geleceği düşünülerek tasarlandı ve güvenlik ve bilgisayar topluluklarından hakettiği desteği alıyor. Otomotiv Endüstrisi Eylem Grubu gibi büyük imalatçı dernekleri, Cisco Systems gibi büyük tedarikçilerin ürün taahhütlerinin yanı sıra Uluslararası Bilgisayar Güvenliği Birliği aracılığıyla bir uyumluluk sertifikası programının oluşturulması ile ilgili son onaylar, IPSec'in yolunda olduğunun iyi bir işaretidir. 21. yüzyılda işletmeler arası iletişim için endüstri standardı.

Adı :Halil Durmuş

Numara:150757017

Bölüm :Bilgisayar Mühendisliği(İ.Ö)

**Bölüm 2.2.13: Kablosuz İnternet Güvenliği**

**İçindekiler Sayfa**

1. **Giriş 15**
2. **Kablosuz İnternet Kimdir? 15-16**
3. **Uygulama Türleri Nelerdir? 16-17**
4. **Güvenli İletim Yöntemleri Nasıl 17-18**
   1. **Frekans Bölmeli Çoklu Erişim (FDMA)**

**Teknolojisi 18**

* 1. **Zaman Bölmeli Çoklu Erişim (TDMA) Teknolojisi 18-19**
  2. **Mobil İletişim için Global Sistemler (GSM) 19-20**
  3. **Kod Bölmeli Çoklu Erişim (CDMA) Teknolojisi 20-21**
  4. **Diğer Yöntemler 21**

1. **Güvenli Kablosuz Cihazlar Nasıl? 22**
   1. **Doğrulama 22-23**
   2. [**Gizlilik**](https://tureng.com/tr/turkce-ingilizce/gizlilik) **23**
   3. **Kötü Amaçlı Kod ve Virüsler 23-24**
2. **Güvenli Ağ Altyapı Bileşenleri Nasıl? 24**
   1. **“WAP'taki Boşluk” 24-25**
   2. **WAP Ağ Geçidi Mimarileri 25**
      1. **Servis Sağlayıcıdaki WAP Ağ Geçidi 25-26**
      2. **Ana Bilgisayardaki WAP Ağ Geçidi 26-27**
      3. **Servis Sağlayıcı’nın WAP Ağ**

**Geçidinden Host’un WAP Proxy'sine Geçiş 28-29**

**7.Sonuç 29-30**

**Kaynakça 30**

**1.Giriş**

O zamanlar ticaret ve güvenlik, gündemde yüksek değildi (ağın kullanılabilirliğini korumak hariç). İnterneti ilk günlerde ticarileştirme düşüncesi neredeyse hiç duyulmamıştı. Aslında, İnternet'in ürün ve hizmet satmak için kullanılması uygunsuz görüldü. Ticari faaliyetler ve güvenlik ihtiyaçları, son birkaç yılda güçlü bir şekilde ortaya çıkan İnternet üzerinde daha yeni bir gelişmedir.

Bugün, aksine, kablosuz İnternet, ticaretin başından beri itici güç olarak tasarlanıyor. Dünyanın dört bir yanındaki milletler ve kuruluşlar, çizim işi umudunda altyapı, iletim sıklıkları, teknoloji ve uygulamaları satın almak için milyonlarca hatta milyarlarca dolar harcıyor. Bazı açılardan bu, yeni binyılın “toprak acelesi” haline geldi. O zaman, güvenliğin de erken dönemde kritik bir rol oynaması gerektiği anlamına gelir - paranın el değiştirdiği yerlerde, güvenlik bu aktiviteye eşlik etmelidir.

Kablosuz endüstrisi henüz başlangıç ​​aşamasında olsa da, kablosuz İnternet için cihazlar, altyapı ve uygulama geliştirme dünya çapında hızla artmaktadır. Öngörüsü olanlar, güvenliğin bu tasarımların başlarında yapmaması gerektiğini bileceklerdir. Bu bölümün amacı, gelişmekte olan bu sektörde ele alınması gereken önemli güvenlik sorunlarından bazılarını vurgulamaktır. Bunlar, kablosuz bir İnternet servisini veya uygulamasını dağıtmak isteyen herhangi bir işletmenin, kendi işletmelerini ve müşterilerini korumak ve bu yeni sınırdaki yatırımlarını korumak için göz önünde bulundurmaları gerekeceği konusundaki endişeler.

Bu arada, bu bölümün odağında dizüstü bilgisayarlar ve kablosuz modemler kullanarak İnternete erişmekle ilgili değil. Uzun yıllardır var olan bu teknoloji, çoğu durumda, geleneksel kablolu İnternet erişiminin bir uzantısıdır. Bu bölüm de mutlaka İnternet tabanlı olmayan, ancak bölümleri kendi başlarına hak eden kablosuz LAN ve Bluetooth konularına odaklanmayacak. Aksine, konsantrasyon doğal olarak cep telefonları ve PDA'lar (kişisel dijital asistanlar) gibi normal bilgisayarlardan çok daha az bilgi işlem kaynağına sahip taşınabilir İnternet cihazlarındadır. Bu nedenle, bu aygıtlar, farklı teknolojilerle başa çıkmak için farklı programlama dilleri, protokoller, şifreleme yöntemleri ve güvenlik perspektifleri gerektirir. Bununla birlikte, küçük boyutlarına ve sınırlamalarına rağmen, bu cihazların, özellikle kendileri için tasarlanan elektronik ticaret ve intranetle ilgili uygulamalar nedeniyle bilgi güvenliği üzerinde önemli bir etkiye sahip olduğunu belirtmek önemlidir.

**METERYAL VE YÖNTEM**

**2.Kablosuz İnternet Kimdir?**

Günümüzde, kablosuz İnternet kullanıcılarının sayısının yakında milyonlarca kablolu İnternet kullanıcısını geçeceğini gösteren birçok çalışma ve tahmin bulunmaktadır. Varsayım, zaten dışarıda olan milyonlarca dünya çapında cep telefonu kullanıcısına, her gün binlerce insanın kattığı bir popülasyona dayanıyor. Bu mobil kullanıcıların her biri internete cep telefonları üzerinden erişmeyi seçerse, bu nüfus gerçekten de kablolu internet kullanıcılarının sayısını birkaç kez kolayca aşabilir. Bu çok büyük bir potansiyel, bu büyümekte olan sanayiye yatırım yapma ümidiyle önemli kaynaklar ve yatırımlar tahsis eden birçok işletmeye sahip.

Kablosuz İnternet hala çok genç. Birçok cep telefonu kullanıcısı henüz cep telefonlarından internete erişemiyor. Çoğu, hangi hizmetlerin sağlanacağını görmek için “bekle ve gör” tavrı alıyor. Kablosuz İnternet erişimi olan çoğu kişi, bu hizmetin sağlayabileceği potansiyeli deneyen ilk uygulayıcılar. Kablosuz cihazlardaki ciddi sınırlamalar nedeniyle - küçük ekranlar, son derece sınırlı bant genişliği ve diğer sorunlar - hem kablolu hem de kablosuz Internet erişimine sahip çoğu kullanıcı, bugün için kablosuz cihazların masaüstünün yerini almayacağını itiraf edecek İnternete ulaşmanın birincil yolu olarak bilgisayarları ve dizüstü bilgisayarları her zaman. Birçoğu, bugün kablosuz bir cihaz kullanarak “interneti taramanın” hayal kırıklığı yaratan bir egzersiz olabileceğini itiraf ediyor. Bu kablosuz İnternet kullanıcılarının çoğu, aşağıdaki sıkıntıları dile getirdi:

* İnternete bağlanmak için çok yavaş .
* Hareket halindeyken, mobil kullanıcıların oturumun ortasında bağlantısı kesilebilir. Sayısal tuş takımı kullanarak cümleleri yazmak zahmetlidir.
* Kablosuz interneti, özellikle dakika başına faturalandırıldığında kullanmak pahalıdır.
* Kablosuz cihazlarda çok az veya hiç grafik görüntüleme özelliği yoktur.
* Ekranlar çok küçük ve kullanıcıların uzun bir mesajı okumak için sürekli kaydırma yapması gerekiyor.
* Web siteleriyle ilgili sık karşılaşılan hatalar var (temel olarak günümüzde çoğu Web sitesi henüz kablosuz İnternet uyumlu değil).

**3.Uygulama Türleri Nelerdir?**

Günümüzün kablosuz teknolojisinin sıkıntılarını ve sınırlamalarını tanıyan birçok işletme, kablosuz cihazlarını ve hizmetlerini, kablolu İnternet erişimi için zorunlu olarak değil, kablolu İnternet'in sağlayabileceklerini genişleten özel hizmetler olarak tasarlıyor. Bu hizmetlerin çoğu, bir bilgisayarın önünde oturmak zorunda kalmadan, her zaman ve her yerde taşınabilir bilgi erişiminin çekici kolaylığını vurgulamaktadır - temel olarak, birinin cebinde taşıyabileceği Internet hizmetleri. Açıkçası, bilginin özlü, taşınabilir, kullanışlı ve erişimi kolay olması gerekir. Günümüzde mevcut olan veya tasarlanan mobil servis örnekleri şunları içerir:

* Bir cep telefonu kullanarak çevrimiçi alışveriş yapmak; gerçek bir mağazanın içindeyken çevrimiçi fiyatları mağaza fiyatları ile karşılaştırma
* Mevcut hisse senedi fiyatları, alım satım fiyatı uyarıları, ticari anlaşma ve portföy bilgilerini her yerde almak
* Banka işlemlerini yapmak ve hesap bilgilerini edinmek
* Seyahat programları almak ve rezervasyon rezervasyonları
* Kişiselleştirilmiş haberler ve hava durumu tahminlerini edinmek • En son piyango numaralarını almak
* Ekspres paketler için mevcut teslimat durumunu elde etmek
* “Hareket halindeyken” e-posta okuma ve yazma • envanter, müşteri listeleri vb. Gibi şirket içi veritabanlarına erişim.
* Harita yol tarifi alma • Kullanıcının bulunduğu yere göre en yakın ATM makinelerini, restoranları, tiyatroları ve mağazaları bulmak
* 911'i aramak ve acil durum servisini hızlı bir şekilde arayanın yerini belirlemek
* Bir Web sitesine göz atmak ve aynı oturum içinde sitenin temsilcisi ile canlı konuşmak.

