
**TÜRKİYE BİLİŞİM DERNEĞİ**

**KAMU BİLGİ İŞLEM MERKEZLERİ YÖNETİCİLERİ BİRLİĞİ**

**Kamu Bilişim Platformu XI**

# MOBİL UYGULAMALARDA GÜVENLİK

**Sürüm 1.0**

**2. BELGE GRUBU**

**Nisan 2009**

**TBD Kamu-BİB**

**Kamu Bilişim Platformu XI**

# MOBİL UYGULAMALARDA GÜVENLİK

Sürüm 1.0

## 2. BELGE GRUBU

Bu belge, TBD Kamu-BİB' in ***onbirinci dönem*** çalışmaları kapsamında, **2. Belge Grubu (BG2)** tarafından hazırlanmıştır. Mobil Uygulamaların Güvenliğine yönelik kavramları, uluslararası standartları, kısıtlamaları, korunmasızlık ve tehditleri, riskleri ve alınabilecek önlemlere ilişkin önerileri içermektedir.

### Hedef Kitle

Çalışmanın içeriği, mobil cihaz ve mobil uygulama kullanan tüm vatandaşlara yöneliktir.

### Yayını Hazırlayanlar


TURHAN YÜKSELİYOR (Belge Grubu Başkanı)

Dr. CEMİL ULU (Belge Grubu Başkan Yrd.)



**Belge No** : TBD/Kamu-BIB/2009-BG2

**Tarihi** : 24/03/2009

**Durumu** : Nihai Rapor – S 1.0

## 2. Belge Grubu

| | | |
|---|---|---|
| **Belge Grubu Başkanı** | TURHAN YÜKSELİYOR | (INNOVA) |
| **Kamu-BİB YK Temsilcisi** | AHMET PEKEL | (TCMB) |
| | AYKUT DALYAN | (TURKCELL) |
| **Belge Grubu Başkan Yrd.** | Dr. CEMİL ULU | (TCMB) |
| **Grup Üyeleri** | SERDAR MURAT ÖZTANER | (TCMB) |
| | TUBA EBRU KARAZİNCİR | (SSM) |
| | MUSTAFA ONUR ÖZORHAN | (TCMB) |
| | MUZAFFER YILDIRIM | (EGA) |
| | ÖZGÜR ŞANLI | (TCMB) |
| | AHMET KAYMAZ | (DMO) |
| | EMİN CEBE | (SSM) |

# İÇİNDEKİLER

# Tanımlar ve Kısaltmalar

| | |
|---|---|
| **3G** | "3. Generation". Geniş Alan Hücresel paket ve devre anahtarlamalı mobil şebekesi için III. kuşak standart ve teknolojisi. |
| **4G** | "4. Generation". IP temelli, paket anahtarlamalı, geniş kapasiteli, ses, veri ve çoklu ortam servislerinin istenilen yerde ve zamanda sunulabildiği en son mobil teknolojisi [1]. |
| **AAA** | "Authentication, Authorization, Accountability" Kimlik onayı, yetkilendirme ve izlenebilirlik işlevsellikleri. CDMA veri şebekelerinde yer alan AAA sunucular, bu üç özelliği IP üzerinden destekler. |
| **AES** | "Advanced Encryption Standard". 128, 256 ve 512 bit anahtarlamayı destekleyen gelişmiş simetrik şifreleme sistemi. |
| **Ağ Geçidi** | Kurum bilişim iç ve dış ağındaki nesnelere kontrollü erişimlerin sağlandığı ve paketlerin denetlendiği donanım ve yazılım cihazları. |
| **Anti virüs Yazılımı** | Virüslerin bloke edilmesi ve sezinlenmesine yarayan yazılım. |
| **APN** | "Access Point Name". GSM mobil şebekesinde paket veri bağlantısı için servis türünün tanımlandığı erişim noktası bileşeni. APN erişim noktasında SMS ve MMS mesajlarının teslimat bilgisinin yanında, İnternet sayfalarının protokol çevrimin yapıldığı WAP kapısına bağlantısı, İnternet IPv4 veya IPV6 bağlantısı servisleri verilmektedir [2]. |
| **ARP** | "Address Resolution Protocol". IP adresinden MAC adresine çözümleme protokolü. |
| **Bilgi Bütünlüğü** | Bilginin sahibi tarafından yaratılmasından sonra yetkili ve yetkisiz değiştirilmediğinin sağlanması. |
| **Bilgi Güvenlik Politikası** | Bilginin güvenliğinin sağlanması için gerekli genel kurallar. |

| | |
|---|---|
| **Bluetooth** | Kısa mesafede sabit ve mobil cihazlardan veri değişimi için geliştirilmiş bir telsiz iletişim protokolü ve bu özelliği destekleyen cihazların teknolojik özelliği. |
| **BSS** | "Base Station Subsystem". GSM şebekesinde kullanılan baz istasyonları ve bunlara ait denetleyici Mobil Operatör ağ bileşenleri. BSS, mobil cihazlar ve Mobil Operatör GSM Ağ anahtarlama sistemi arasındaki trafik ve işaretleşme bilgilerinden sorumludur [3]. |
| **BTK** | Bilgi Teknolojileri ve İletişim Kurumu. |
| **CDMA** | "Code Division Multiple Access". Radyo iletişim teknolojilerinde kullanılan Yayılı Spektrum temelli kanal erişim metodudur [4]. |
| **CDMA2000** | Ses, veri ve işaretleşme sinyalinin mobil cihaz ve Mobil Hücre siteleri arasında iletişimini sağlayan ve CDMA temelli 2.5G ve 3G teknolojisindeki sayısal Mobil Standardı [4]. |
| **CDMAone** | Ses, veri ve işaretleşme sinyalinin mobil cihaz ve Mobil Hücre siteleri arasında iletişimini sağlayan ve CDMA temelli II. Kuşak ilk sayısal Mobil Standardı. Diğer adları IS-95 ve TIA-EIA-95' dir [4]. |
| **EDGE** | "Enhanced Data Rates for GSM Evolution". GSM Mobil ana standardına gelişmiş veri transfer hızları ekleyen mobil telefon teknolojisi. EDGE teknolojisi 8 seviyeli PSK modülasyonu kullanır. |
| **Erişilebilirlik** | Bilişim Sistemi ve bilginin istendiğinde hizmet verilecek konumda sağlanması için gerekli mekanizma. |
| **Erişim Hakları** | Bilgisayardaki bir nesne üzerine kullanıcı, grup ve rollerin erişim seviyelerinin belirlendiği kurallar. |
| **ESHS** | Elektronik Sertifika Hizmet Sağlayıcısı. |
| **ESN** | "Electronic Serial Number". Mobil cihazların, bağlı olunan Mobil Operatörler tarafından aktivasyonunda kullanılan 32 bitlik kontrol numarası [5]. |
| **Gizlilik** | Bilginin durduğu ortamda, işlenmesinde ve iletiminde |

| | |
|---|---|
| | istenmeyen ve yetkisiz kullanıcıların görülmesini engellemesini sağlamak. |
| **GPRS** | “General Packet Radio System”. II. ve III. Kuşak Mobil İletişim sistemlerinde kullanılan paket temelli orta hızda mobil veri servisi sağlayan, IP, PPP ve X.25 bağlantılarını destekleyen servis [6]. |
| **GSM** | “Global System for Mobile Communications”. İşaretleme ve konuşma kanallarının sayısal olan, farklı operatörler arasında dolaşım imkanı sağlayan, veri iletişimine imkan sağlayan mobil telefon operatörleri tarafından kabul edilen Uluslararası “Global System for Mobile Communication” II. Kuşak standardı. |
| **Günlük** | “Log”. Olay ve aktivitelerin düzenli işlendiği dosya. |
| **IMEI** | “International Mobile Equipment Identity”. Uluslararası Mobil Cihaz Tanımlayıcı numarası. Her GSM ve UMTS Mobil telefonlarda bulunan ve bu cihazı diğerlerinden ayırt eden biricik numara [7]. |
| **IV** | “Initializing Vector”. Şifreleme algoritmalarında, aynı düz metnin aynı anahtarla şifrelenmesinde elde edilen şifre dizisi her durumda aynı olduğundan ve bu durumun güvenlik ataklarına karşı hedef oluşturması nedeniyle, bu zafiyeti önlemek için blok ve dizi düz metnin şifreleme öncesi bir bölümüne eklenen ve değiştirilebilen veri [8]. |
| **İnternet** | Dünya üzerinde sahipsiz, bilgi paylaşımı amacı ile ortaya çıkmış TCP/IP temelli bilgisayar ağı. |
| **İntranet** | Kurumun kendi çalışanlarının kullandığı bilgisayar şebekesi. |
| **Kapı Yazılımı** | Birbirinden farklı iki bilgisayar ortamının bağlanması için gereken sistem veya yazılım. |
| **Kaynak Kodu** | Bilgisayar makine diline çevrilmemiş ve derlenmemiş bilgisayar programı. |
| **Kimlik Denetimi** | Konunun nesneye kontrollü ve güvenli erişiminin sağlanması için gerekli bilgisayar önlemlerinin tümü. |

| | |
|---|---|
| **Klonlama** | “Clonning”. Herhangi bir şeyin aynısının kopyalanması işlemi. |
| **Korunmasızlık** | Bir varlık ve sürece ait olan, tehditlerin yararlanabildiği istenmeyen güvenlik açığı. |
| **Kriptografi** | Açık metin bilginin başkaları tarafından anlaşılmamasının sağlanması için matematiksel bir algoritma ve anahtar ile şifrelenmesini gerçekleştirilen yazılım ve donanım işlevleri. |
| **Kritik Bilgi** | Kurum için önemli bilgi. |
| **LAN** | “Local Area Network”. Yerel Alan Ağı. |
| **LDAP** | “Lightweight Directory Access Protocol”. İnternet ortamları için geliştirilmiş, Hiyerarşik Dizin Sistemlerine erişim protokol standardı. |
| **MIM Atağı** | “Man-In-The-Middle” saldırıları. Tüm iletişimin kötü amaçlı bir saldırgan tarafından kaynak ve hedef konuların bilgisi dışında iletişimin arasına girerek yönetildiği ve dinlenebildiği bir güvenlik saldırısı türü. |
| **MIN** | “Mobile Identification Number”. Mobil Operatörlerin, mobil cihazların tanımlanmasında kullandıkları 10 haneli biricik numara. MIN, TIA standartları ve PCS teknolojilerinin desteklediği mobil cihazlara özel biricik numara [9]. |
| **MMS** | “Multimedia Messaging Service”. Mobil Çoklu Ortam Mesajlaşma Hizmeti anlamına gelir. Cep telefonu ile fotoğraflı, sesli, animasyonlu ve videolu mesajların gönderilmesine olanak tanır. |
| **NSS** | “Network Sub System”. GSM şebekesinde anahtarlama ve PSTN-Mobil Cihaz arasındaki iletişimi sağlayan Mobil Operatörlere ait ağ bileşeni. NSS, GSM ana şebekesi olarak da adlandırılmakta olup genellikle devre anahtarlamalı yapıdadır ve Ses, SMS ve devre anahtarlamalı veri gibi geleneksel GSM bilgilerini işler [10]. |
| **Oturum Anahtarı** | Bir oturum süresince geçerli olan şifreleme anahtarı. |
| **Ön Bellek** | “Buffer Overflow”. Bilgisayar programının tahmin edilen ve |

| | |
|---|---|
| **Taşması** | tasarlanan yapısının zorlanarak aşırı bilgi sınırlarına karşı kendi bütünlüğünü ve güvenliğini kaybetmesine yol açan güvenlik zafiyeti. |
| **Özet Fonksiyon** | Açık metin üzerinden belli standartlara göre özetinin alınmasına yarayan algoritma. Özet bilgi geri çevrilemez. |
| **Parola** | Konuya özgü, başkaları tarafından bilinmemesi gereken ve konunun erişiminde kontrol edilen ek bilgi. |
| **Parola Kırma** | Parolanın başkaları tarafından öğrenilmesi için uygulanan yöntem ve metotlar. |
| **PCS** | "Personel Communication Service". 1900 Mhz aralığındaki sayısal Mobil servislerinden kullanılan Frekansı bandı. Bir diğer adı GSM-1800'dir [11]. |
| **PDA** | "Personel Digital Assistance". Bilgisayarla senkronize olabilen, saat, takvim, adres defteri, iş listesi işlevlerini içeren, işletim sistemi ile çalışan basit ve taşınabilir bilgisayar. |
| **PIN** | "Personel Identification Number". Kullanıcının sistemdeki kimlik denetiminin doğrulmasında kullanılan gizli ve sayısal numara. |
| **PKI** | "Public Key Infrastructure". Açık Anahtar Altyapısı. |
| **PSK** | "Phased Shift Keying". Faz Kaydırmalı anahtarlama modülasyonu. |
| **RADIUS** | "Remote Authentication Dial-In Service". Merkezi erişim, kimlik denetimi (yetkilendirme dahil) ve izlenebilirlik yönetimi temin eden ağ protokolü. |
| **Risk** | Bir tehdidin, açıklıktan yararlanma olasılığı. Risk, tehdit olasılığı ve korunmasızlık ile doğru orantılıdır. |
| **Risk Değerlendirmesi** | Riskleri ve olası hataları tespit etme işlemi. |
| **Risk Yönetimi** | Risk analizi ve riski azaltmak veya en aza indirmek için güvenlik gereklerinin seçimi ve bunun sürekli yönetilmesi işlemi. |