Yeni ve daha yenilikçi hizmetler işlerinde. Yeni ve gelişmekte olan herhangi bir teknoloji olarak, kablosuz hizmetler ve uygulamalar genellikle pek çok umut ve yutturmaca ile birlikte bazı sağlıklı şüpheciliklerle çevrilidir. Ancak teknoloji ve hizmetler zamanla olgunlaştıkça, dünkü deneyler yarının standartları olabilir. İnternet bu gelişen ilerlemenin büyük bir örneğidir. Kablosuz İnternet'in geliştirilmesi, muhtemelen daha da hızlı olmasına rağmen, muhtemelen aynı evrimsel döngüden geçecektir.

Bununla birlikte, herhangi bir yeni teknoloji gibi, güvenlik ve güvenlik sorunları da itibarına zarar verebilir ve en baştan tasarıma akıllıca dahil edilmemesi durumunda yararlanabilir. Bu amaçla yazıldığından bu amaç göz önünde bulundurulur.

Kablosuz İnternet çok fazla alanı kapladığından, aynı güvenlik için de geçerli. Bu bölüm, birkaç seçili kategoride kablosuz İnternet ile ilgili güvenlik sorunlarını tartışıyor, kablosuz cihazlara iletim yöntemleriyle başlıyor ve bazı altyapı bileşenlerinin kendileri ile bitiyor.

**4.Güvenli İletim Yöntemleri Nasıl**

Uzun yıllar boyunca, analog cep telefonu iletimlerinin kesişmesi oldukça kolaydı. Analog cep telefonları mevcut olduğu sürece bilinen bir problem olmuştur. Özel radyo tarama cihazları kullanarak kolayca yakalanabilirler. Bu sebeple, pek çok diğerinde olduğu gibi, birçok cep telefonu servis sağlayıcısı, abonelerine dijital servisleri tanıtmakta ve eski bir servise benzetmeyi azaltmaktadır.

Öte yandan, dijital cep telefonu yayınları, müdahale etmek için genellikle daha zorludur. Bu, aynı kablosuz yayınlarda, yeni kablosuz İnternet servislerinin çoğunun dayandığı bir sistem.

Bununla birlikte, dijital hücresel iletim için tek bir yöntem yoktur. Aslında, kablosuz iletim için bugün mevcut birkaç farklı yöntem vardır. Örneğin, Amerika Birleşik Devletleri'nde Verizon ve Sprint gibi sağlayıcılar öncelikle CDMA (Kod Bölmeli Çoklu Erişim) kullanır, AT&T öncelikle TDMA (Zaman Bölmeli Çoklu Erişim) kullanır ve Voicestream GSM (Mobil İletişim için Global Sistemler) kullanır. Cingular gibi diğer sağlayıcılar, coğrafi konuma bağlı olarak birden fazla yöntem (TDMA ve GSM) sunar. Tüm bu yöntemler, radyo frekanslarını kullanma şekilleri ve kullanıcıları bu frekanslara ayırma şekilleri bakımından farklılık gösterir. Bu bölüm bunların her birini daha ayrıntılı olarak ele almaktadır.

Cep telefonu kullanıcıları, genellikle kablosuz Internet erişimi istiyorlarsa, gerçekten de umursamıyorlarsa, belirli bir iletim yöntemini seçmekle ilgilenmiyorlar. Bunun yerine, çoğu kullanıcı servise kaydolduklarında favori kablosuz servis sağlayıcılarını seçer. Sağlayıcılarının hangi aktarım yöntemini kullandığı genellikle kullanıcıya karşı şeffaftır. Bununla birlikte, servis sağlayıcı için tamamen farklı bir konudur. Hangi yöntemi uygularlarsa uygulayın, altyapısı üzerinde önemli bir etkisi var. Örneğin, kullandıkları telsiz teçhizatı türü, konuşlandırılacak iletim kulelerinin yeri ve sayısı, kullanabilecekleri trafik miktarı ve abonelerine satacağı cep telefonu türleri, seçilen dijital iletim yöntemiyle doğrudan ilişkilidir. .

**4.1.Frekans Bölmeli Çoklu Erişim (FDMA) Teknolojisi**

Analog veya dijital tüm hücresel iletişim, kablosuz servis sağlayıcı tarafından satın alınan veya tahsis edilen radyo frekansları kullanılarak iletilir. Her servis sağlayıcı tipik olarak bir radyo frekansı spektrumunu çalıştırmak için ilgili hükümetten lisans satın alır.

Analog hücresel iletişim tipik olarak, Frekans Bölmeli Çoklu Erişim (veya FDMA) teknolojisi olarak adlandırılan şey üzerinde çalışır. FDMA ile her servis sağlayıcı, radyo frekansı spektrumunu ayrı frekans kanallarına böler. Her kanal, tek yönlü bir iletişim oturumunu destekleyen belirli bir frekanstır; ve her kanal 10 ila 30 kilohertz (kHz) genişliğe sahiptir. Düzenli bir iki yönlü telefon görüşmesi için, her cep telefonu arayanına iki frekans kanalı atanır: biri gönderilecek, diğeri alacak.

Her telefon görüşmesi iki kanalı kapladığından (iki frekans), özel radyo tarama ekipmanı, ekipman doğru frekans kanalına ayarlandıktan sonra canlı bir analog telefon görüşmesine dokunmak için çok zor değildir. Şifreleme eklenmezse, analog hücresel iletişimde çok az gizlilik koruması vardır.

**4.2.Zaman Bölmeli Çoklu Erişim (TDMA) Teknolojisi**

Dijital hücresel sinyaller ise çoğu analog radyo frekans taramasına dirençli olan çeşitli kodlama teknikleriyle çalışabilir. (Kablosuz iletişimde "kodlama" kelimesinin şifreleme anlamına gelmediğine dikkat edin. Burada "Kodlama" genellikle bir sinyalin bir formattan diğerine, örneğin kablolu bir sinyalden kablosuz sinyale dönüştürülmesi anlamına gelir.)

Bu tekniklerden birine zaman bölmeli çoklu erişim veya TDMA denir. FDMA'ya benzer şekilde, TDMA tipik olarak radyo spektrumunu çoklu 30 kHz frekans kanallarına (bazen frekans taşıyıcıları denir) ayırır. Her iki yönlü iletişim, bu frekans kanallarından ikisini gerektirir: biri göndermek diğeri almak için. Ancak, TDMA ayrıca, her bir frekans kanalını ses / veri kanalı adı verilen üç ila altı zaman dilimine böler, böylece şimdi altı taneye kadar dijital ses veya veri oturumu aynı frekans kullanılarak gerçekleştirilebilir. TDMA ile bir servis sağlayıcı aynı anda FDMA'ya göre daha fazla çağrı yapabilir. Bu, altı seansın her birine aynı frekans içinde belirli bir zaman dilimi atamak suretiyle gerçekleştirilir. Her zaman dilimi (veya ses / veri kanalı) süresi yaklaşık yedi milisaniyedir. Zaman dilimleri hızlı dönüşlerde tekrar tekrar düzenlenir ve iletilir. Her arayan için ses veya veriler, arayan kişiye atanan zaman dilimine yerleştirilir ve ardından iletilir. Karşılık gelen zaman diliminden gelen bilgiler hızlı bir şekilde çıkartılır ve görüşme veya oturumu bir araya getirmek için alıcı hücresel baz istasyonunda tekrar birleştirilir. Bu zaman dilimi (veya ses / veri kanalı) bir arayana atandıktan sonra, o arayana sona erinceye kadar oturum süresi için ayrılmıştır. TDMA'da, bir kullanıcıya bütün bir frekans atanmaz, ancak frekansı, her biri belirlenmiş bir zaman dilimine sahip diğer kullanıcılarla paylaşır.

Bu bölümün yazılmasından itibaren, TDMA telefon konuşmalarını ve veri akışlarını kablosuz alanda dolaşırken gizlice dinleyen pek çok vaka olmamıştır. Özel bir teçhizata veya test teçhizatına erişim, muhtemelen bu tür bir başarı için gerekli olacaktır. Yasadışı olarak değiştirilmiş bir TDMA cep telefonunun da bu işi yapması mümkündür.

Bununla birlikte, bu, gizli dinlemenin olanaksız olduğu anlamına gelmez. Kablosuz bir İnternet oturumu ile ilgili olarak, böyle bir oturumun gerçekleştirdiği tam yolu göz önünde bulundurun. Bir mobil kullanıcının bir İnternet Web sitesi ile iletişim kurması için, cep telefonundan gelen bir kablosuz veri sinyali sonunda İnternet'i geçmeden önce kablolu bir sinyale dönüştürülür. Kablolu bir sinyal olarak, bilgiler Web sitesine erişinceye kadar İnternet'te açık metin olarak seyahat edebilir. Her ne kadar kablosuz sinyalin kendisi müdahale etmekte zorlanabilirse de, bir kez kablolu bir sinyal haline geldiğinde, Internet'te dolaşan tüm şifrelenmemiş iletişim ile aynı durdurma güvenlik açılarına maruz kalır.

Önlem olarak, internetten gizli bilgiler varsa, yöntemden bağımsız olarak, bu oturumu baştan sona şifrelemek gerekir. Şifreleme daha sonraki bir bölümde ele alınmıştır.

**4.3.Mobil İletişim için Global Sistemler (GSM)**

Dijital iletimin bir diğer yöntemi, Mobil İletişim için Global Sistemlerdir (GSM). GSM aslında sadece iletim yönteminden daha fazlasını kapsayan bir terimdir. GSM servislerinin çeşitliliğinden, mevcut GSM cihazlarının kendisine kadar tüm hücresel sistemi kapsar. GSM, öncelikle Avrupa ülkelerinde kullanılmaktadır.

Dijital bir iletim yöntemi olarak GSM, bir TDMA varyasyonunu kullanır. FDMA ve TDMA'ya benzer şekilde, GSM servis sağlayıcısı, ayrılan radyo frekansı spektrumunu çoklu frekans kanallarına böler. Bu sefer, her bir frekans kanalı 200 kHz daha büyük bir genişliğe sahiptir. Yine, FDMA ve TDMA'ya benzer şekilde, her bir GSM cep telefonu iki frekans kanalı kullanır: biri göndermek diğeri almak için.

TDMA gibi, GSM ayrıca her bir frekans kanalını ses / veri kanalı adı verilen zaman aralıklarına böler. Ancak, GSM ile sekiz zaman dilimi vardır, böylece şimdi aynı frekansı kullanarak sekiz taneye kadar dijital ses veya veri oturumu gerçekleşebilir. TDMA’ya gelince, bir zaman dilimi (veya ses / veri kanalı) bir arayana tahsis edildiğinde, arayana, sona erinceye kadar oturum süresi boyunca atanmıştır.

GSM, güvenliği artıran ek özelliklere sahiptir. Her GSM telefonu bir abone kimlik modülü (veya SIM) kullanır. SIM, kredi kartı boyutunda bir akıllı kart veya posta pulu boyutunda bir yonga gibi görünebilir. Bu çıkarılabilir SIM, kullanım sırasında GSM telefonuna yerleştirilir. Akıllı kart veya çip, aboneye ait cep telefonu numarası, aboneye ait kimlik doğrulama bilgileri, şifreleme anahtarları, telefon numaraları dizini ve bu aboneye ait kısa kaydedilmiş mesajlar gibi aboneye ait bilgiler içerir. SIM çıkarılabildiğinden, abone bu SIM'i bir telefondan alabilir ve başka bir GSM telefonuna yerleştirebilir. SIM'li yeni telefon daha sonra abonenin kimliğini alacaktır. Kullanıcının kimliği belirli bir telefona değil, çıkarılabilir SIM'in kendisine bağlı. Bu, bir abonenin, telefon numaralarını değiştirmeden farklı GSM telefonlarına kullanmasını veya yükseltmesini mümkün kılar. Başka bir ülkede bir GSM telefonu kiralamak da mümkündür, bu ülke farklı GSM frekanslarında ileten telefonları kullansa bile. Elbette bu düzenleme, sadece farklı ülkelerden gelen GSM servis sağlayıcıların birbirleriyle uyumlu düzenlemelere sahip olması durumunda işe yarar.

SIM, kimlik doğrulama aracı olarak işlev görür, çünkü GSM telefonları onsuz kullanılamaz. SIM bir telefona yerleştirildikten sonra, kullanıcıların bu SIM'le ilişkili kişisel kimlik numaralarını (PIN) girmeleri istenir (SIM PIN’ etkin ise). Doğru PIN numarası olmadan, telefon çalışmayacaktır.

Kullanıcının telefona doğrulanmasının yanı sıra, SIM, bağlantı sırasında telefonu telefonun kendisine doğrulamak için de kullanılır. SIM'deki kimlik doğrulama (veya Ki) tuşunu kullanarak, telefon, her görüşme sırasında servis sağlayıcının Kimlik Doğrulama Merkezine doğrulanır. Süreç, bazı açılardan bir PC'yi uzaktan bir ağa kaydetmek için bir belirteç kartı kullanmaya benzer şekilde, bir meydan okuma yanıt tekniği kullanmaktadır.

SIM'deki tuşların, kimlik doğrulamanın yanı sıra başka bir amacı vardır. SIM tarafından oluşturulan şifreleme (veya Kc) tuşu, cep telefonu ile servis sağlayıcının iletim ekipmanları arasındaki iletişimi gizlilik amacıyla şifrelemek için kullanılabilir. Bu şifreleme, en azından bu iki nokta arasında gizli dinlenmeyi önler.

TDMA'ya benzer olan GSM yayınları, radyo frekansı tarama ekipmanlarını kullanarak müdahale etmek zor, ancak imkansız değildir. Üzerinde bir frekans bulunan sekiz kullanıcı olabilir ve bu sayede dijital sinyaller ayıklanır. GSM, SIM kartı kullanarak şifreleme ekleyerek araya girmeye karşı başka bir güvenlik katmanı ekleyebilir.

Ancak, kablosuz İnternet oturumları söz konusu olduğunda, bu şifreleme biçimi uçtan uca koruma sağlamaz. Yolun sadece bir kısmı gerçekten korunuyor. Bu, TDMA İnternet oturumlarında daha önce bahsedilen soruna benzer. Tipik bir kablosuz İnternet oturumu hem kablosuz hem de kablolu bir yol izler. GSM şifreleme, yalnızca cep telefonu ile servis sağlayıcının iletim sitesi - kablosuz bağlantı arasındaki yolu korur. Oturumun geri kalanı, kablolu yayın İnternet üzerinden - servis sağlayıcının sitesinden İnternet Web sitesine - hala net olarak seyahat edebilir. İnternet oturumunun tamamını gizli tutmak gerekiyorsa, uçtan uca şifreleme yapılması gerekecektir.

**4.4.Kod Bölmeli Çoklu Erişim (CDMA) Teknolojisi**

Başka bir dijital iletim yöntemine kod bölmeli çoklu erişim veya CDMA denir. CDMA, ABD ordusu tarafından yıllardır radyo iletişimini kesmek ve sıkışmak için daha zor hale getirmek için kullanılan bir iletim teknolojisi olan yayılma spektrumuna dayanmaktadır. Qualcomm, CDMA spread spectrum teknolojisini cep telefonları alanına dahil eden öncülerden biridir.

Bir radyo frekansı spektrumunu dar frekans bantlarına veya zaman aralıklarına bölmek yerine, CDMA aynı zamanda bir frekans kanalı olarak da adlandırılan bu radyo spektrumunun çok büyük bir bölümünü kullanır. Frekans kanalı 1.25 megahertz (MHz) genişliğindedir. Çift yönlü iletişim için, her cep telefonu bu geniş CDMA frekans kanallarından ikisini kullanır: biri gönderilecek, biri alacak.

İletişim sırasında, her ses veya veri oturumu ilk önce bir dizi veri sinyaline dönüştürülür. Daha sonra, sinyaller belirli bir arayana ait olduklarını belirtmek için benzersiz bir kodla işaretlenir. Bu kod sözde rasgele gürültü (PN) kodu olarak adlandırılır. Her cep telefonuna, her oturumun başında baz istasyonu tarafından yeni bir PN kodu atanır. Bu kodlanmış sinyaller daha sonra çok geniş bir radyo frekansı spektrumuna yayılarak iletilir. Kanal genişliği çok büyük olduğu için, diğer birçok kullanıcı oturumunu aynı anda idare etme kapasitesine sahiptir, her bir seans tekrar onları uygun arayanla ilişkilendirmek için benzersiz PN kodları ile etiketlenir.

Bir CDMA telefonu, kendisine yönelik veri sinyallerini almak için uygun PN kodunu kullanarak iletimleri alır ve diğer tüm kodlanmış sinyalleri yok sayar.

CDMA ile, baz istasyonlarıyla iletişim kuran cep telefonları aynı geniş frekans kanallarını paylaşıyor. Her arayanı ayıran, kullanılan frekans (FDMA'daki gibi) veya belirli bir frekanstaki (TDMA veya GSM'deki gibi) zaman aralığı değil, o arayan kişiye atanan PN gürültü kodu. CDMA ile, bir ses / veri kanalı, benzersiz bir PN koduyla işaretlenmiş bir veri sinyalidir.

Tek bir CDMA görüşmesini yakalamak zor olacaktır çünkü dijital sinyalleri çok geniş bir radyo frekansı spektrumuna yayılmıştır. Konuşma, yalnızca tek bir frekansta yapılmaz, bu da taramayı zorlaştırır. Ayrıca, PN gürültü kodunu bilmeden, bir gizli dinleme cihazı, ilgili oturumu kullanılan birçok frekanstan çıkaramaz. Kesişmeyi daha da karmaşıklaştırmak için, tüm kanal genişliği aynı anda diğer birçok arayan tarafından doldurulur ve aramaya müdahale etmeye çalışan herkes için çok miktarda gürültü çıkar.

Ancak, daha önce diğer dijital iletim yöntemlerinde görüldüğü gibi, CDMA cep telefonlarını kullanarak yapılan İnternet oturumlarının araya girmesi imkansız değildir. Önceden olduğu gibi, CDMA dijital sinyallerinin kendileri müdahale etmekte zorlanabilse de, bu kablosuz sinyaller kablolu sinyallere dönüştürüldükten sonra, bu sinyaller İnternet'te dolaşırken yakalanabilir. Uçtan uca şifreleme kullanmadan, kablosuz İnternet oturumları, Internet üzerinden seyahat eden diğer şifrelenmemiş iletişim kadar savunmasızdır.