| | |
|---|---|
| **Saldırgan** | Korunmasızlıktan yararlanan kötü amaçlı iç ve dış kullanıcı. |
| **Sayısal İmza** | Sayısal Sertifika ortamlarında konuya ait, konunun kimlik denetlenmesi, bilgi bütünlüğünün doğrulanması ve inkâr edilemezlik prensiplerini içeren şifreli bilgi dizisi. |
| **Sayısal Sertifika** | İçerisinde konuya ait Genel Anahtar, Sertifika Otorite bilgisi, konuya ait seçkin ad, geçerlilik süresi gibi bilgiler içeren dosya. Sürümüne ve türüne (Nitelikli sertifika, X.509 V3 sertifikası v.b) göre ek bilgiler içerebilir. |
| **Sertifika Otoritesi** | Sayısal Sertifika üretimi ve yönetiminden sorumlu yazılım veya birim. |
| **SMS** | "Short Message Service". GSM Mobil iletişim sistemlerinde kullanılan, mobil telefon cihazları arasında 160 adet karakter ile iletişimin sağlandığı Mobil Kısa Mesaj Servisi. |
| **SOAP** | "Simple Object Access Protocol". Dağıtık uygulamalarda ve web servislerinin haberleşmesinde kullanılmak üzere tasarlanan, XML mesaj formatı kullanan, istemci/sunucu mantığına dayalı nesne erişim protokolüdür. |
| **Solucan** | Bir sistemden diğerine kendi kendine çoğalarak üreyen zararlı yazılım kodu. |
| **SPAM** | İnternet üzerinde aynı mesajın veya bilginin yüksek sayıdaki kopyasının, bu tip bir mesaji alma talebinde bulunmamış kişilere gönderilmesi. |
| **SSL** | "Secure Socket Layer". HTTP trafiğinin güvenliğini sağlamak üzere geliştirilmiş uçtan uca sadece OSI Aktarma katmanına kadar veri bütünlüğünün ve Kimlik Denetimin sağlandığı güvenlik iletişim protokolü. |
| **SSO** | "Single Sign On". Kullanıcının tek bir kullanıcı adı ve parola girişi yaparak, yetki sahibi olduğu tüm bilgisayar ve sistemlere tekrar parola girişi ihtiyacı doğmadan erişiminin sağlanabildiği yöntem. |
| **Sunucu** | Üzerinde bulunduğu ağdaki kullanıcıların ortak bilgi veya |

| | |
|---|---|
| | programları paylaştığı yazılım veya donanım. |
| **Tehdit** | Korunmasızlıktan yararlanan, istenmeyen süreç veya kullanıcı. |
| **Tehdit Analizi** | Tehditlerin belirlenmesi ve sınıflandırılması işlemi. |
| **Test Ortamı** | Geliştirilen yazılımların veya süreçlerin sınandığı donanım ve yazılım ortamı. |
| **TIA** | "Telecommunication Industry Association". Telefon ve veri iletişimi alanlarında standartlar üreten, 600 civarında iletişim firmasını temsil eden, merkezi ABD'de bulunan küresel ticari bir organizasyon. |
| **TKIP** | "Temporal Key Integrity Protocol". IEEE 802.11 kablosuz iletişim standardında kullanılan güvenlik protokolü. |
| **UICC** | "Universal Integrated Circuit Card". GSM ve UMTS ağında kullanılan akıllı kart. |
| **UMTS** | "Universal Mobile Telecommunications System". Diğer bir adı 3GSM olan , 4G Mobil teknolojisi tarafından da kullanılacak olan, havadaki ara yüz olarak W-CDMA kullanan 3. kuşak Mobil Ağ Teknolojisi [12]. |
| **Veri Bozulması** | Verinin ilk üretildiğinden beri yetki dışı veya arıza ile değişmesi. |
| **Virüs** | Çoğalması için bir dosya veya nesneye ihtiyaç duyan zararlı yazılım kodu. |
| **VLAN** | "Virtual Local Area Network". Sanal Yerel Alan Ağı. |
| **VPN** | "Virtual Private Network". Bilişim ağlarına güvensiz iletişim ortamlarından ve uzaktan güvenli olarak bağlanma olanağı sağlayan teknoloji (Sanal Özel Ağ). |
| **VTYS** | Veri Tabanı Yönetim Sistemi. |
| **WAN** | "Wide Area Network". Geniş Alan Ağı. |
| **WAP** | "Wireless Application Protocol". Telsiz Uygulama Protokolü. Düşük bant genişliği ve yüksek gecikme süreli telsiz cihazların iletişiminde kullanılan uygulama katmanı iletişim protokolü WAP-1 ve WAP-2 türleri vardır. |

| | |
|---|---|
| **WEB** | “World Wide Web”. |
| **Web Tarayıcısı** | İnternet WEB ortamına erişim sağlayan kullanıcı yazılımı. |
| **WEP** | “Wired Equivalent Privacy”. Kablosuz ağ bağlantılarında çalışan şifreleme yöntemi. |
| **WI-FI** | “Wireless Fidelity”. IEEE 802.11 telsiz teknolojilerini kullanan, farklı telsiz cihazların birlikte çalışabilmesi için oluşturulmuş akreditasyon standardı ve bu teknolojideki telsiz iletişim ağı [13]. |
| **WIMAX** | “World Interoperability for Microwave Access”. IEEE 802.16 telsiz standardını kullanan farklı telsiz cihazlarının birlikte çalışabilmesi için oluşturulmuş akreditasyon standardı ve yüksek hızda İnternet bağlantısı sunan kablosuz teknolojisi [14]. |
| **WLAN** | “Wireless Local Area Network”. Kablosuz Yerel Alan Ağı. |
| **WTLS** | “Wireless Transport Layer Security”. Kablosuz Aktarım Katmanı Güvenliği. WAP iletişimi için mahremiyet, veri bütünlüğü ve kimlik denetimi güvenlik özelliklerini sağlayan WAP protokolü. |
| **Yama** | Hata düzeltmek ve güvenlik açığını kapatmak için geliştirilen ek yazılım. |
| **Yama Yönetimi** | Yamaların kontrollü yapılması için gerekli kurallar dizisi. |
| **Zararlı Kod** | Güvenliği tehlikeye sokan, genelde taşınabilir yazılım parçası. |

# Şekiller



# Tablolar

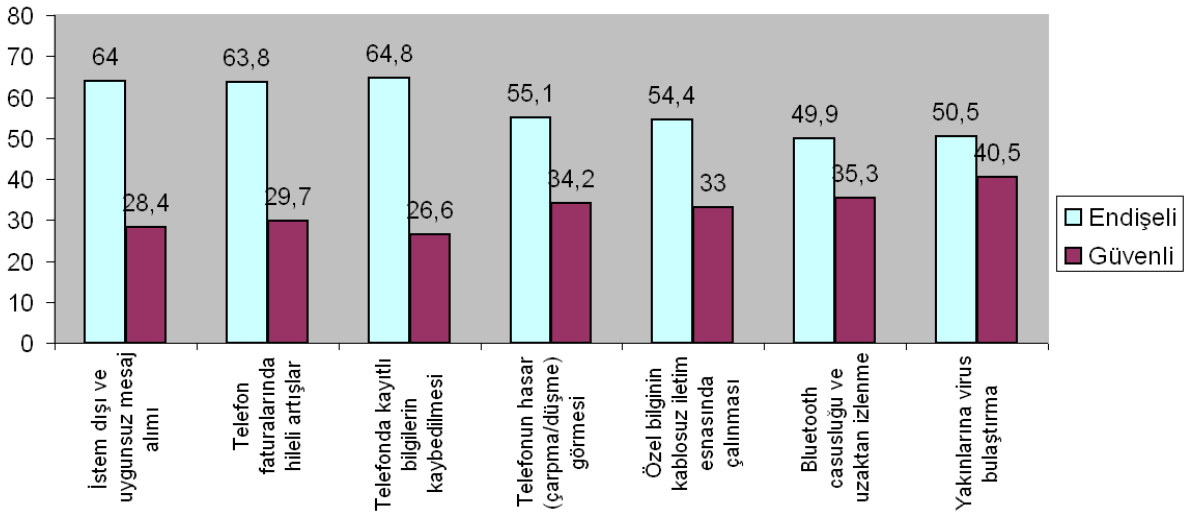
# 1 MOBİL UYGULAMA GÜVENLİĞİ

## 1.1. Giriş

Günümüzde, mobil teknoloji günlük yaşamın ayrılmaz bir parçası haline gelmiştir. Cep telefonu başta olmak üzere dizüstü bilgisayar, PDA gibi taşınabilir cihazların yetenekleri gün geçtikçe gelişmekte, buna paralel olarak bu tür mobil cihazlara bağımlılık artmaktadır. Kişisel bilgiler, e-posta içerik ve adresleri, özel telefon numaraları gibi hassas verilerin mobil cihazlarda saklanma eğilimi artmakta ve adeta bir kişisel bilgisayar gibi kullanılabilmektedir. Kişisel bilgisayarlara özgü saldırı tiplerinin yanında, mobil olma özelliğinden kaynaklanan ek güvenlik tehditlerinin ve saldırı girişimlerinin de olması, mobil uygulamalarda güvenliğin önemini daha da artırmaktadır. Tüm bu gelişmeler bilişim güvenliği kapsamında mobil güvenliğin ayrı olarak ele alınmasını zorunlu hale getirmiştir.

Mobil teknoloji kullanıcılara yaşamı kolaylaştıran önemli faydalar sunmaktadır. Mobil ticaret, mobil bankacılık, uzaktan erişimin mobil hale gelmesi ilk akla gelen güncel yeniliklerden sadece birkaç örnektir. Ancak, mobil teknolojinin sağladığı esneklik ek güvenlik risklerini de beraberinde getirmektedir. Bu riskler, mobil cihazların taşınabilir fiziksel özellikleri nedeniyle bizzat kendileri olmakla birlikte kullanım şeklinden kaynaklanan unsurları da kapsamaktadır. Bir restoranda veya takside unutulan bir cep telefonunun içerisindeki bilgiler şifre ile korunmuş olsa dahi cihazın ve bilgilerin tekrar yerine konma maliyetinin dikkate alınması gerekmektedir. Birçok kullanıcının kullanım kolaylığını kaybettiği düşüncesiyle PIN kodu kullanmadığı, hassas bilgilerini şifrelemediği bir mobil cihazın çalınma veya kaybolmasının açacağı olumsuz sonuçlar kolaylıkla tahmin edilebilir. Kurumsal açıdan değerlendirildiğinde ise, yeterli güvenlik önlemleri alınmamış bir mobil cihaz ile işyerindeki hizmet sunucularına bağlanan kullanıcının bilgilerine erişebilen bir saldırganın kurum için oluşturabileceği tehdidin maliyeti parayla dahi ölçülemeyebilir [15, 16, 17, 18].

Bir güvenlik firmasının 2008 yılında yayınladığı Mobil Güvenlik Raporu [19], mobil cihazların karşı karşıya kaldığı riskler konusunda kullanıcı bilincinin arttığını ortaya koymaktadır. Rapor, kullanıcıların yaklaşık %86'sının cep telefonlarında maruz kalabileceği hileli fatura artışları, bilgi kaybı ve hırsızlık gibi güvenlik riskleri konusunda endişe taşıdığını ortaya koymaktadır. Bilinçli olarak korunmasız cihaz kullanım oranı %79 iken, kullanıcıların %15'i güvenlik düzeyi konusunda emin değillerdir. Yapılan araştırma, tüketicilerin güvenli mobil araç ve servislerin sağlanması konusunda şebeke operatörlerinin sorumluluk almasını beklemektedir. Şekil 1'de, araştırma sonucunda mobil telefon kullanıcılarının güvenlik endişesi taşıdığı konuların dağılımı gösterilmektedir.