**4.5.Diğer Yöntemler**

Birçoğu daha önce tartışılan türlerin türevleri olan ve bazıları hala geliştirilme aşamasında olan ek dijital iletim yöntemleri vardır. Geliştirilmekte olan bunlardan bazıları

üçüncü nesil veya 3G iletim yöntemleri. TDMA, GSM ve CDMA gibi ikinci nesil (2G) teknolojiler, günümüzün tipik modem hızlarından daha yavaş olan 9,6 - 14,4 Kbps (saniye başına kilobit) iletim hızları sunar. 3G teknolojileri ise daha hızlı iletmek ve daha büyük miktarda veri taşımak için tasarlanmıştır. Bazıları video iletiminin yanı sıra yüksek hızlı İnternet erişimi sağlama yeteneğine sahip olacak.

**5.Güvenli Kablosuz Cihazlar Nasıl?**

Günümüzde kurumsal ağlara uygulandığını gördüğü gibi, İnternet güvenliği, çeşitli nedenlerden dolayı, kablosuz telefonlarda ve PDA'larda uygulamada zor olabilir. Bu cihazların çoğu sınırlı CPU, hafıza, bant genişliği ve depolama yeteneklerine sahiptir. Sonuç olarak, çoğu hayal kırıklığıyla yavaş ve sınırlı bir bilgi işlem gücüne sahip. Tipik bir iş istasyonunda işlem yapmak bir saniyeden daha az zaman alabilen sağlam güvenlik özellikleri, kablosuz bir cihazda potansiyel olarak birkaç dakika sürebilir, bu da mobil kullanıcı için pratik ya da elverişsiz hale getirebilir. Bu cihazların çoğu, tipik iş istasyonlarında bulunan donanım özelliklerinin yalnızca bir kısmına sahip olduğundan, taşınabilir cihazlardaki güvenlik özellikleri genellikle hafif ve hatta bulunmaz - İnternet güvenliği açısından. Ancak, bu aynı cihazlar artık hassas şirket intranetlerine giriş yapmak veya mobil ticaret ve bankacılık yapmak için kullanılıyor. Her ne kadar bu kablosuz cihazlar her yönden daha küçük olsa da, güvenlik ihtiyaçları eskisi kadar önemlidir. Kurumsal BT ve bilgi güvenliği departmanlarının, kurumsal ağları doldurmaya başlarken bu cihazları görmezden gelmeleri bir hata olur. Sonuçta, bu cihazlar ayrımcılık yapmıyor; bir ağdaki diğer düğümlerle aynı şirket varlıklarına girmek için tasarlanabilirler. Bu cihazlarla ilgili güvenlik unsurlarından bazıları burada incelenmiştir.

**5.1.Doğrulama**

Telsiz telefon kullanıcılarının kimliklerini doğrulama süreci uzun yıllar süren uygulama ve gelişim sürecinden geçti. Servis sağlayıcıların kablosuz servis hırsızlığını azaltmaya çalışırken uzun yıllara dayanan deneyimleri göz önüne alındığında, dijital cep telefonlarının bugün sahip olduğu en güvenilir güvenlik özelliklerinden biridir. Servis sağlayıcılar, servislerinin kullanımı için kimlerin ücretlendirileceğini bilmeye büyük ilgi duyduğundan, mobil kullanıcının kimliğini doğrulamak çok önemlidir.

Daha önce belirtildiği gibi, GSM telefonlar, kullanıcı hakkında kimlik doğrulama bilgisi içeren SIM kartlar veya cips kullanırlar. SIM'ler genellikle kimlik doğrulama ve şifreleme anahtarları, kimlik doğrulama algoritmaları, kimlik bilgileri, aboneye ait telefon numaraları, vb. Taşır.

Bununla birlikte, önemli bir not, bu kimlik doğrulama şeklinin mutlaka İnternet ile ilgili işlemler için geçerli olmadığıdır. Mobil kullanıcıyı yalnızca İnternet işlemleriyle ilgili konuşuyorsa, iletimin yalnızca bir parçası olan servis sağlayıcının telefon şebekesine doğrular. Uçtan uca İnternet işlemlerini güvence altına almak için, mobil kullanıcıların hala gerçekten yasal olduklarını doğrulamak için, bağlandıkları İnternet Web sunucularını doğrulamaları gerekir. Aynı şekilde, Internet Web sunucularının da meşru kullanıcılar olduklarını ve sahtekâr olmadıklarını doğrulamak için kendisine bağlanan mobil kullanıcıları doğrulamaları gerekir. Bununla birlikte, kablosuz iletişim servis sağlayıcıları nadiren, cep telefonundan İnternet Web sitesine kadar uçtan uca kimlik doğrulama hizmeti sağlamada görevlidirler. Bu sorumluluk genellikle İnternet Web sunucularının ve uygulamalarının sahiplerine düşer.

Baştan sona kimlik doğrulama için çeşitli yöntemler bugün uygulama düzeyinde denenmektedir. Güvenli mobil ticaret uygulamalarının çoğu, yalnızca tek faktörlü kimlik doğrulaması sağladığı için elbette sınırlamaları olan eski bir bekleme kimliği ve parola kullanıyor. Diğer kuruluşlar, SIM'lere açık / özel anahtar çiftleri, dijital sertifikalar ve diğer açık anahtar altyapısı (PKI) bileşenleri gibi ek güvenlik bileşenleri ekleyerek GSM SIM'leri denemektedir. Bununla birlikte, dijital sertifikaların kullanımı işlem yoğun olabileceğinden, cep telefonları ve elde tutulan cihazlar genellikle bu güvenlik bileşenlerinin hafif versiyonlarını kullanır. Daha küçük işlemcileri kablosuz cihazlara yerleştirmek için, dijital sertifikalar ve bunlarla ilişkili ortak anahtarlar, kablosuz cihazda bulunan kaynaklara bağlı olarak, genellikle masaüstü Web tarayıcılarında dağıtılanlardan daha küçük veya daha zayıf olabilir.

**5.2.**[**Gizlilik**](https://tureng.com/tr/turkce-ingilizce/gizlilik)

Kablosuz cihazlarda gizliliğin korunması, bazı ilginç zorluklar doğurur. Genellikle, bir tarayıcıyla bir Web sitesine eriştiğinde ve giriş yapmak için bir parola girdiğinde, diğerlerinin birinin ekranında gerçek parolayı görmesini engellemek için bir tür parola yıldız işaretleriyle veya başka bir yer tutucuyla gizlenir. Cep telefonlarında ve elde tutulan cihazlarda, parolanın maskelenmesi yazarken sorun yaratabilir. Cep telefonlarında, çoğu kullanıcı için zahmetli ve sıkıcı olan bir yöntem olan sayısal tuş takımını kullanarak harfler sık ​​sık girilir.

Gizliliğin korunmasındaki bir diğer zorluk, şifreler ve kredi kartı numaraları gibi gizli bilgilerin, kullanıldıktan sonra mobil cihazın hafızasından silinmesini sağlamaktır. Çoğu zaman, bu tür hassas bilgiler kablosuz Internet uygulaması tarafından değişkenler olarak depolanır ve daha sonra cihazın hafızasına önbelleğe alınır. Cep telefonlarının hafızasında kalan kredi kartı numaralarının, aynı sitelere erişmek için aynı telefonları ödünç alan diğer kişiler tarafından tekrar kullanılabileceği belgelenmiş durumlar olmuştur. Bir kez daha, uygulama tasarımcıları buradaki gizliliği korumakta baş mimarlar. Programcıların, kullanıcı bu uygulamayı kullanmayı bitirdiğinde mobil cihazın hassas bilgi hafızasını temizlemek için bir uygulama tasarlamaları önemlidir. Bu bilgilerin cihazın hafızasında bırakılması kullanıcının bir dahaki sefere tekrar girmek zorunda kalmasına izin vermese de, ilgili PIN veya şifreyi bir banka ATM kartına yazmak kadar risklidir.

Gizliliğin korunmasındaki bir başka zorluk da, kablosuz cihazdan İnternet'teki hedefine ve geriye dönerken hassas bilgilerin gizli kalmasını sağlamaktır. Geleneksel olarak, kablolu İnternet için çoğu Web sitesi, istemciden Web sunucusuna kadar tüm yolu şifrelemek için Güvenli Yuva Katmanı (SSL) veya halefi Transport Layer Security (TLS) kullanır. Bununla birlikte, birçok cep telefonu, özellikle cep telefonları, SSL'yi verimli bir şekilde çalıştırmak için hesaplama gücünden ve bant genişliğinden yoksundur. SSL'nin ana bileşenlerinden biri RSA ortak anahtar şifrelemesidir. Web sitesinde uygulanan şifreleme gücüne bağlı olarak, bu açık anahtar şifreleme biçimi işlemci ve bant genişliği yoğun olabilir ve mobil cihazı iletişim oturumunun kendisinin pratik olamayacak kadar yavaş olduğu noktaya kadar vergi uygulayabilir.

**5.3.Kötü Amaçlı Kod ve Virüsler**

Kablosuz cihazlara yapılan güvenlik saldırılarının sayısı, iş istasyonlarına ve sunuculara yapılan saldırılara kıyasla küçüktü. Bunun nedeni, kısmen, çoğu mobil cihazın, özellikle cep telefonlarının, kötü niyetli kod ve virüslerin kullanabileceği yeterli işlemci, bellek veya depolamaya sahip olmamasıdır. Örneğin, günümüzde virüs yaymak için popüler bir yöntem, onları e-postalara ekli dosyalarda saklamaktır. Bununla birlikte, çoğu mobil cihaz, özellikle de cep telefonları, e-posta eklerini saklama veya açma yeteneğinden yoksundur. Bu, mobil cihazları hedef olarak göreceli olarak çekici kılmamaktadır çünkü hasar potansiyeli göreceli olarak düşüktür.