**Şekil 1: Mobil Telefon Kullanıcı Endişelerinin Konulara Göre Dağılımı (%)**

Geçmişte, mobil cihazların üzerindeki yazılımların özel olması, üzerlerinde bir işletim sistemi bulunmaması veya mevcut işletim sistemlerinin cihaza özel tasarlanmış olması, bu yazılımlar ile ilgili yaygın bilgi olmaması tehdit sayısını oldukça sınırlı tutmuştur. Ancak son dönemlerde farklı işletim sistemi, uygulama ve iletişim protokolleri ile çalışan mobil cihazlar daha fazla tehdide maruz kalmaktadır.

Hazırlanan bu belgede, mobil cihazların güvenlik unsurları detaylı olarak ele alınmıştır. Mobil ortamın doğası nedeniyle ortaya çıkan güvenlik açısından zorlayıcı kısıtlar (taşınabilir olması nedeniyle kontrol zorluğu, işlemci ve bellek gibi kaynak yetersizliği v.b.) göz önüne alınarak, olası tehditler, riskler ve alınabilecek önlemler iyi uygulama örnekleri ile anlatılmıştır. Birçok alanda olduğu gibi mobil güvenlik konusunda da standart kullanımının yararlarına değinilmiş ve bu konuda uluslararası grup ve organizasyonların çalışmalarından bahsedilmiştir. Ayrıca, özel sektörde olduğu gibi, kamu kurum ve kuruluşlarının vatandaşlara ve diğer kamu kurum ve kuruluşlara verdiği hizmetlerin mobil ortama taşınması konusunda yaptıkları çalışmalar (mobil devlet) hakkında bilgi verilmiştir. Son bölümde ise, gelecekte mobil uygulamaların sahip olacakları gelişmiş işlevsel özellikler gelecekteki mobil teknoloji ve güvenlik özellikleri açısından değerlendirilmiştir.

## 1.2. Kapsam

Raporda, *mobil uygulama*, taşınabilir cihazlarda (cep telefonu, dizüstü bilgisayar, PDA, akıllı cep telefonları gibi) koşan ve buna bağlı telsiz ve mobil iletişim ortamlarını kullanan uygulama olarak ele alınmış olup; *mobil uygulamalarda güvenlik* bu ortam ve cihazlardaki bilgilerin gizlilik, erişebilirlik ve bütünlüğünün sağlanmasına yönelik risklerin belirlenmesi ve buna karşı alınabilecek önlemler bütünü olarak değerlendirilmiştir.

Mobil uygulamalarda güvenlik kapsamında aşağıdaki hususlar temel olarak yer almakta olup bu belgenin içeriğini oluşturmaktadır:

- Mobil cihazların fiziksel ve sistem güvenliği,
- Mobil cihazlarda saklanan bilgi ve verilerin güvenliği,
- Mobil cihazlarda koşan uygulamaların güvenliği,
- Mobil cihazlara yönelik geliştirilen kablosuz iletişim ağı protokol ve teknolojilerinin (Bluetooth, WiFi, WIMAX, 3G, 4G gibi) güvenliği,
- Mobil uygulamanın koştuğu sunucu, kapı geçidi (gateway) ve altyapı güvenliği.

# 2 MOBİL UYGULAMALARIN KULLANDIĞI TEKNOLOJİ, İLETİŞİM PROTOKOLLERİ VE GÜVENLİK ÖZELLİKLERİ

Bu bölüm, mobil uygulamaların koştuğu ortamın gereksinimi olan dünya üzerinde kullanılan önemli teknoloji ve iletişim protokolleri ve bunlara ait güvenlik özelliklerini içermektedir.

## 2.1. Mobil Telekom Teknolojileri

Mobil Telekom sektöründe ikinci kuşak teknolojilerdeki gelişmeler tamamlanmış ve üçüncü kuşak teknolojilerin kullanımına geçilmeye başlanmıştır. Dünyada üçüncü kuşak teknolojilerin kullanımı Asya-Pasifik ülkelerinde 2002 yılında, Avrupa ülkelerinde kullanılmasına ise 2004 yılında başlanmıştır. Sektör ülkemizde, IP tabanlı 3.kuşak teknolojilere geçiş aşamasındadır.

3. Kuşak Teknolojileri ile birlikte;

- IP tabanlı ağ yapısı sayesinde daha hızlı ve çeşitli İnternet tabanlı uygulamaların mobil ortamda kullanımına olanak sağlanacaktır.
- Geniş ağ yapısında binlerce ağ ve milyonlarca abone bağlantısı olanağı sağlanabilecektir.

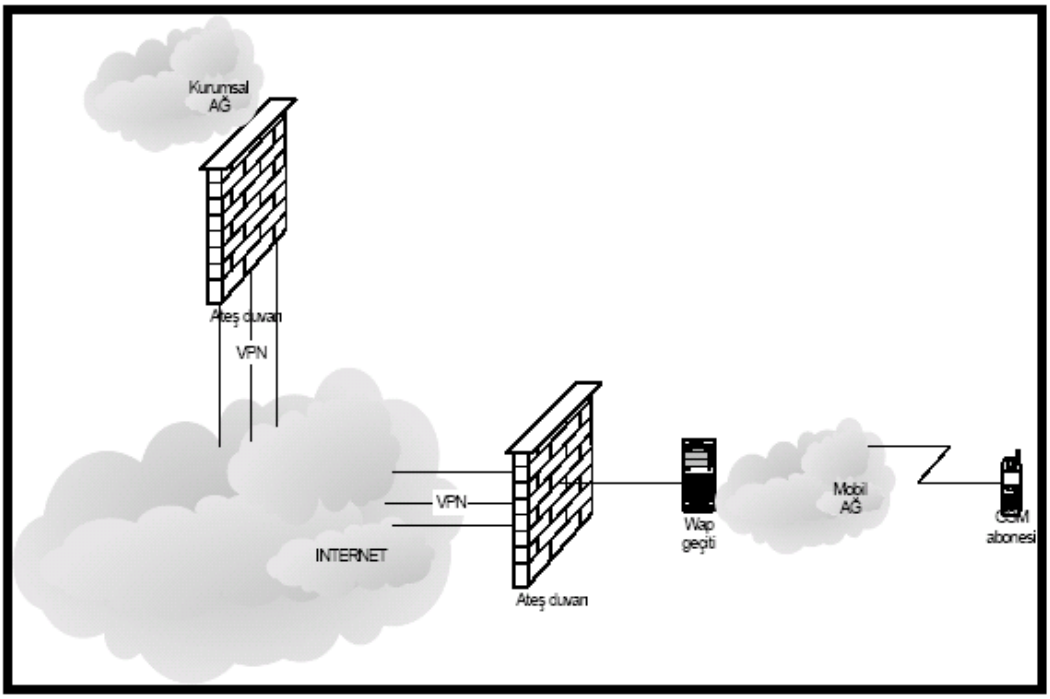
Tablo 1'de günümüzde kullanılan Mobil Teknolojilere yönelik açıklamalar gösterilmektedir.

**Tablo 1: Mobil Teknolojiler**

| Kuşak | Teknolojiler | Açıklama |
|---|---|---|
| 2 Kuşak | GSM, CDMA, TDMA | SMS ve WAP teknolojileri |
| 2 ½ Kuşak | GPRS/EDGE | 2001 yılında, hız ve daha geniş servis özelliği |
| 3. Kuşak | UMTS | 2002 yılında, Geniş bant mobil veri iletişimi özelliği |
| 4. Kuşak | UMTS, IEEE 802.21, EDGE, 3PPP Sürüm 10 | 2012 yılından sonra, IP temelli , yüksek hızlı (100Mbit/s ve 1 Gbit/s) ve yüksek kaliteli İnternet hizmetleri |

2. Kuşak kapsamında WAP ve SMS teknolojileri ile İnternet tabanlı hizmetlerin birçoğu kullanılamamaktadır (Bknz. Şekil 2). Bu iki teknoloji, sahip olduğu güvenlik açıklıkları

nedeniyle özellikle bankacılık uygulamalarında kısıtlı olarak kullanılabilmektedir. 3. Kuşak teknolojilerin kullanılmaya başlanmasıyla birlikte daha etkin güvenlik çözümlerine ihtiyaç duyulacaktır.




**Şekil 2: WAP Erişim Kontrolü**

4. Kuşak; ses, veri, çoklu ortam mesajlaşma (MMS) ve yüksek çözünürlüklü televizyon hizmetlerinin yüksek hızla, daha güvenli ve yüksek kaliteli olarak mobil ortamlarda iletilmesine olanak sağlayacak gelecek teknolojisidir.

## 2.2. IEEE 802.11 Kablosuz Ağ İletişim Protokolleri

Kablosuz bilgisayar iletişiminde kullanılan 2.4, 3.6 ve 5 GHz radyo frekanslarında çalışan bir dizi iletişim protokol standardı olan IEEE 802.11, son yıllarda kullanılan birçok telsiz iletişim protokolleri ve teknolojilerinin kaynağıdır.

802.11, telsiz bağlantılarda, özellikle lisanssız endüstriyel, bilimsel ve tıbbi (industrial scientific medical – ISM) frekans bandında radyo frekansının (*RF*) nasıl kullanılacağını tanımlayan, IEEE tarafından yayınlanmış bir standarttır.

Standart ilk olarak 1997 yılında 2.4 Ghz bandında 1-2 Mbps veri transfer hızı öngörülerek yayınlanmıştır. Günümüze gelene kadar standardın 802.11a, 802.11b, 802.11g ve taslak 802.11n sürümleri yayınlanmıştır.

Söz konusu standartların veri transfer hızlarını etkileyen unsur, kullandıkları modülasyon teknikleridir. DSSS (Direct Sequence Spread Spectrum) ve OFDM (Orthogonal Frequency Division Multiplexing) olarak adlandırılan tekniklerden DSSS, OFDM'e göre daha basit ve uygulaması daha ucuzdur. OFDM ise veri transfer hızını arttıran bir tekniktir.

IEEE 802.11a, 5 GHz bandında OFDM modülasyon tekniği ile çalışmaktadır. 802.11b, 2.4 GHz ISM bandında DSSS modülasyon tekniğini kullanarak 1, 2, 5.5 ve 11 Mbps veri transfer hızlarında çalışır. 802.11g ise aynı bantta OFDM modülasyon tekniğini kullandığından daha yüksek veri transfer hızlarına (6, 9, 12, 18, 24, 48 ve 54 Mbps) ulaşabilmektedir. 802.11g aynı zamanda DSSS tekniği kullanımına da imkan vererek 802.11b ile geriye doğru uyumludur.

2.4 GHz bandının daha yüksek frekanslara göre bir takım avantajları bulunmaktadır. Bunlar arasında daha iyi menzile sahip olması ve yayınının, örneğin beton duvar gibi nedenlerle, kolaylıkla engellenememesi sayılabilir. Ancak, 2.4 GHz bandında çalışan pek çok cihaz olması sebebiyle bu banttaki iletişim, elektromanyetik etkileşime ve karıştırmaya (enterferans) maruz kalabilmektedir.

802.11n, henüz taslak bir standarttır. İlave güç veya RF bandı tahsis edilmeden veri aktarım hızının ve menzilinin arttırılması amacıyla bu standartta uç noktalarda birden fazla radyo ve anten kullanılmaktadır. Bunların her biri aynı frekansta birden çok akım oluşturarak yayın yaparlar. MIMO (multiple input/multiple output) teknolojisi ile yüksek veri transfer hızında bir akım aslında düşük hızdaki birden fazla akımın aynı anda yayınlanmasıyla oluşturulur. Standardın aktif ancak onaylanmamış 7. taslak sürümü Eylül 2008'de yayınlanmıştır. Tablo 2'de IEEE 802.11 standartlarına ait sürümlerin özellikleri sunulmuştur.

Orijinal 802.11 standardında güvenlik için iki tip kimlik denetimi tanımlanmıştır. Bunlar açık kimlik denetimi ve WEP anahtarlı kimlik denetimidir. Açık kimlik denetiminde herhangi bir şifreleme metodu kullanılmaz ve güvenlik açısından oldukça zayıftır. WEP ise telsiz bağlantı güvenliğini bir kablolu bağlantıya denk hale getirmek için düşünülmüş bir kimlik denetimi türüdür. Basit bir şifreleme metodu kullanılır, parolalar statiktir ve kolayca kırılabilirler.

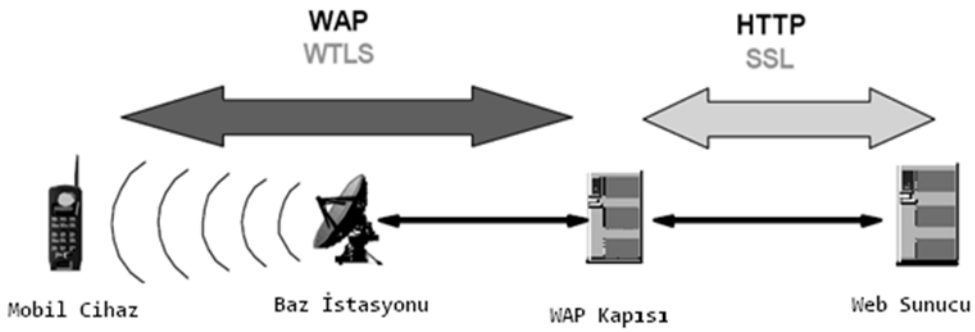
WAP, mobil hücresel telefon gibi kısıtlı kaynağa sahip mobil ve telsiz cihazların iletişim protokolüne ait WTLS, WAP iletişimi için veri bütünlüğü, mahremiyet ve kimlik denetimi güvenlik özelliklerini sağlamaktadır.

**Tablo 2: IEEE 802.11 Protokolleri ve Özellikleri**

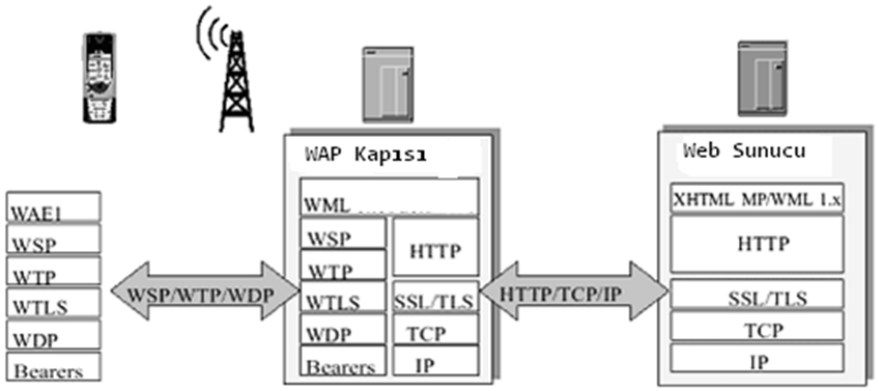
| | 802.11a | 802.11b | 802.11g | | 802.11n |
|---|---|---|---|---|---|
| **Bant** | 5.7 GHz | 2.4 GHz | 2.4 GHz | | Doğrulanmamıştır Muhtemelen 2.4 ve 5 GHz bantları |
| **Kanallar**[1] | 23'e kadar | 3 | 3 | | |
| **Modülasyon** | OFDM | DSSS | DSSS | OFDM | MIMO-OFDM |
| **Veri Transfer Hızı** | 54 Mbps'e kadar | 11 Mbps'e kadar | 11 Mbps'e kadar | 54 Mbps'e kadar | İki akımlı MIMO için 248 Mbps olacağı düşünülmektedir |
| **Menzil** | ~35 m | ~38 m | ~ 100 m kadar | | ~300 m kadar |
| **Yayınlanma Tarihi** | Ekim 1999 | Ekim 1999 | Haziran 2003 | | Eylül 2008 (7. Taslak sürüm) |
| **Avantaj** | - Hızlı,<br>- Enterferans daha az | - Düşük maliyet,<br>- iyi menzil | - Hızlı,<br>- İyi menzil,<br>- Engellerden kolaylıkla etkilenmez | | - Çok iyi veri transfer hızı,<br>- Gelişmiş menzil |
| **Dezavantaj** | - Yüksek maliyet<br>- Daha kısa menzil | - Yavaş,<br>- Enterferans'a müsait | - 2.4 GHz bandında çalışan diğer cihazlarla enterferans'a girebilir | | |

[1] Üst üste binmeyen kanallar

İlk yıllarda kullanılan WAP protokolü (WAP-1) Şekil 3'de gösterildiği üzere WAP kapılarında protokol çevrimine (Bknz. Şekil 4) tabi tutulmaktadır.




**Şekil 3: Standart WAP Mimarisi**



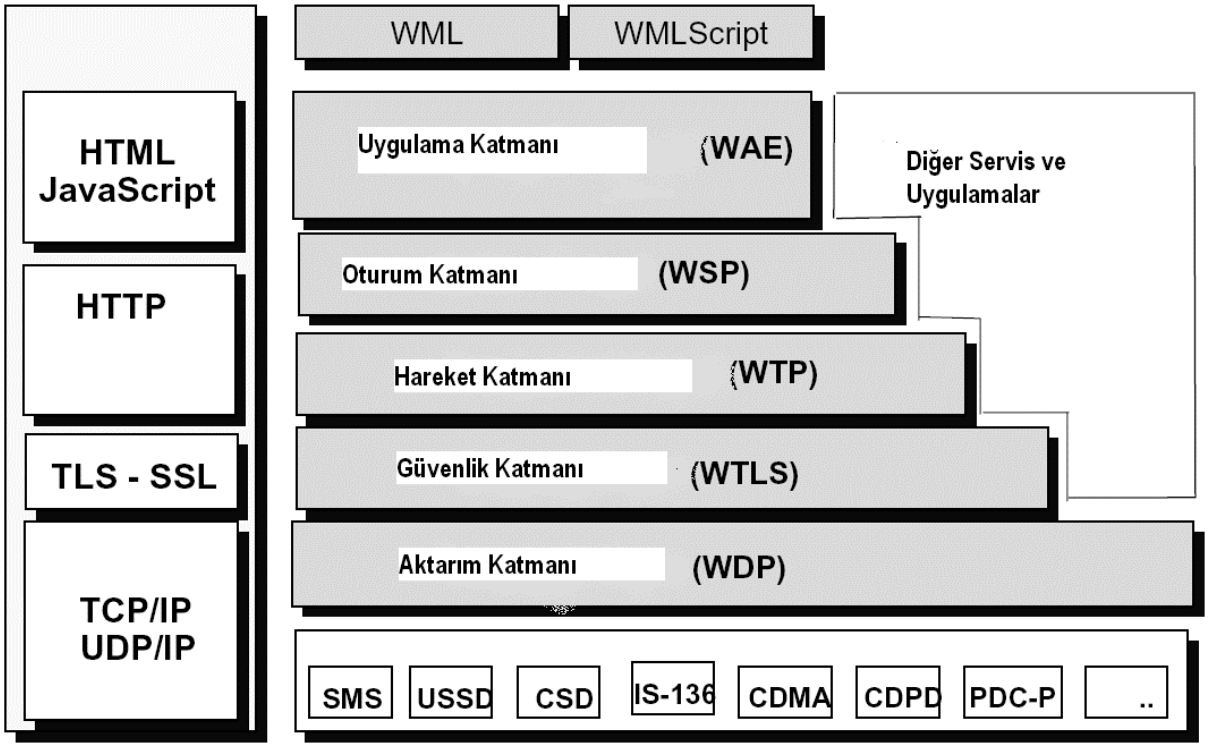

**Şekil 4: WAP – HTTP Çevrimi**

Şekil 4 'ün, OSI katmanlarındaki protokol dizilişi ise Şekil 5'de gösterilmektedir.

İlk yıllarda kullanılan WAP-1 protokolü'nde görülen güvenlik eksikleri aşağıda sıralanmıştır:

- Şifrelenen mobil cihaz veya sunucu bilgisinin WAP kapılarında deşifre edilmesi ve tekrar şifrelenmeye gereksinim duymaktadır.
- Uçtan uca güvenliğin sağlanması mümkün olmadığından, trafik MIM ataklarına maruz kalmaktadır.

- Bağlantının SSL/TLS bölümünün kontrol edilmesi mümkün değildir.
- WAP kapı yazılımlarında güvenlik problemleri ile karşılaşılması söz konusudur.




**Şekil 5: WAP OSI Katmanları Protokol Dizilişi**

Bu problemlerin giderilmesi amacı ile 2002 yıllarında ortaya çıkan WAP-2, WTLS (güvenlik katmanı) ile aşağıda özellikler desteklenmiştir:

- *Veri bütünlüğü:* Mobil cihaz ve WAP kapısı arasında trafiğin, mesaj kimlik denetimi sayesinde yetkisiz olarak değişmediği,
- *Veri gizliliği:* Şifreleme olanakları kullanılarak mobil cihaz ve WAP kapısı arasındaki trafiğin üçüncü taraflar tarafından görünememesi,
- *Kimlik denetimi:* Sayısal sertifika kullanılarak hedef ve alıcı arasında kimlik denetiminin gerçekleştirilmesi.

2003 yılında IEEE 802.11i standardına bağlı olarak WPA (Wi-Fi Protected Access) kablosuz ağlar için güvenlik modeli yayınlanmıştır. Standart tabanlı bir model olması ve gelişmiş şifreleme tekniğinin bulunması, bu modeli güçlü bir kimlik denetleme mekanizması haline getirmiştir. Günümüzde ise 802.11i/WPA2, kullanılması gereken standart olarak kabul

görmektedir. Bu standartta, WPA'de kullanılan TKIP şifreleme metodu yerine daha gelişmiş AES şifreleme metodu kullanılmaktadır.

## 2.3. Wi-Fi ve 802.11 Telsiz Yerel Alan Ağı Güvenliği

Wi-Fi, kablosuz İnternet ve ağ bağlantısı sağlayan bir teknolojidir. WiFi destekli dizüstü bilgisayarlar ve PDA'lar, kablosuz erişim noktalarına ve buna bağlı olarak İnternete bağlantı sağlayan teknolojidir.

Wi-Fi uyumlu cihazlar, PDA'ler ve diğer taşınabilir cihazların yakınlarındaki kablosuz erişim noktaları aracılığı ile yerel alan ağına bağlanabilmesini sağlar. Bağlantı, kablosuz erişim noktaları ve cihazın ortak desteklediği IEEE 802.11 protokolünün a, b, g ve n sürümlerine bağlı olarak 2.4 GHz veya 5 GHz radyo frekansında gerçekleştirilir. Wi-Fi'ın sağladığı yararlar aşağıda belirtildiği gibi özetlenebilir:

- Wi-Fi, diğer kablosuz bağlantı teknolojilerine göre daha ucuz ve kullanımı kolaydır.
- Ağ bağlantısı için kablo gereksinimi yoktur.
- Özel lisans istemeyen frekanslarda çalışır.
- WEP, WPA, WPA2 gibi şifreleme, IEEE 802.11x gibi kimlik yetkilendirme güvenlik olanaklarını kullanabilir.

Buna karşılık aşağıdaki dezavantajları barındırmaktadır:

- Wi-Fi uyumlu cihazlar, diğer kablosuz cihazlardan etkilenebilir ve birbirlerinin iletişimini engelleyebilirler (Lisans gerektirmeyen frekans aralığının kullanılması nedeni ile).
- Wi-Fi uyumlu cihazlarda güç tüketimi daha yüksektir.
- Standardın uluslararası düzenlemelerinde bazı farklılıklar söz konusu olabileceğinden farklı ülkeler için üretilen Wi-Fi uyumlu cihazların bazı kanallarında iletişim sorunları çıkabilir.
- 2.4 GHz bandındaki 802.11b ve g uyumlu Wi-Fi cihazlarının iletişimi, aynı frekans bandında çalışan telsiz, bluetooth veya benzer radyo frekansındaki cihazlar tarafından engellenebilir.

Radyo Frekansı ile iletişimde bulunan telsiz ağlardaki radyo frekansı, ortama yapılan yayının birden fazla ağ şebekesi ve bileşeni tarafından alınmakta ve dolayısı ile telsiz ağ sinyalini hangi cihazın ve ağ bileşenin aldığını kontrol etmek mümkün olmamaktadır. Bundan

dolayı, 802.11 telsiz yerel ağlarında yazılım temelli link seviyesinde, özellikle şifreleme konusunda güvenlik önlemleri alınmaktadır.

### 2.3.1. Erişim Kontrol Listesi Önlemi

802.11 telsiz ağlarında kullanılan *Erişim Kontrol Listesi* kısıtlaması, bilinmeyen ve yetkisiz kullanıcıların filtrelenmesi esasına dayalıdır. Bu amaçla, yerel ağ erişimine izin verilen cihazların MAC adresi Telsiz Erişim Noktasına baştan tanımlanarak sadece tanımlı MAC adres cihazları yerel ağa bağlanmasına izin verilir. Bu güvenlik yönteminde, ağ bazında mobil cihazın kimliği denetlenmekte olup, cihazdaki verilerin gizliliği, bütünlüğü ve erişilebilirliği ile kullanıcıların izlenebilirliği ve mahremiyeti gibi ek güvenlik hususlar karşılanamaz.