Bununla birlikte, mobil cihazlar hala saldırılara açık durumdadır ve daha fazla bilgi işlem, bellek ve depolama özellikleriyle geliştikçe gittikçe daha fazla hale gelecektir. Daha yüksek hızlarla, daha hızlı indirme yetenekleriyle ve daha iyi işlemlerle, mobil cihazlar yakında tüm sömürülebilir güvenlik açıklarıyla bugünkü iş istasyonlarının eşdeğeri olabilir. Bu bölümün yazılmasından itibaren, cep telefonu üreticileri, yeni nesil cep telefonlarının Java gibi dilleri destekleyeceğini, böylece kullanıcıların organizatör, hesap makinesi ve oyun gibi yazılım programlarını Web özellikli telefonlarına indirebileceklerini duyuruyorlardı. Bununla birlikte, olumsuz tarafta, kullanıcılar için farkında olmadan kötü niyetli programları (veya “kötü amaçlı yazılımları”) kendi cihazlarına indirmeleri için daha fazla fırsat açılır. Aşağıdaki atasözü mobil cihazlar için geçerlidir: “Ne kadar çok beyinleri olursa, hedef olarak o kadar çekici olurlar.”

**6. Güvenli Ağ Altyapı Bileşenleri Nasıl?**

Bilgi güvenliği alanında çalışan birçoğumuzun bildiği gibi, güvenlik genellikle birçok bileşen kullanılarak kurulur, ancak genel gücü sadece en zayıf halkası kadar iyidir. Bazen biri ağ üzerinden mümkün olan en güçlü şifrelemeyi ve cihazlarda en güçlü doğrulamayı kullanmanın bir önemi yoktur. Zincir boyunca herhangi bir yerde zayıf bir bağlantı varsa, saldırganlar bu güvenlik açığına odaklanacak ve sonunda en az çabayı ve en az miktarda kaynak gerektiren bir yolu seçerek bundan faydalanabilir.

Kablosuz İnternet dünyası hala nispeten genç ve devam etmekte olan bir çalışma olduğu için, uyguladığı teknolojiye bağlı olarak güvenlik açıkları çok fazla. Bu bölüm, WAP (Kablosuz Uygulama Protokolü) kullananlar için bazı altyapı açıklarına odaklanmaktadır.

**6.1.“WAP'taki Boşluk”**

Şifreleme, E-ticaret dünyasında paha biçilmez bir araç olmuştur. Birçok çevrimiçi işletme, istemci ve Web sunucusu arasındaki İnternet işlemlerini korumak için uçtan uca şifreleme sağlamak için SSL (Güvenli Yuva Katmanı) veya TLS (Aktarım Katmanı Güvenliği) kullanır. Bununla birlikte, WAP kullanılırken, oturum için şifreleme etkinleştirilirse, her biri iletimin iki farklı yarısını koruyan genellikle iki şifreleme bölgesi uygulanır. SSL veya TLS, genellikle Web sunucusu ile daha önce belirtilen WAP ağ geçidi adı verilen önemli bir ağ cihazı arasındaki ilk yolu korumak için kullanılır. WTLS (Kablosuz Aktarım Katmanı Güvenliği), WAP ağ geçidi ve kablosuz mobil cihaz arasındaki ikinci yolu korumak için kullanılır.

WAP ağ geçidi, kablolu sinyalleri kablosuz iletimlerle uyumlu, daha az bant genişliğine sahip yoğun ve sıkıştırılmış bir ikili biçime dönüştürmek için gereken bir altyapı bileşenidir. Bir oturum sırasında SSL gibi şifreleme kullanılırsa, WAP ağ geçidinin, bu SSL trafiğini şifresini çözerek ve WTLS ile yeniden şifreleyerek, diğer yönde ters şifreleyerek SSL korumalı iletimi çevirmesi gerekecektir. Bu çeviri sadece birkaç saniye sürebilir; ancak bu kısa süre zarfında, veriler şifresi çözülmüş WAP ağ geçidinin hafızasına ve ikinci protokol kullanılarak yeniden şifrelenmeden önce temiz bir şekilde oturur. WAP ağ geçidindeki bu kısa süre - bazıları “WAP'taki boşluk” olarak adlandırdı - sömürülebilir bir güvenlik açığıdır. WAP ağ geçidinin bulunduğu yere, ne kadar güvenli olduğuna ve onu korumaktan kimin sorumlu olduğuna bağlıdır.

**6.2.WAP Ağ Geçidi Mimarileri**

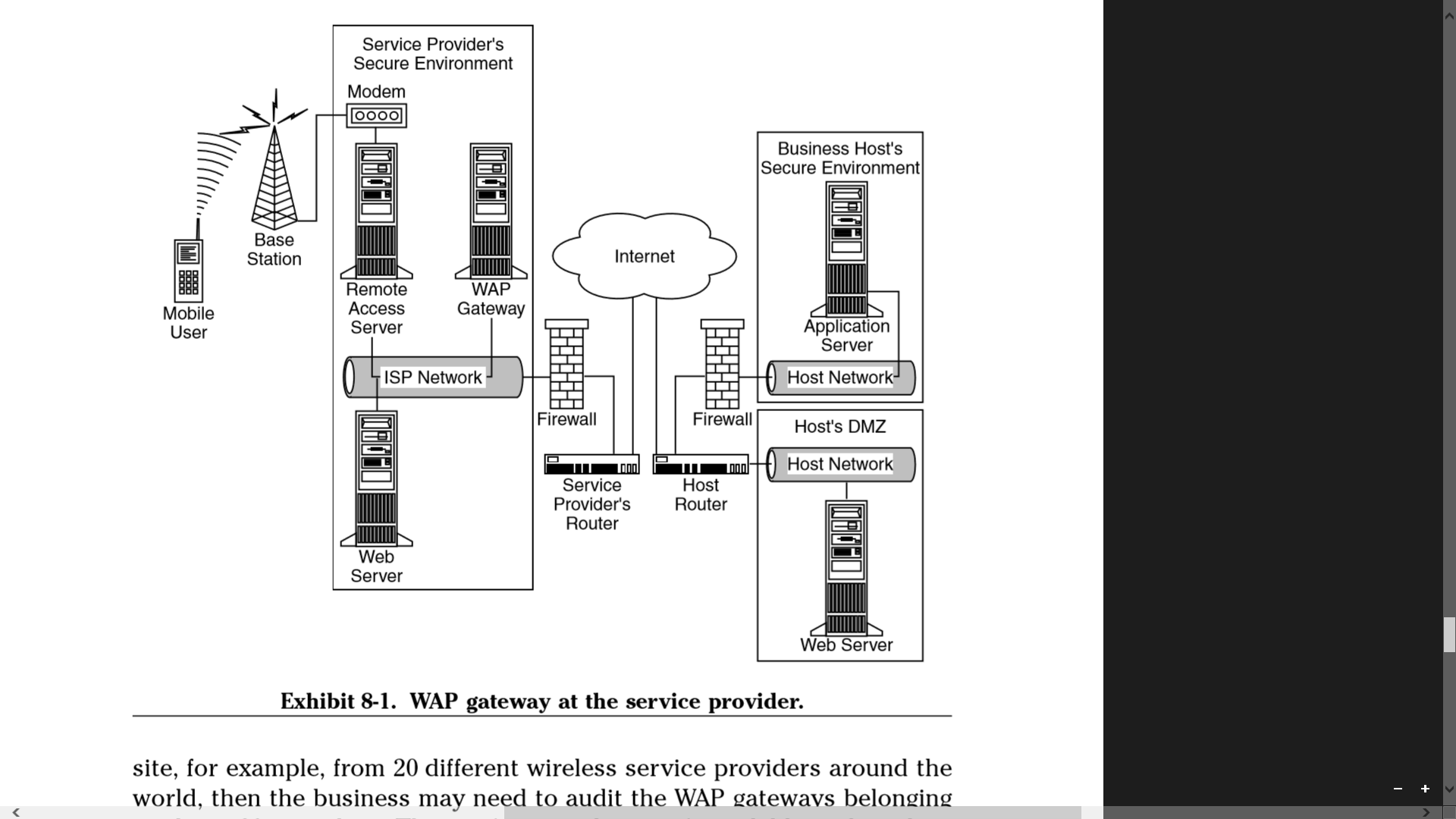
Verilerin duyarlılığına ve izinsiz ifşa edilmesinin sorumluluğuna bağlı olarak, güvenli kablosuz uygulamalar sunan işletmelerin (ve bunun yanı sıra müşterileri), WAP ağ geçidinin nerede bulunduğu, nasıl korunduğu ve kimin koruduğu konusunda endişeleri olabilir. Üç olası mimariler ve bunların güvenlik etkileri incelenmiştir:

**6.2.1.Servis Sağlayıcıdaki WAP Ağ Geçidi**

Çoğu durumda, WAP ağ geçitleri kablosuz servis sağlayıcılarına aittir. Günümüzde güvenli kablosuz uygulamalar kullanan birçok işletme, SSL'den WTLS'ye şifreleme çevirisi yapmak için servis sağlayıcının WAP ağ geçidine güvenir. Bu, hassas kablosuz uygulamaların iş sahiplerinin yanı sıra kullanıcılarının da kablosuz servis sağlayıcılarına WAP ağ geçidini ve içinden geçen hassas verileri güvenli ve güvende tutmalarını emrettiğini gösterir. WAP ağ geçidinin servis sağlayıcının güvenli ortamında bulunduğu bir kurulum örneği sağlar. Şifreleme, kullanıcının cep telefonu ile işletme duvarının arkasındaki uygulama sunucusu arasındaki bir oturumda uygulanırsa, cep telefonu ile servis sağlayıcısının WAP ağ geçidi arasındaki yol genellikle WTLS kullanılarak şifrelenir. WAP gateway ile işletme ana bilgisayarının uygulama sunucusu arasındaki yol, SSL veya TLS kullanılarak şifrelenir.

Bununla birlikte, bu kurulumu kullanan güvenli WAP uygulamaları kullanan bir işletme, verilerin şifresinin çözüldüğü, kısa bir süre için açık bir metne maruz bırakıldığı ve daha sonra şifrelenmiş olduğu için uçtan uca güvenliği garanti edemeyeceğini anlamalıdır. kontrolden uzakta olan dış ağ geçidi. WAP ağ geçidi, genellikle kablosuz servis sağlayıcısının veri merkezinde bulunur ve doğrudan işletmelere karşı sorumlu olmayanlar tarafından katılır. Elbette, WAP ağ geçidini güvenli bir şekilde ve konumda tutmak, servis sağlayıcının yararınadır.

Bazen, bu güveni pekiştirmeye yardımcı olmak için işletmeler, risklerin en aza indirilmesini sağlamak için servis sağlayıcının WAP ağ geçitlerini işletmesinde periyodik güvenlik denetimleri yapmak isteyebilir. Bununla birlikte, bu yolu seçerek, işletmenin birçok WAP ağ geçidini birçok farklı servis sağlayıcıdan incelemesi gerekebileceğini unutmayın. Bir servis sağlayıcı, WAP ağ geçidini öncelikle kendi kablosuz telefon abonelerine İnternet erişimi sağlayacak şekilde ayarlar. Kullanıcılar bir işletmenin güvenli Web sitesine, örneğin dünyadaki 20 farklı kablosuz servis sağlayıcısından arama yapıyorsa, işletmenin bu 20 sağlayıcıya ait WAP ağ geçitlerini denetlemesi gerekebilir. Bu, ne yazık ki, zor bir görev ve güvenliği sağlamak için pratik bir yöntemdir. Her servis sağlayıcı kendi WAP ağ geçidini korumak için farklı bir yöntem uygulayabilir - eğer korunuyorsa. Ayrıca, çoğu durumda, kablosuz iletişim servis sağlayıcıları, sözleşmeye bağlı bir düzenleme olmadığı sürece, güvenli İnternet uygulamaları barındıran sayısız işletmeye değil, kendi cep telefonu abonelerine karşı sorumludurlar.

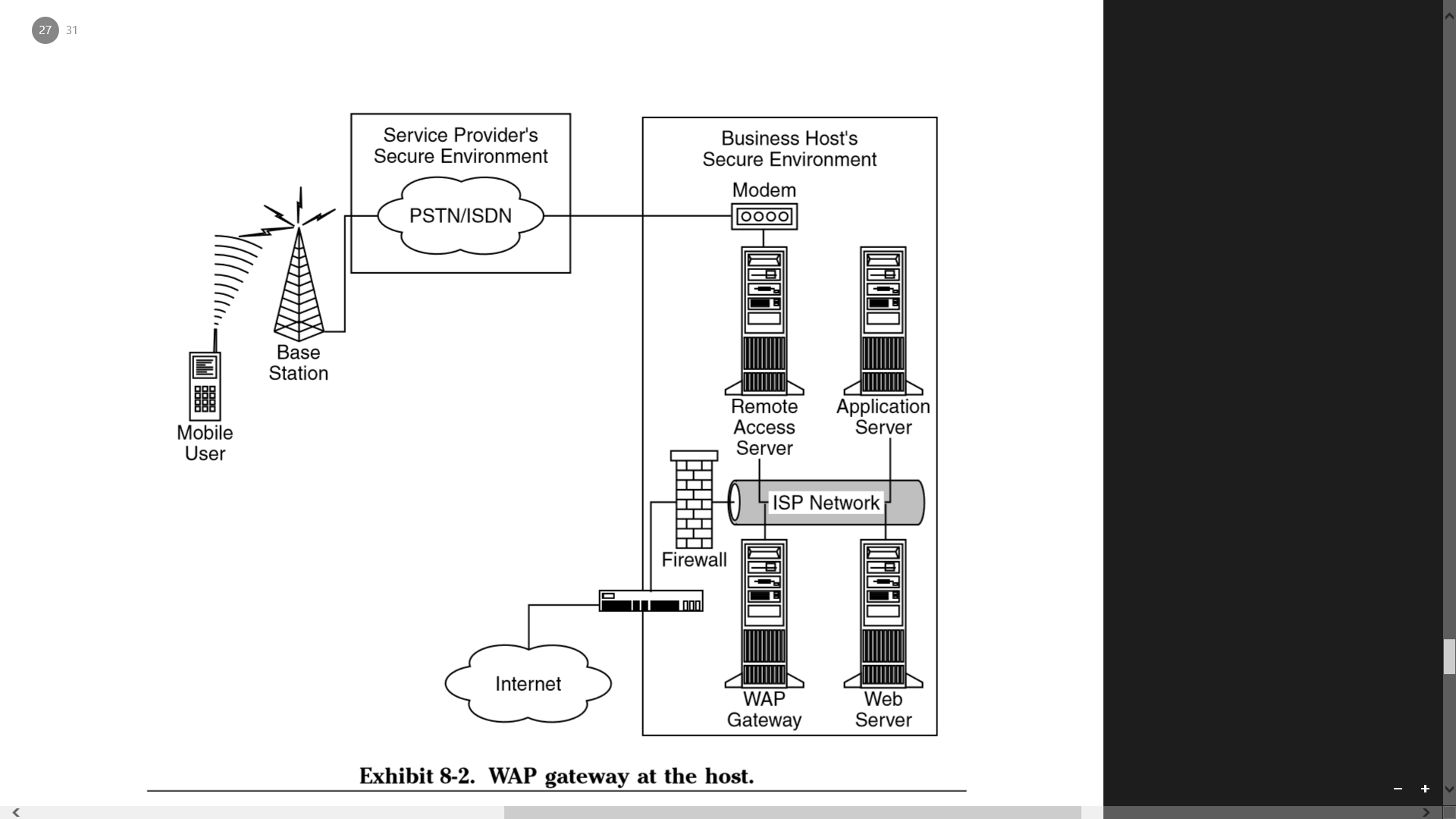


**Şekil 1: Servis sağlayıcıdaki WAP ağ geçidi**

**6.2.2.Ana Bilgisayardaki WAP Ağ Geçidi**

Özellikle finansal, sağlık ve devlet sektörlerinde olmak üzere bazı işletmeler ve kuruluşlar, müşterilerinin hassas verilerini korumada tutmak için yasal gereksinimlere sahip olabilir. Bu hassas verilerin kurumun iç kontrolünün dışında kalması gereksiz bir risk ve yükümlülük teşkil edebilir. Bazılarına göre, “WAP'taki boşluk”, sadece sömürülmeyi bekleyen açık bir gizlilik ihlali olan kırılmış bir boru hattı sunuyor. Bu tür bir ihlali kabul edilemez bulmuş olanlar için, olası bir çözüm, kablosuz servis sağlayıcısının WAP ağ geçidini tamamen geçerek, WAP ağ geçidini iş sahibinin kendi korumalı ağına yerleştirmektir. Sekil 2, böyle bir kurulumun bir örneğini sunar. Nokia, Ericsson ve Ariel İletişim bu tür bir çözüm sunan satıcılardan sadece birkaçıdır.

Bu yaklaşım, WAP ağ geçidini ve WTLSSSL çeviri sürecini, güvenli Web uygulamaları sağlayan aynı kurumun sınırları içinde, güvenilir bir yerde tutmanın yararına sahiptir. Bu kurulumu kullanarak, kullanıcılar genellikle doğrudan kablosuz cihazlarından, servis sağlayıcılarının Genel Anahtarlamalı Telefon Ağı (PSTN) üzerinden ve işletmenin kendi Uzaktan Erişim Sunucuları (RAS) üzerinden arama yaparlar. RAS'a ulaştıklarında, iletim WAP ağ geçidinde devam eder ve daha sonra, iş sahibinin kendi güvenli ortamı içindeki tüm bu cihazların uygulamasına veya Web sunucusuna iletilir.