### 2.3.2. WEP Güvenliği

802.11 ağlarının ilk evrelerinde kullanılan WEP (Wired Equilavance Privacy)'in amacı, veri trafiğinin gizliliğini ve bütünlüğünü sağlamaktır. Bu amaçla, veri paketlerinde 64 bit veya 128 bit RC4 simetrik akış şifreleme metodu kullanılmaktadır. Başka bir deyişle, telsiz veya mobil cihaz ile Telsiz Erişim Noktası arasında bir gizli anahtar (64 bit RC4'de 5 ASCII karakter uzunluğunda, 128 bit RC4'de 13 ASCII karakter uzunluğunda) belirlenmekte ve bu anahtar ile veri trafiği şifrelenmektedir. İlgili Telsiz Erişim Noktasına bağlanacak tüm taşınabilir ve telsiz cihazlar aynı gizli anahtarı kullanmak zorundadır.

İlk kullanıldığı yıllarda güvenli olduğu varsayılan WEP gizli anahtarının sonraki yıllarda kırılabilmesinin tespit edilmesi nedeniyle, algoritması bilinen RC4 ile veri trafiğini yetkisiz olarak ele geçirmek ve ağa yetkisiz olarak bağlanmak mümkün olmaktadır.

Gizli parolanın elde edilmesine ek olarak, WEP ile korunmuş ağa yapılabilecek bir diğer saldırı türü, IV (Initializing Vector) çarpışması ile şifrelenmiş bilginin deşifre edilmesidir.

WEP güvenliğini iyileştirmek için takip eden yıllarda aşağıda belirtilen güvenlik eklentileri yapılmıştır:

- WEP2 ve WEP+ protokolleri yukarıda belirtilen güvenlik zafiyetlerini gidermek maksadı ile devreye alınmıştır. Ancak, WEP2 daha sonra kaldırılmış, WEP+ ise IV zafiyetini diğer ataklara karşı kesin bir çözüm olmadığı tespit edildiğinden kısıtlı bir kullanımda kalmıştır.
- Dinamik olarak gizli anahtarın değiştirildiği Dinamik WEP yöntemi kullanılmıştır. Sürekli ve kısa sürelerle gizli anahtarın değişimi için gerekli olan otomatik anahtar üretim mekanizması WEP'de yer almadığından dolayı IEEE 802.11i'de yer alan TKIP protokolünden (WPA) yararlanılmıştır [20].

### 2.3.3. WPA ve WPA2 Güvenliği

WEP de yer alan güvenlik zafiyetlerinin giderilmesi amacıyla IEEE 802.11'de tanımlı WPA ve WPA2 güvenlik protokolleri kullanılmaya başlanmıştır. WPA, eski ve WEP destekli telsiz erişim noktası cihazları ve ağ kartları ile uyumlu olmasına rağmen, WEP'de yaşanan IV güvenlik zafiyetini gidermek amacı ile devreye alınmıştır. WAP2, IEEE 802.11i standardının zorunlu güvenlik protokolü olup, daha güvenli AES şifreleme algoritması kullanmaktadır. Günümüzde Wi-Fi uyumlu tüm cihazlar için WPA2 zorunlu olarak desteklenmesi gereken bir güvenlik protokolüdür.

Wi-Fi çalışma grubu tarafından, Wi-Fi uyumlu farklı model cihazların birbirleriye uyumluluğunu sağlamak amacıyla EAP (Extensible Authentication Protocol) sertifikasyon türleri tanımlanmıştır [21].

### 2.3.4. IEEE 802.11x Güvenliği

Çoğunlukla Wi-Fi ağlarının güvenliği için kullanılan IEEE 802.11x, aynı zamanda sabit ağların güvenliği için de kullanılabilmektedir. IEEE 802.11x güvenlik çerçevesinde temel olarak aşağıdaki bileşenler yer almaktadır:

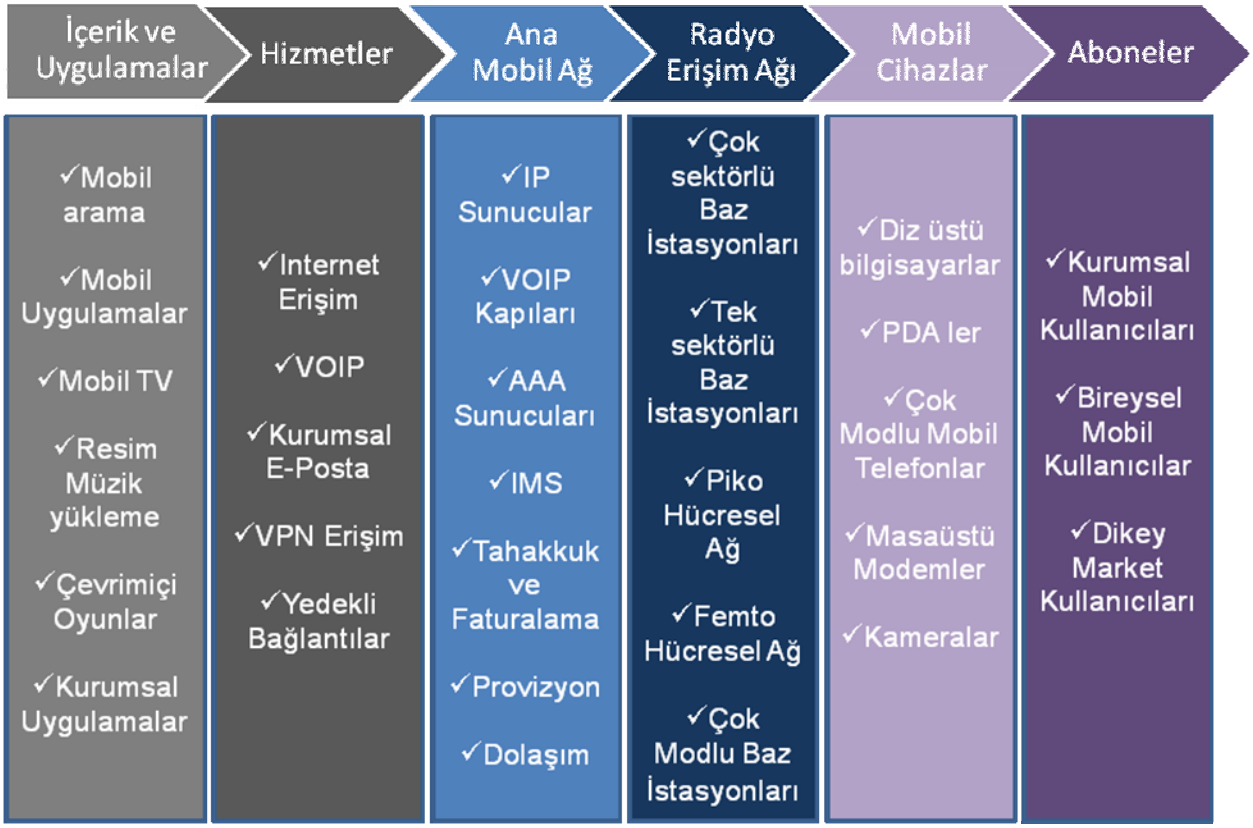
- *İstemci (Sabit veya Mobil):* Standarda göre istemci, üzerinde IEEE 802.11x uyumlu yazılım ve EAP protokolünü kullanan istemci yazılımına sahip olmalıdır.
- *Kimlik Denetleyici:* İstemcinin ilk bağlandığı ağa erişimini temin eden WAP Telsiz erişim noktası veya IEEE 802.11x uyumlu LAN anahtarıdır.
- *Kimlik Denetleme Sunucusu:* Gerçek kimlik denetleme servisinin koştuğu, bağlanan kullanıcıları kimlik ve parola ile denetleyen ağ bileşenidir. IEEE 802.11x standardı kapsamında, Kimlik Denetleme Sunucusu için RADIUS gereklidir.
- *Port Erişim Noktası:* Bağlanılan port ile kimlik denetleme protokolü ve algoritma ile ilgili işlemlerin çalıştırıldığı, EAP mesajlarının gidip geldiği istemci ve Kimlik Denetleme portudur.
- *EAP:* IEEE 802.11x standardında, telsiz erişim ağı için EAPOW (EAP over Wireless), sabit LAN ağı için EAPOL (EAP over LAN) kapsülleme metodu kullanılmaktadır.

IEEE 802.11x, ağa erişim için güvenli kimlik denetimi yapmakta, sadece ilk bağlantı anında kimlik denetimi yapıldığı için bağlantıdan sonra MIM atakları söz konusu olabilmektedir. Bu nedenle, daha güvenli bir kimlik denetimi için IEEE 802.11x'in IPSec protokolü ile desteklenmesi önerilmektedir.

IEEE 802.11x, kimlik denetiminde yetkisiz ağ erişimini engellemekte, ancak yetkili kullanıcının trafiğini kontrol edememektedir. Bundan dolayı, yetkili kullanıcıların ağ içindeki güvenlik yönetimi için IEEE 802.11x'e ilave önlemler alınmalıdır. Ek olarak, IEEE 802.11x'in mevcut güvenlik teknolojileri tamamlayıcı nitelikte olduğu unutulmamalıdır [22].

## 2.4. WIMAX

IEEE tarafından 802.16e:2005 standardı olarak tanımlanan WIMAX, IP temelli İnternet erişim teknolojisi olarak tasarlanmıştır. WIMAX teknolojisinde amaçlanan hem sabit hem de mobil uygulamalar için Servis kalitesinin yükseltilmesi ve aynı zamanda güvenliğin sağlanması amaçlanmıştır. WIMAX'ı diğer telsiz teknolojilerinden ayıran özellikler olarak; tamamı ile IP temelli mevcut ürün, cihaz ve servisleri taşıyabilmesi, hücresel ağlardan daha basit ve daha az ağ bileşenine gereksinim duyması, daha ucuz ve esnek olması sıralanabilir.




**Şekil 6: Standart WIMAX Topolojisi [23]**

Bu bölümde, WIMAX'ın sadece 802.16e-2005 WIMAX Mobil ortam desteği bilgilerine ve güvenliğine yer verilecektir. Mobil ortamlar, sabit ortamlardan daha karmaşık olmalarından dolayı, WIMAX Mobil teknolojisinde, mobil kullanıcı hareket halinde iken kullanıcının telsiz bağlantısı bir mobil baz istasyonundan diğer baz istasyonuna verimli bir şekilde aktarılması gerekmektedir.

WIMAX Mobil, bazıları tarafından 4G teknolojisi olarak adlandırılsa da bu doğru değildir. WIMAX uygulamaları, özellikle Asya ülkelerinde (Güney Kore, Tayvan ve Hindistan) yaygın kullanılmaya başlamış, ABD ve Avrupa ülkelerinde ise bazı operatörler WIMAX uygulamalarını sunma aşamasına gelmişlerdir. Günümüzde, yaklaşık 3 Milyar abonesi olan Mobil Operatörlerin sunduğu uygulama ve teknolojilerle ile bir yarış halinde olan WIMAX'ın 2012 yılından önce 25 Milyon civarında mobil müşterisi olması beklenmektedir[1].

WIMAX Mobil'ın kullanıcı hız ve performansı, kurulacak WIMAX mobil şebekesine ve birçok faktöre bağımlıdır. Kullanıcının WIMAX Mobil hızı, baz istasyonların alınan telsiz trafiğini ana mobil ağa gönderme kapasitesi, radyo sistemlerinde kullanılan MIMO anten sayısına, alandaki hava koşullarına, bölgedeki engel durumuna, ortak kullanılan WIMAX şebeke elemanlarının yüklenme durumuna ve mobil cihazın hızına bağımlıdır.

Kullanıcının gönderme ve alma hızı asimetrik olup, ortalama yükleme hızı 20Mhz bir kanalda 30Mbps'dır. Bu hız kurumda aynı anda ortalama 30 kişi tarafından kullanılıyor ve bu kullanıcıların yarısı aynı anda yükleme yapıyorsa her bir kişin ortalama yükleme hızı 2 Mbps olmaktadır.

WIMAX güvenliği aşağıdaki başlıklarda özetlenebilir [24]:

- *Veri Gizliliği ve Tutarlılığı:* WIMAX teknolojisi veriyi güvenli AES algoritması ile simetrik olarak şifreler. AES simetrik bir şifreleme yöntemi olması nedeniyle, veriyi gönderen ve alanın aynı anahtara sahip olması gerekmektedir.

  Ayrıca WIMAX Mobil teknolojisi, 802.16e:2005 standardına göre simetrik ve gizli anahtar bilgisini Mobil kullanıcı ve Baz istasyonu arasında iletmek için PKI (Açık Anahtar Altyapısı) kullanabilir. PKMv2 (Privacy and Key Management Protocol Sürüm 2) mekanizması ile mobil kullanıcı kimlik denetimi yapıldıktan sonra (kimlik ve parola), kullanıcıya Yetkilendirme Anahtarı gönderilmektedir. Yetkilendirme anahtarından verinin şifreleneceği simetrik AES anahtarı elde edilmektedir. PKMv2 ile asimetrik RSA genel anahtar değişimi mobil kullanıcı ve baz istasyonu arasında gerçekleşir. Ahahtar değişimi için X.509 sertifikası veya SIM kartı (Mobil telefonlar için) gizli bilgileri kullanılabilmektedir.

- *Kimlik Denetimi:* WIMAX 'da kullanıcı kimliğinin doğrulanması yukarıda belirtilen Kimlik Denetleyici ve Kimlik Denetim Sunucusu ile sağlanmaktadır. Bu amaçla EAP Protokolü kullanılmaktadır. Kimlik Denetleme Sunucusu için RADIUS veya DIAMETER protokol desteği gerekmektedir.

[1] Senza Fili Consulting, 2007

WIMAX güvenliğinde, kullanıcı erişim kontrolü, kullanıcı kimlik denetimi, veri trafiğinin gizliliği, iletilen verinin tutarlılığı mümkündür [25].

## 2.5. BlueTooth

Elektronik cihazların (sabit ve mobil) kısa mesafelerde (yaklaşık 10 metre civarında) birbirleri ile iletişim kurabilmesini sağlayan bir teknolojidir. Bluetooth ile cihazlar arası dosya paylaşımı, veri, ses ve resim iletişimi, İnternet bağlantısı yapılabilmektedir.

Bluetooth, ISM 2.4 GHz bandında çalışan bir kısa mesafe iletişim teknolojisidir. Bu teknoloji standardı, ürün geliştiriciler için hem bağlantı (link layer) katmanında, hem de uygulama (application layer) katmanında tanımlamalar içerdiğinden ses ve veri taşıma yeteneğine sahip bulunmaktadır. Bluetooth teknolojisinin önemli özellikleri olarak; yüksek güvenlik seviyesine sahip olması, sağlamlık, düşük güç ve düşük maliyet sıralanabilir.

Bluetooth teknolojisi, diğer pek çok cihazın da çalıştığı 2.4 GHz bandında çalışıyor olmasına rağmen, sahip olduğu AFH (Adaptive Frequency Hopping) yeteneği sayesinde üzerindeki enterferans etkisini önemli ölçüde azaltmayı başarmıştır. AFH çalışma prensibiyle, spektrumu kullanan diğer cihazlar tespit edilerek kullandıkları frekans bandının kullanımından kaçınılmakta ve böylece kullanıma uygun frekans bandının belirlenmesi ile enterferans engellenmektedir.

Bluetooth teknolojisi, ilk olarak Bluetooth SIG (Special Interest Group) tarafından geliştirilen bir teknoloji olmasına rağmen, kablosuz kişisel alan ağlarındaki (WPAN - wireless personal area network) kullanım etkinliği göz önünde bulundurularak IEEE'nin 2002 yılında yayınladığı IEEE Std 802.15.1 belgesi ile standartlaştırılmıştır.

WPAN'lar kısa mesafe içerisinde özel bir grupta yer alan cihazlar arasında bilgi taşımak amacıyla kullanılırlar. Bir WPAN'da gerçekleştirilen bağlantıda, kablosuz yerel alan ağlarındakinin aksine, altyapı ya hiç yoktur ya da çok azdır. 'Link' dışındaki dünyaya hemen hemen hiçbir bağlantı yoktur.

802.15.1 standardının orijinal amacı, bir WPAN cihazı ile IEEE 802.11 cihazı arasında veri transferi için kabul edilebilir bir birlikte çalışma seviyesi tanımlamaktır. Bunun çok da yapılabilir olmadığının belirlenmesine rağmen, 802.15.1–2005 standardı IEEE 802.11b sınıfı cihazlarla daha iyi ortak çalışabilirlik sağlamak için tanımlanmış mekanizmalar içermektedir. Her iki standart ve önceki sürümleri, tamamıyla Bluetooth SIG tarafından geliştirilen teknolojiye dayanarak oluşturulmuşlardır.

Bluetooth teknolojisinde çalışma menzili cihazın sınıfına göre değişiklik göstermektedir. Sınıf 3 radyolarda 1 ila 3 metre, Sınıf 2 radyolarda (daha çok mobil

cihazlarda bulunan) yaklaşık 10 metre ve Sınıf 1 radyolarda (endüstriyel uygulamalarda kullanılan) yaklaşık 100 metredir.

Veri aktarım hızı olarak, bluetooth sürüm 1.2 için 1 Mbps, bluetooth sürüm 2.0 + EDR (Enhanced Data Rate) için 3 Mbps'a kadar desteklenmektedir.

Bluetooth, birden fazla veri şifreleme katmanı ve kimlik doğrulama önlemi kullandığı için güvenli bir teknolojidir. Bluetooth cihazlar, diğer bluetooth cihazları tanımak için PIN ve bluetooth adresinin bir kombinasyonunu kullanmaktadır. Ayrıca, güvenliği bir kat daha arttırmak için veri şifreleme de (örneğin 128 bit şifreleme) kullanılabilmektedir. Bluetooth cihazların kullandığı modülasyon tekniği olan FHSS (Frequency-Hopping Spread Spectrum) de ilave bir güvenlik seviyesi oluşturmaktadır. FHSS tekniğinde, sadece uygun şekilde senkronize olmuş verici ve alıcı arasında veri aktarımı mümkün olmaktadır.

Bluetooth teknolojisinin bir sonraki sürümü olan Bluetooth 3.0'ın 2009 yılı içinde yayınlanması beklenmekte olup, söz konusu sürüm Gartner Grup tarafından 2009-2010 yıllarında izlenecek teknolojiler listesinde üst sıralarda yer almıştır. Bu sürümün bu kadar üst sıralarda yer almasının sebebi ise, çok düşük güç tüketimine sahip olmasının beklenmesidir.

## 2.6. 3. Nesil

3G (3. Nesil) teknolojisinin 2G teknolojisinden çok daha güçlü güvenlik ve servis kalitesinin olması için çeşitli araştırmalar yapılmıştır. 3G hakkında çalışmalar yapan en önemli çalışma ekibi 3GPP'dir. 3GPP üç temel prensip kapsamında 3G teknolojisini tasarlamıştır:

- Standart GSM teknolojisinde kabul görmüş ve kendini kanıtlamış güvenlik mimarisi 3G'de de kullanılacaktır.
- 2G teknolojisinde eksik olan veya düzeltilmesi gereken güvenlik eksiklikleri 3G ile giderilecektir.
- 3G teknolojisi ile sunulacak servisler için gerekli güvenlik önlemleri alınacaktır.

3G teknolojisi ile birlikte kullanmaya başlanabilecek servislerin kullanıcının hatalı kullanımına ve çeşitli suistimallere karşı korunaklı olması gerekmektedir. Hatta bu önlem, daha servisin geliştirme aşamasında alınmalıdır. 3G teknolojisi ile daha yüksek hızlarda servis alınmaktadır. Söz konusu hız sayesinde mobil ihtiyaçlar artık bir alışkanlığa dönüşmesi beklenmektedir. Bu nedenle, güvenlik kriterlerinin net olması ve dünya çapında kolay erişilebilir olması gerekmektedir. 3G teknolojisi günümüzde bir çok ülkede kullanılmaktadır. Uluslararası dolaşım (*roaming*) sırasında mobil uygulamasını kullananlar için farklı şebekeler içinde güvenlik standartları mutlaka geliştirilmelidir. En önemlisi, temel risk analizi yapılarak güvenlik önlemleri kategorize edilmelidir.

3G'yi destekleyen cihazlar aynı zamanda 2G ve 2+ G'yi de desteklemektedir. Her ne kadar yeni nesil cihazlarla 3G teknolojisi kullanılsa bile, içerisindeki SİM kart ve şebeke anahtarlama eski SİM kart üzerinde olmaktadır. Bu nedenle 3G operatörleri 3G servislerini SİM modülü üzerinden yapmayı kabul etmemektedirler. Ayrıca, 3G teknolojisi 3G kullanıcıları arasında doğrudan bağlantıyı ve PSTN, N-ISDN, GSM, X25 ve IP şebeke gibi diğer altyapıları da desteklemektedir.

Tüm 3G şebekeleri IPV6 sürümünü kullanmaktadır. Burada:

- Kullanıcı doğrulama,
- Radyo ara yüzünde şifreleme,
- Kullanıcı bilgilerinin gizliliği,
- Çıkarılabilir kullanıcı modüllerinin kontrolü,
- Ana şebeke ile uygulama arasındaki güvenlik

dikkat edilmesi gereken ana başlıklardır.

3G şebeke anahtarlamasında her ne kadar SİM kart kullanılsa da, IP tabanlı bir iletişime sahiptir. Dolayısı ile, İnternet üzerinden gelecek ataklara karşı önlemlerin alınması gerekmektedir [26].

# 3 MOBİL TEKNOLOJİDE GÜVENLİĞİ KISITLAYICI HUSUSLAR

Bu bölümde, mobil cihazların ve mobil ortamlar için geliştirilen uygulamaların, güvenlik perspektifinden bakıldığında mobil olmayanlardan farklı olarak sahip oldukları problemler ve kısıtlar ele alınmaktadır.

## 3.1. Cihaz Kaynaklı Problemler ve Kısıtlar

Teknolojideki gelişmeler işlem gücü, hafıza vb. alanlarda hızlı bir ilerlemeye neden olsa da günümüzde kullanılan akıllı telefon, PDA vb. mobil cihazlar sahip oldukları kaynaklar bakımından hala kısıtları bulunan cihazlardır. Bu kısıtlar nedeniyle bir güvenlik bileşeninin cihazlar üzerinde çalıştırılması performans problemlerine yol açabileceğinden, bu güvenlik ürünleri çoğunlukla geliştirilip kullanıcıya sunulmamakta ya da kullanıcılar tarafından kullanılmamaktadır. Benzer gerekçelerle yüksek işlem gücü gerektiren yöntemler yerine daha düşük işlem gücüne ihtiyaç duyan ancak daha az güvenli yöntemler tercih edilmektedir.

PDA ve akıllı telefon dünyasında ürün çeşitliliği çok fazladır ve bu ürünler üzerinde çalışan işletim sistemleri ve desteklenen olanaklar birbirlerinden farklıdır. Bu nedenlerle, kullanıcılara sunulan güvenlik paketleri genellikle sınırlı sayıdaki ürün tipi için kullanılabilmektedir. Aslında belirli bir standardın bulunmaması nedeniyle tüm ürünlerde çalışabilecek bir güvenlik paketinin geliştirilmesi de kolay değildir.

## 3.2. Mobilite Kaynaklı Problemler ve Kısıtlar

Kurumsal ağlarda bulunan bilişim kaynakları, güvenlik duvarı, saldırı önleme sistemi gibi merkezi güvenlik sistemleri ile korunmaktadır. Kurumsal güvenlik çözümlerinin kullanılmasındaki en önemli etkenler, alınması gereken önlemleri kullanıcı inisiyatifine bırakmadan alabilmek, merkezi yönetim sayesinde önlemleri hızlı ve etkin bir şekilde hayata geçirebilmektir. Ancak mobil cihazlar, bu tip merkezi güvenlik sistemlerinin koruması altında değildirler. Dolayısıyla bu cihazların üzerinde bulunabilecek güvenlik açıkları bir saldırgan tarafından doğrudan kötü amaçlar için kullanılabilir. Bu tip durumların önüne geçebilmek için yamaların uygulanması ve yazılımların güncel sürümlerinin kullanılması gerekmektedir. Bu noktada mobil cihazlarla ilgili bir diğer sorun karşımıza çıkmaktadır. İnsanlar mobil cihazlarını ve uygulamalarını güncel tutmak konusuna, masaüstü bilgisayarlarını güncel tutmak konusundan daha az hassas davranabilmektedir. Kurumsal bir ortam düşünüldüğünde, kurum bilgilerinin bulunabileceği mobil cihazların güvenliğinin sağlanması

ve kurum dışında dağıtık bir ortamda bulunan cihazların üzerindeki tüm yazılımların güncel olup olmadığının tespiti önemlidir.