****

**Şekil 2 :Ana bilgisayardaki WAP ağ geçidi.**

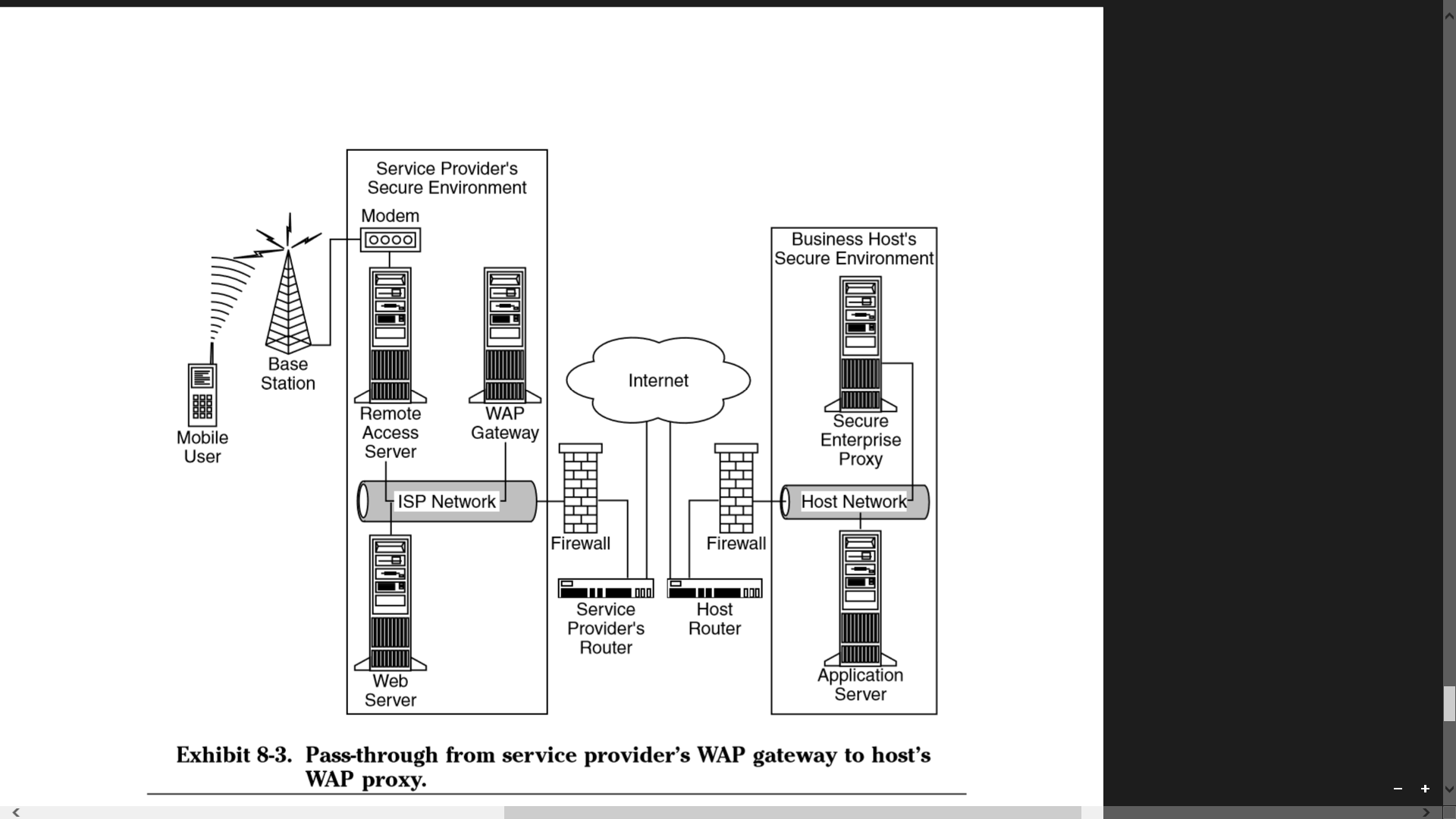
Baştan sona daha iyi güvenlik sağlasa da, bu yaklaşımın sakıncası, işletme sahibinin modemleri ve RAS bankalarını kurması ve böylece kullanıcıların çevirmek için yeterli erişim noktasına sahip olmaları gerektiğidir. İşletmenin kullanıcıları yeniden yapılandırması gerekir 'Cep telefonları ve PDA'lar doğrudan işletmeye işaret eder' tipik olarak servis sağlayıcının yerine kendi WAP ağ geçidine. Ancak, tüm cep telefonları kullanıcı tarafından bu yapılandırmaya izin vermez. Ayrıca, bazı cep telefonları yalnızca bir WAP ağ geçidine işaret ederken, diğerleri birden fazla kişiye işaret edecek kadar şanslı. Her iki durumda da, tüm bu kablosuz aygıtları, işletmenin kendi WAP ağ geçidini gösterecek şekilde tek tek yapılandırmak, önemli ölçüde zaman ve çaba gerektirebilir.

Cep telefonları yalnızca tek bir WAP ağ geçidine işaret edebilen kullanıcılar için bu düzenleme başka bir sorunu daha ortaya koymaktadır. Bu kullanıcılar şimdi İnternet'teki diğer WAP sitelerine erişmek istiyorsa, yine de işletme ana bilgisayarının WAP ağ geçidi üzerinden geçmeleri gerekir. Eğer ana bilgisayar Internet'e giden trafiğe izin veriyorsa, ana bilgisayar kendi WAP ağ geçidine işaret etmek için yeni yapılandırılmış olan bu kullanıcılar için bir İnternet servis sağlayıcısı (ISS) olur. Bir geçici ISS olarak hareket eden, ev sahibi kaçınılmaz olarak birçok işletme için gereken önemli kaynaklar nedeniyle istenmeyen bir yük olabileceği hizmet ve kullanıcı ile ilgili konulara katılmaya ihtiyaç duyacaktır.

**6.2.3.Servis Sağlayıcı’nın WAP Ağ Geçidinden Host’un WAP Proxy'sine Geçiş**

Uçtan uca güvenli şifreli işlemler sağlamak isteyen ancak kendi WAP ağ geçitlerini kurmanın idari zorluklarından kaçınmak isteyen işletmeler için başka yaklaşımlar da var. Sekil 3'te gösterildiği gibi bu yaklaşımlardan biri, WTLS ile şifrelenmiş verilerin, kullanıcının mobil cihazından ve servis sağlayıcısının WAP ağ geçidinden olduğu gibi değişmemesini sağlamaktır. WTLS-SSL şifreleme çevirisi, şifrelenmiş veriler işletme ana bilgisayarının kendi güvenli ağında bulunan ikinci bir WAP ağ geçidi benzeri cihaza ulaşana kadar gerçekleşmez. Böyle bir çözüm geliştiren satıcılardan biri Openwave Systems (Phone.com ve Software.com’un bir kombinasyonu). Openwave, bu ikinci WAP ağ geçidi benzeri aygıta Secure Enterprise Proxy'yi çağırır. Şifreli bir oturum sırasında, servis sağlayıcının WAP ağ geçidi ve işletmenin Secure Enterprise Proxy'si birbirleriyle anlaşır, böylece servis sağlayıcısı, esasen bu Proxy'yi kullanan işletmeye değiştirilen şifreli verileri iletir. Bu çözüm, servis sağlayıcının WAP ağ geçidini kullanır, çünkü mobil kullanıcılar için uygun İnternet erişimi sağlamak için hala gereklidir, ancak WTLS-SSL şifreleme çevirisini orada yapmaz ve dolayısıyla gizli verileri açığa çıkarmaz. Şifre çözme işlemi, işyerinin kendi güvenli ağında, Secure Enterprise Proxy'de veya uygulama sunucusunda geçirilir ve gerçekleştirilir.

Bununla birlikte, bu yaklaşımın bir dezavantajı, özel mülkiyetidir. Bu yazının yazıldığı sırada, Openwave çözümünün çalışması için üç tarafın bileşenleri yalnızca Openwave'den uygulaması gerekecektir. Kablosuz iletişim servis sağlayıcılarının, Openwave’in en son WAP ağ geçidini kullanmaları gerekir. Aynı şekilde, güvenli uygulamaları barındıran işletmenin, söz konusu ağ geçidi ile şifreleme geçişini görüşmek için Openwave’in Secure Enterprise Proxy’ini kullanması gerekir. Ek olarak, mobil cihazların kendilerinin de Openwave'in en son Web tarayıcısını, en azından Mikro tarayıcı sürüm 5'i kullanmaları gerekir. Dünyadaki WAP özellikli telefonların yaklaşık yüzde 70'i Openwave Micro-browser'ın bazı versiyonlarını kullanıyor olmasına rağmen, bu telefonlar sürüm 3 veya 4'ü kullanıyorlar. Ne yazık ki, bu tarayıcıların çoğu kullanıcı tarafından yükseltilemiyor, bu nedenle çoğu kullanıcının bu çözümü kullanmak için yeni cep telefonları satın alması gerekebilir. Bu çözümün meyve vermesi ve popüler hale gelmesi biraz zaman alabilir.



**Şekil 3:Servis sağlayıcının WAP ağ geçidinden ana makinenin WAP proxy'sine geçiş**

Bunlar, kablosuz Internet aygıtları için uçtan uca şifreleme sağlama konusundaki tek çözüm değildir. Çalışmalardaki diğer yöntemler, uygulama düzeyinde şifreleme uygulamak, cep telefonu SIM kartlarına şifreleme anahtarları ve algoritmalar eklemek ve WAP özelliklerinin bir sonraki revizyonuna daha güçlü şifreleme teknikleri eklemek, belki de “WAP'taki boşluk” u tamamen ortadan kaldırmaktır

**7.Sonuç**

Bilgi güvenliği mesleğinde birçok uygulayıcı için iki sağlam öneri:

• Kablosuz güvenlik sorunları ve çözümlerinden haberdar olun.

• Kablosuz aygıtları görmezden gelmeyin.

BT ve bilgi güvenliği mesleklerindeki çoğu kişi, yeni kablosuz İnternet cihazlarını kısaca kişisel araçlar veya yönetici oyuncakları olarak görür. Birçoğu, kurumsal bilgisayarlarını, sunucularını ve ağlarını koruma sorunları ile uğraşmakla meşguldür, başka bir aygıt sınıfı için endişelenmeyi hayal edemezler. Birçok kurumsal güvenlik politikası, mobil el cihazlarını ve cep telefonlarını güvenceye almaktan hiç söz etmez, ancak bu aynı şirketlerden bazıları zaten kendi dahili e-postalarına erişmek için bu cihazları kullanıyor. Duyulan yaygın yanlışlık şudur: bu cihazlar çok küçük olduğu için, böyle küçük bir cihazın yaratacağı zarar ne olabilir?

Güvenlik departmanları, bilgi varlıklarının anabilgisayar dünyasından dağıtılmış bilgisayar hesaplamaya geçişiyle mücadele etmek zorunda kaldı. Bu evrim sırasında güvenliği nereye uygulayacağınız konusunda birçok kurumsal tutum değişmek zorunda kalmıştır. Abartı olmadan, kurumsal bilgi işlem bir başka önemli göç aşaması geçiriyor. Kurumsal bilgi varlıklarına kablosuz yollardan erişilebilecek kadar fazla değildir, çünkü kablosuz dizüstü bilgisayarlar yıllardır bunu yapıyor; bunun yerine erişim araçları daha ucuz hale gelecek ve böylece hacimsel olarak daha büyük hale gelecektir. 3000 dolarlık bir dizüstü bilgisayar kullanmak yerine, kullanıcılar (veya davetsiz misafir) artık yalnızca 40 dolarlık bir İnternet özellikli cep telefonunu kullanarak her yerden hassas bir kurumsal ağa erişebilir. Zaman içinde, bu mobil cihazlar işlem gücü, bellek, bant genişliği, depolama, kullanım kolaylığı ve son olarak popülerliği artıracaktır. Kurumsal kaynaklardan kaçınılmaz olarak yararlanacak olan bu son maddedir.

**Kaynakça**

**Kitap:**

1. Blake, Roy, Wireless Communication Technology , Delmar Thomson Learning, 2001.

2. Harte, Lawrence et al., Cellular and PCS: The Big Picture , McGraw-Hill, 1997.

3. Howell, Ric et al., Professional WAP, Wrox Press Ltd., 2000.

4. Muller, Nathan J., Desktop Encyclopedia of Telecommunications, second edition , McGrawHill, 2000.

5. Tulloch, Mitch, Microsoft Encyclopedia of Networking, Microsoft Press, 2000.

6. Van der Heijden, Marcel and Taylor, Marcus, Understanding WAP: Wireless Applications, Devices, and Services, Artech House Publishers, 2000.

**Makaleler ve Site:**

1. Saarinen Markku-Juhani,

Attacks Against the WAP WTLS Protocol, University of Jvyskyl,Finland.

2. Saita, Anne, Case Study: Securing Thin Air, Academia Seeks Better Security Solutions for Handheld Wireless Devices, http://www.infosecuritymag.com, April 2001.

3. Complete WAP Security from Certicom, <http://www.certicom.com>.

4. Radding, Alan, Crossing the Wireless Security Gap, http://www.computerworld.com, Jan. 1, 2001.

5. Does Java Solve Worldwide WAP Wait?, http://www.unstrung.com, April 9, 2001.

6. DeJesus, Edmund X., “Locking Down the… Wireless Devices Are Flooding the Airwaves with Millions of Bits of Information. Securing Those Transmissions Is the Next Challenge Facing E-Commerce, http://www.infosecuritymag.com, Oct. 2000.

7. Izarek, Stephanie, Next-Gen Cell Phones Could Be Targets for Viruses, http://www.foxnews.com, June 1, 2000.

8. Nobel, Carmen, Phone.com Plugs WAP Security Hole, eWEEK, September 25, 2000.

9. Schwartz, Ephraim, Two-Zone Wireless Security System Creates a Big Hole in Your Communications, http://www.infoworld.com, Nov. 6, 2000.

10. Appleby, Timothy P., WAP — The Wireless Application Protocol (White Paper), Global Integrity.

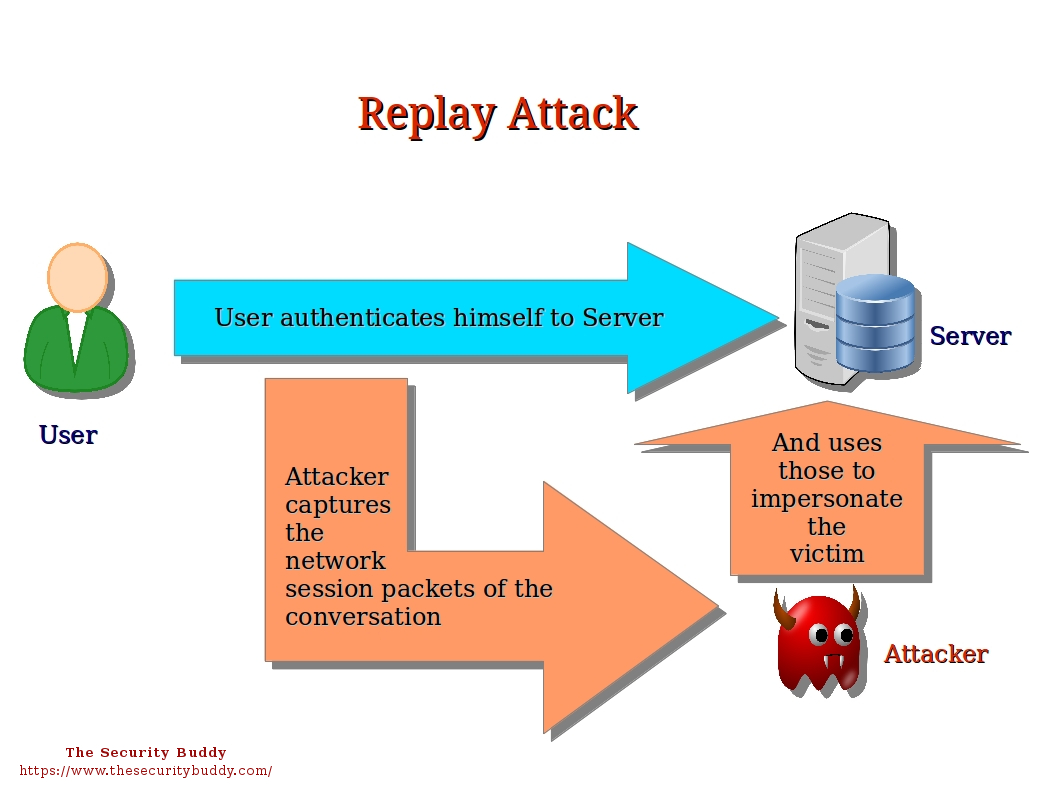
11. Wireless Devices Present New Security Challenges — Growth in Wireless Internet Access Means Handhelds Will Be Targets of More Attacks, CMP Media, Inc., Oct 21, 2000.

**Tekrar Saldırıları**

**Tekrar Saldırısı Nedir?**

Bazen playback saldırısı olarak da isimlendirilen tekrar saldırısı, kötü niyetli biri kişinin bir ağ üzerinden geçen geçerli bir veri iletimini ele geçirip  bunu tekrarlayarak gerçekleştirdiği bir siber saldırıdır.

Orjinal verinin geçerli olması nedeniyle (genellikle yetkili bir kullanıcıdan geldiği için) ağın güvenlik protokolleri saldırıya normal bir veri transferi muamelesi yapar. Orjinal mesaj ele geçirildiği ve bire bir aynı şekilde tekrar iletildiği için, tekrar saldırılarını gerçekleştiren bilgisayar korsanlarının bu mesajların şifresini çözmesi gerekmez.



**Şekil 1:Tekrar Saldırısı Akış Şeması**

<https://www.thesecuritybuddy.com/vulnerabilities/what-is-replay-attack/>

**Saldırganlar tekrar saldırısıyla ne yapabilir?**

* Tekrar saldırıları, korunan bir ağ üzerinde depolanan bilgiye görünürde geçerli kimlik bilgileri sunarak erişim sağlamak üzere kullanılabilir.
* Aynı zamanda, finansal kurumları da işlemlerin ikinci kez tekrarlanması  yönünde kandırarak saldırganların kurbanlarının hesaplarından doğrudan paraçekmesine olanak verir.
* bilgisayar korsanları **şifreli** mesajların farklı parçalarını bir araya getirir ve ortaya çıkan şifreli metni ağa sunarak kopyala-yapıştır saldırısı olarak bilinen saldırıyı gerçekleştirebilir.
* Saldırganlar gönderilen **datayı** değiştiremez çünkü  ağ bunu reddedecektir ve bu da saldırının eski faaliyetleri tekrarlamadaki etkinliğini sınırlar.
* Ayrıca bu saldırılardan korunmak göreceli olarak daha kolaydır. Veri iletimine saat damgası eklemek kadar basit bir korunma bile basit tekrar saldırı girişimlerine karşı koruma sağlar

**Bir Tekrar Saldırısını Durdurma**

Böyle bir saldırıyı önlemek, doğru şifreleme yöntemine sahip olmakla ilgilidir. Şifreli mesajlar içinde "anahtarlar" taşır ve aktarım sonunda kodları çözüldüğünde mesajı açarlar. Bir tekrarlama saldırısında, orijinal mesajı ele geçiren saldırganın anahtarı okuyabileceği veya deşifre edebileceği önemli değildir. Tek yapması gereken, her şeyi - mesaj ve anahtar - birlikte yakalamak ve tekrar göndermek.

Bu olasılığı önlemek için, hem gönderenin hem de alıcının, yalnızca bir işlem için geçerli olan ve bir daha kullanılamayan bir tür kod olan tamamen rastgele bir oturum anahtarı oluşturması gerekir.

Bu tür bir saldırı için bir başka önleyici önlem, tüm mesajlarda zaman damgası kullanmaktır. Bu, bilgisayar korsanlarının belirli bir süreden daha uzun bir süre önce gönderilen mesajları yeniden göndermelerini önler, böylece bir saldırganın gizlice dinlenmesi, iletinin sifonu çekilmesi ve yeniden gönderilmesi için fırsat penceresini azaltır.

Mağdur olmaktan kaçınmanın başka bir yolu da, yalnızca bir kez kullanılan ve atılan her işlem için bir parolaya sahip olmaktır. Bu, mesaj bir saldırgan tarafından kaydedilmiş ve tekrar gönderilmiş olsa bile, şifreleme kodunun süresinin dolmuş ve artık çalışmamasını sağlar.

**Son Söz**

* Tekrar saldırıları başarılı olurlarsa ağ güvenliği için gerçek bir tehdit teşkil eder. Diğer birçok saldırı tipinin aksine, tekrar saldırıları verinin şifresinin çözülmesini gerektirmez bu da onları sürekli daha da fazla güvenli şifreleme protokolüyle karşı karşıya kalan kötü niyetli kişiler için etkin bir  çözüm haline getirir.

**Kaynakça**

[1] <https://www.binance.vision/tr/security/what-is-a-replay-attack>

[2] <https://www.bgasecurity.com/makaleler/>

[3] <https://dergipark.org.tr/download/article-file/465726>

[4] <https://www.binance.vision/security/what-is-a-replay-attack>

[5]<https://www.careerride.com/Networking-replay-attacks.aspx>

[6]<https://medium.com/coinmonks/what-is-a-replay-attack-b0e2c3b1dec4>