Gizli bilgilerin mobil cihazlar üzerinde tamamen güvensiz ortamlara taşınması, özellikle de kolayca çalınabilecek ya da bir yerlerde unutulabilecek olmaları düşünüldüğünde, önemli bir problemdir. Bu kapsamda, sunulan korunma olanaklarının mobil cihaz kullanıcısı tarafından uygulandığından emin olmak gerekmektedir. Bilindiği gibi güvenlik ve kullanım kolaylığı genellikle birbiriyle çelişen hususlardır ve kullanıcının kendi inisiyatifine bırakıldığında güvenliği bir kenara bırakarak kullanım kolaylığını tercih etmesi ihtimali oldukça yüksektir. Cihazların belirli bir güvenlik standardını destekleyip desteklemediğini denetlemekten ise, bu cihazların dağıtık bir ortamda bulunması nedeniyle kolay değildir. Dağıtık yapının yanı sıra, cihazların denetlemeyi gerçekleştirecek merkezi sistem ile arasındaki iletişim kopabilir ya da kolaylıkla engellenebilir.

Mobilite nedeniyle saldırganların izini takip etmek mümkün olmayabilmektedir.

## 3.3. İletişim Kaynaklı Problemler ve Kısıtlar

Mobil cihazlar kablosuz ağ teknolojilerini kullanmaktadır. Kablosuz ağ teknolojisinde verilerin bir iletişim ağı bağlantı cihazı (hub gibi) kullanımında olduğu gibi hedef gözetmeksizin yayınlanması, bu verilerin mobil cihazla aynı ortamda bulunan herhangi birisi tarafından elde edilebilmesi anlamına gelmektedir.

Mobil cihazlar çoğunlukla birden fazla iletişim olanağına (örneğin, WiFi, GSM, Bluetooth vb.) sahiptir ve bu da güvenlik risklerini artıran bir unsurdur. Örneğin, 802.11g protokolü aracılığıyla kurumsal ağa sanal özel ağ (VPN) bağlantısı bulunan bir cihaza, yanlışlıkla açık ve korumasız bırakılmış bluetooth ara biriminden sakıncalı bir programın yüklenmesi durumunda, bu zararlı programın niteliğine göre kurumsal ağa zarar vermek mümkün olabilmektedir.

## 3.4. Kablosuz İletişimin Kısıtları

Mobil uygulamaların temelini oluşturan en önemli özellik kablosuz iletişimdir. Kablosuz iletişimin doğası gereği kablolu iletişimde alınabilen fiziksel önlemlerin pek çoğunun kullanılması imkansızdır. Kablosuz iletişimi sağlamak için gönderilen sinyaller mobil cihazla kablosuz yayın yapan cihaz arasında şifrelenmiş olsa dahi dinlenebilmesi (sniffing) kablolu iletişime göre çok daha kolaydır. Bu kolaylık sonucu olarak, yeterince dinleme yapılan bir iletişimde çok güçlü şifreleme teknikleri kullanılmış olsa bile şifrelerin kırılması mümkündür.

## 3.5. İletişim Operatörleri ve Sağlayıcılarından Kaynaklanan Kısıtlar

İletişim operatörleri her ne kadar geniş bir kablosuz ortamda hizmet verseler de bir takım kısıtlara sahiptirler. Bu kısıtları teknolojik ve servis kaynaklı olabilmektedir. Teknolojik olarak servis kalitesini etkileyen her şey aslında operatörler için birer kısıt olarak değerlendirilmektedir. Mobil cihazdan şebekeye çıkan bir sinyalin hava ara yüzünden iletilmesi kısıtlı bir kaynakla olmaktadır. Bu kaynak, kullanıcı suistimali, bölgesel yoğun kullanım ve donanımsal sorunlar nedeni ile hızlı bir şekilde tüketilebilir. Bu noktada hava ara yüzü sıkışır ve bağlantı sağlanamaz. Söz konusu sıkışma mobil uygulamaya erişimi engelleyecek ve servisi çalışmaz hale getirebilmektedir.

Operatörler tarafından veri akışının sağlanması gereken servislerde verinin güvenli bir altyapıdan geçerek iletilmesi bilgim güvenliği açısından önemlidir. Bu güvenli altyapı, kablosuz ortamdan gelen verinin karaya indirilerek uçtan uca karasal hatlarla teslimi şeklinde olabilir. Son kullanıcı ve servis sağlayıcı arasındaki bu bağlantı operatörler tarafında tesis edilmektedir. Burada gerek şebekesel gerekse de donanımsal kaynak kullanımından kaynaklı kısıtlara dikkat edilmelidir.

İletişimin kurumsal ağdan çıktığı andan itibaren iletişim sağlayıcının kontrolünde olması da önemli bir kısıt olarak gösterilebilir. Paketler kurumsal ağdan çıkıp mobil cihaza ulaştığı ana kadar tümüyle iletişim sağlayıcıların kontrolündedir. Kurumsal ağdan çıkan paketler önce İnternet ağı üzerinden iletişim sağlayıcıların ağına girer, bu ağ içinden geçerek mobil cihaza iletilmek üzere gerekli iletişim protokolü üzerinden mobil cihaza iletilir. Bu noktada dikkat edilmesi gereken bir nokta da, kurumsal ağadan çıkan paketlerin birkaç iletişim sağlayıcı ağından geçerek mobil cihaza ulaşabilir.

# 4 MOBİL UYGULAMALARDA TEHDİT, KORUNMASIZLIK, RİSK VE ÖNLEMLERİ

Günümüzde üretilen mobil cihazlar ve bu cihazlar üzerindeki uygulamalar hayatımıza sadece kolaylıkları değil aynı zamanda yeni risk ve tehditleri de beraberinde getirmiştir. Kişisel ve kurumsal bilgiler, mobil cihazlarda, bu cihazlara rahatlıkla takılabilecek, çıkarılabilecek ve değiştirilebilecek harici hafıza kartlarında taşınmaya başlamıştır. Ayrıca mobil cihazlara gelen e-postalarda ekonomik ve hukuki konular tartışılabilmektedir. Kişisel takvim, adresler, bankacılık işlemler içinkullanılan parolalar cihazlara kaydedilmektedir. Silikon teknolojisi sayesinde harici hafıza kartların alacağı veri miktarı arttıkça yukarıda değindiğimiz konulara benzer konulara mobil cihazlarda daha çok yer açılmaktadır.

Mobil cihazların üzerinde bu işlemlerin yaygınlaşmaya devam ediyor oluşunu iki temel nedenle özetleyebiliriz:

a. Boyutu ve taşınabilirliği,

b. Kablosuz ağlara bağlanma ara yüzü ve kablosuz ortamlarda çalışabilecek servislere sahip olması

Diğer taraftan cihazların boyutu, taşınabilir olması, sürekli yenilenmesi nedeni ile bir takım güvenlik açıkları oluşmaktadır.

Bu çalışmada, mobil cihazlardan söz ederken sadece cep telefonu, PDA vb cihazlardan değil, son dönemde boyutu küçülen ve hayatımızın bir parçası olan dizüstü bilgisayarlar da kastedilmektedir.

## 4.1. Mobil Uygulamalara Ait Korunmasızlıklar

### 4.1.1. Cihazın Fiziksel Zarar Görmesi, Çalınması ve Elden Çıkarılması

Mobil cihazların boyutlarından ve kullanımından kaynaklı olarak, gerek fiziksel olarak zarar görmesi gerekse de kayıp veya çalıntı durumuna düşmesi mümkündür. Çalıntı durumunda üzerindeki bilgiler şifreleme vasıtası ile korunmuş olsa dahi, hem cihazın hem de üzerindeki bilgilerin yerine koyma maliyeti bulunmaktadır. Bu durum cihazların fiziksel olarak korunmasını zorunlu kılmakta ve hırsızlığa karşı kullanıcıları tedbirli olmaya yöneltmektedir. BTK (Bilgi Teknolojileri ve İletişim Kurumu)'nın kayıtlı telefon sisteminin devreye girmesi ile çalıntı telefon sayısında bir süre düşüş gözlenmiştir. Ancak ülkemizde kayıp, çalıntı telefon sayısı 2008 yılında bir önceki yıla göre artış tespit edilmiştir. 2007 yılında doğrulanan 18 bin ihbar varken, 2008 yılının 11 ayında doğrulanan ihbar sayısı 26 bin 800 olmuştur. Diğer taraftan Gartner Grubun yaptığı bir araştırmada 2001 yılında 250.000 adet cep telefonu ve PDA havaalanında kaybedilmiş ve bunların %30 undan azı sahipleri tarafından bulunmuştur

[27]. Özellikle mobil İnternet kullanımının artması ile aynı korunmasızlık ve risk dizüstü bilgisayarlar için de geçerli hale gelmiştir.

### 4.1.2. Yetkisiz Kişiler Tarafından Cihazlara Erişilebilmesi

Gerek cep telefonları gerekse de PDA gibi el terminalleri üzerinde kullanıcı bazlı güvenlik önlemlerini almak basit ama bir o kadar da kararlılık gerektiren bir konudur. Cihaz güvenlik kodu ve PIN kodunu cihazlar üzerinden silmek veya cihaza bu tür güvenlik önlemleri vermek özel bilgilerin korunması açısından önemlidir. Bunun yanı sıra sıklıkla "1234", "0000" gibi basit ve kolay tahmin edilebilir PIN numaraları kullanılmaktadır. Bu tür PIN numaraları genelde cihazların fabrika ayarlarıyla gelmekte olup saldırganlar tarafından ilk denenen numaralardır.

Mobil uygulamalar için yazılan programların büyük çoğunluğunda, kullanıcının kolay çalışması amacıyla, güvenlik için gerekli parola ve PIN kodu kullanılmamaktadır. Özellikle kurumsal bilgiler için bu durum kritik bir güvenlik zafiyeti şeklinde karşımıza çıkmaktadır.

### 4.1.3. Kullanıcı ve Kurumsal Güvenlik Bilincinin Eksikliği

Tüm bilişim ortamlarında değişik kullanıcı grupları için güvenlik bilincinin oluşması güvenlik risklerinin azalmasına imkan veren en verimli yöntemlerden biridir. Mobil uygulama ortamlarında da standart kullanıcı, teknik ve kurumsal yönetim kullanıcıları aşağıdaki yöntemlerle bilinçlendirilmelidir:

- Değişik kullanıcı tiplerine yönelik yıllık güvenlik eğitim ve bilinçlendirme programları düzenlenmesi ,ve bu programlarda güncel mobil tehdit, kullanım ve risklere yer verilmesi,
- Kurumsal güvenlik politikasında mobil güvenliğe yönelik maddelerin yer almasının sağlanması ve politikanın tüm kullanıcılara duyurulması,
- Kurumsal Kapı (Portal) üzerinden güncel mobil uygulamalardaki tehdit, korunmasızlıklara yönelik duyuruların yapılması,
- Düzenli kurumsal korunmasızlık test ve analizlerin yapılması ve zafiyet tespit edilen durumlarda kullanıcılara yönelik tehdit ve korunmasızlık bilgilerinin kullanıcılarla paylaşılması,
- Yeni işe başlayan kullanıcılara bu konuda güvenlik farkındalık ve bilinçlendirme eğitim programlarının uygulanması.

### 4.1.4. Mobil Uygulamalarda Kullanılan Sistem Yazılımlarına ait Korunmasızlıklar

Mobil cihazlarda kullanılan işletim sistemlerinin çok çeşitli olması, bu işletim sistemlerin öncelikle işlevsellik gereksinimleri göz önüne alınarak piyasaya sürülmesi, firmaların gerekli güvenlik testlerini yapmamaları mobil uygulamaların koştuğu sistem yazılımlarından kaynaklanan birçok korunmasızlığı beraberinde getirmektedir.

Özellikle mobil kullanıcı bileşenlerinde kullanılan işletim sistemi ve kullanılan İnternet tarayıcı (browser) bileşenlerinden kaynaklanan çok sayıda korunmasızlık söz konusudur. Buna önlem olarak, düzenli ve sürekli olarak güvenlik açıklarını gideren yamalar duyurulmaktadır.

### 4.1.5. Mobil Uygulamaların Birden Fazla Tarafa Gereksinim Duyması

Bu belge kapsamında ele alınan mobil uygulamalar, kablosu ortamdan iletilen bir tür sabit web uygulaması olarak ele alınabilir. Bu durumlarda planlanan mobil uygulamanın kullanıcı (istemci) bileşeni hareket halindedir veya sabit bir ortamdan uygulamayı kullanmamaktadır. Kurumsal bir mobil uygulama içinde; kullanıcı bileşeni, kurumsal sunucular ve mobil iletişim ortamını sağlayan mobil operatör, mobil cihaz üreticisi, standart uygulamalarda uygulama sağlayıcı şirket gibi kontrolü kurum dışında olan üçüncü taraflar bulunmaktadır. Bu nedenle, mobil uygulamalar kurumun tam kontrolü kapsamında olmayıp, sabit uygulamalara göre daha fazla korunmasızlığa sahiptir. Önlem olarak, üçüncü taraflarla yapılacak işbirliği ve anlaşmalarda mutlaka güvenlik maddeleri yer almalı, kullanılan servis türlerinde güvenli teknoloji kullanan servis yöntemleri seçilmelidir.

### 4.1.6. Mobil Ajan Uygulama Bileşenlerinin Özelliğinden Kaynaklanan Korunmasızlıklar

Mobil uygulamaların büyük çoğunluğunda kullanıcı bileşeninde koşan mobil ajanlar söz konusudur. Günümüzde mobil ajanlı uygulamalar PDA, telekomünikasyon sistemleri, bilişim yönetimi, servis yönetimi ve bilgisayar simülasyonları gibi birçok alanda kullanılmaktadır. Mobil uygulama ajanının çalışmasını ve yüklenmesini sağlayan bilgisayar sunucu bileşeni ağdan ayrılsa dahi mobil ajanları yüklendiği ortamda çalışmaya devam ederler. Mobil ajanlı uygulama teknolojisinin yeni olması, mobil ajanının kimlik denetimi, tanınması, güvenli mesajlaşması, hedef kaynağın doğrulanması, sertifikasının kontrol edilmesi gibi bir dizi güvenlik önlemine ihtiyaç duyması ve bunların yapılmaması durumunda mobil ajanlı uygulamalar teknolojisi gereği bir korunmasızlık oluşturmaktadır.

## 4.2. Mobil Uygulamalara Ait Tehditler

Bölüm 4.1'de belirtilen mobil uygulamalara ait korunmasızlıktan yararlanan başlıca tehditler aşağıda verilmektedir.

### 4.2.1. Zararlı Yazılımlar (Malware)

Mobil cihazlar ve PDA'ler üzerindeki yazılımlarda güvenlik önlemleri açısından eksiklikler gözlemlenmektedir. Gerek dizüstü bilgisayarlar gerekse de cep telefonları ve PDA'lere önlem alınmadığı takdirde rahatlıkla virüs ve diğer zararlı yazılımlara maruz kalabilmektedir. Zararlı yazılım kaynakları şu şekilde sıralanabilir:

- *İnternet'ten indirilen dosyalar*: Günümüzde kullanıcılar, oyun, güvenlik yamaları, günlük hayatta sıkça kullanılan yazılım (sözlük vb), gibi ihtiyaçlarını ücretsiz ya da paylaşımlı olarak İnternetten indirmektedirler. İndirilen dosyalar aracılığıyla zararlı yazılımlar cihaza yerleşebilmektedir. Bu nedenle, gerek cep telefonu ve PDA'lerde gerekse diz-üstü bilgisayarlarda lisanslı veya doğruluğu onaylanmış yazılımların kullanılması önerilmektedir.
- *Mesajlaşma Servisleri:* Mobil cihazlara gönderilen MMS ve e-mail mesajlarının ekinde virüs ya da zararlı programlar iletilebilmektedir. Genel olarak, anlık mesajlaşmaları destekleyen tüm cihazlarda bu tehlikenin söz konusu olabileceği değerlendirilmelidir. Bu nedenle, kullanıcılar cihazlarına gelen mesajlar kontrol edilerek ve seçici davranaak açılmalı ve cihazlarında güvenli yazılımlar çalıştırmalıdır.
- *Bluetooth İletişimi:* Mobil cihazlar arasında çeşitli dosyaların (metin, film, müzik dosyları vb) gönderimi için bluetooth teknolojisi son derece pratik ve kullanışlıdır. Bluetooth teknolojisinde cihazların etkileşimi iki aşamalı olmaktadır. Bluetooth özelliği açık bir cihazı diğer bir cihazın görmesi ve bağlantı için istek göndermesi ilk aşamayı oluşturur. İkinci aşama ise karşı cihazın olumlu cevap vermesi ile bağlantının gerçekleşmesi şeklindedir. Bu bağlantı sırasında kötü yazılımlar da cihaza aktarılabilmektedir.

Zararlı yazılımlar ile mobil cihazlara doğru gerçekleştirilebilecek ataklar ise şu şekilde sıralanabilir [28]:

- *Yerine geçme:* Zararlı yazılım sayesinde cihaz üzerinde adeta uzak masa üstü erişimi sağlanarak mobil cihaz üzerinden bilgiler alınabilir.
- *Veri akışını kesme:* Cihaza doğru olan her türlü veri akışı kesilebilir.

- *Bilgi hırsızlığı:* Cihaza yerleşen zararlı yazılım tüm bilgileri toplayarak cihazdan dışarı gönderebilir.
- *Arka kapı (Backdoor):* Zararlı yazılım cihazda korunmsız bir arka kapı oluşturarak diğer ataklara açık hale getirir.
- *Servisi kötüye kullanma:* Cihaza yerleşmiş yazılım, servisi çok amaçlı kullanarak, kullanıcının fazla ücret ödemesine yol açar.
- *Erişilebilirlik:* Cihaz üzerindeki zararlı yazılım diğer cihazlarla etkileşimi sağlayarak farklı verilere erişim sağlayabilir.
- *Şebekeye giriş:* Cihaz üzerindeki zararlı yazılım farklı bir kimlik doğrulamaya gerek kalmaksızın şebekeye erişebilir.
- *Solucan (Wormable):* Cihaz üzerindeki zararlı yazılım, son derece rahat çoğalan solucanlar olabilir ve diğer cihazlara doğru hızla yayılır.

### 4.2.2. BlueSnarfing Saldırıları

BlueSnarfing, bluetooth teknolojisinin açıklarından yararlanan kablosuz iletişim esnasında bilgi çalmayı hedefleyen bir saldırı çeşididir [17, 29, 30]. Özellikle cep telefonları ile sağlanan bluetooth bağlantısı esnasında, nesne değişim adı verilen protokoldeki zafiyet kullanılarak kullanıcının cihazındaki adres, e-posta ve diğer kişisel bilgileri hiçbir iz bırakılmadan çalınabilmektedir. Saldırgan, kurbanının cihazı ile senkranizasyon gerçekleştirerek içerisindeki bilgi ve servislere yetki alabilmektedir. Bu işlem için gerekli yazılım ve nasıl kullanılacağı hakkındaki bilgiler açık olup erişmek mümkündür.

BlueSnarfing saldırılarından korunmanın en iyi yolu olarak, özellikle kullanılmadığı durumlarda bluetooth bağlantısının kapatılması gerektiği önerilmektedir.

### 4.2.3. Drive-by Spamming

Drive-by Spamming saldırısı, kablosuz yerel iletişim ağı (WLAN) zafiyetlerinden yararlanılarak ağa erişim yetkisi edinilmesi ve ağ üzerinden istenmeyen mesajların gönderilmesini hedeflemektedir. İletişim ağlarında güvensiz giriş noktaları arayarak işleme başlayan ve sonrasında korunmasız bir e-posta sunucusu bulmayı hedefleyen saldırgan, hedefine ulaştığında yetkili bir kullanıcı gibi yüksek sayıda istenmeyen e-postalar gönderebilmektedir. Araştırmalara göre %60-80 civarında kablosuz yerel iletişim ağı, sistem yöneticilerin fabrika ayarlarını değiştirmemesi nedeniyle bu tür saldırılara karşı zafiyet göstermektedir [29].

### 4.2.4. Wardriving ve Warchalking

Kablosuz ağların kırılabilmesi ve içeri sızabilmek için öncelikle saldırganın açık ağları keşfetmesi gerekmektedir. Bu amaçla yapılan kablosuz ağ taraması, kablosuz ağdaki uygun AP (*access point*, giriş noktası)'lerin bulunabilmesi yöntemidir. Kablosuz ağ kartının her paketi kabul eden modda çalışması ve yazılımın iletişime açık bir AP tespit etmesi ile kablosuz bir ağ bulunabilir. Bu aşamadan sonra saldırgan, belirlediği AP ile ilgili SSID, WEP, MAC gibi gerekli bilgilere erişebilir, WEP anahtarı zayıf ise bir yazılım yardımı ile kırabilir ve birtakım loglar toplayabilir.

Kablosuz ağ taramak için kullanılan yollardan birkaçı Wardriving, Warchalking, Warstrolling ve Warflying'dir. Bunlardan en çok bilinenlerinden Wardriving ve Warchalking hakkında aşağıda bilgi verilmekedir [31, 29, 30].

Wardriving, güvenlik seviyesi az olan veya olmayan bir kablosuz ağ tespit etme yöntemidir. Saldırgan bir dizüstü bilgisayar veya el bilgisayarı ile arabasında otururken bu amaçla geliştirilmiş yazılım araçları kullanarak bir kablosuz ağ tespit edebilir. Daha sonra uygun bir AP tespit ederek zayıflıklarını araştırabilir ve hatta İnternet bağlantısını bile engelleyebilir.

Warchalking, sembollerden oluşan bir dildir. 2002 yılında bir grup arkadaş tarafından tasarlanan ve yayınlanan, yol kenarlarında veya duvarlarda orada bir kablosuz ağın olduğunu gösteren sembollerden oluşmaktadır. Bu sembollerin içerisinde kablosuz ağlarla ilgili SSID, bant genişliği gibi önemli bilgiler yer almaktadır. Semboller kullanılarak Wardriving için gerekli olan istasyona ve ağa ait birçok bilgi alınabilir.

### 4.2.5. Servis Kesintisi (DoS) Saldırıları

Servis kesintisi saldırıları, sunucu veya iletişim ağı kapasitesini zorlayarak kullanıcıların hizmet almasını engellemeyi hedeflemektedir. Bu sayede, hizmet veren firmalara maddi kayıp verebilecekleri gibi itibar kaybına da yol açmaktadırlar. Kablosuz iletişim ağları da diğer kablolu ağlar gibi bu tür saldırılara oldukça açık olup saldırganlar için önemli bir hedef teşkil etmektedirler.

IEEE 802.11i protokolü ile birlikte kablosuz ağların güvenliğine yönelik geliştirmeler yapılmış olsa da, alınan önlemler iletişimin veri katmanında uygulanıp yönetim katmanında bir koruma sağlamamaktadır. DoS saldırılarının kaynağını yönetim katmanında bulunan bu zafiyetler oluşturmaktadır. Bu açıklar ile DoS saldırılarına imkan sağlayacak kablosuz ağ konfigürasyon ve bileşen bilgilerine erişim mümkün olabilmektedir [32].

IEEE 802.11w protokolü ile birlikte kablosuz DoS saldırılarına karşı gelişmiş güvenlik önlemleri hedeflenmiş olup bu saldırılara karşı önemli bir başarı alınabileceği ümit edilmektedir.

### 4.2.6. Spam

Mobil cihaz teknolojisinin gelişmesi ile birlikte sadece kısa mesaj (SMS) değil, e-posta, mobil çoklu ortam (görüntülü, sesli, fotoğraflı, vb.) mesaj (MMS) ve sesli mesaj gibi teknolojiler de cihazlar üzerinde kullanılmaya başlanmıştır. Operatörlerden gönderilen bu tür mesajlarla herhangi bir güvensiz ortam yaratılmasa bile, söz konusu mesajlar bir cihazdan farklı bir cihaza yönlendirilirken veya bluetooth teknolojisi ile transfer edilirken bir takım güvenlik açıkları ortaya çıkabilmektedir. Ayrıca, gerek anlık gelen tanıtım mesajları gerekse e-postalar cihaz hafızasını doldurabilmekte ve kullanıcıya gereksiz servis kullanım ücreti olarak yansıyabilmektedir.

### 4.2.7. SMiShing Atakları

Mobil cihaz ve uygulamaların yaygınlaşması ile 2006 yıllarından başlayarak yeni mobil tehditleri gündeme gelmiştir. Bunlardan SMiShing atakları SMS servisi ile yapılan bir tür kandırmaca mesaj gönderimi atağıdır. Kısa mesaj kullanılarak gerçekleştirilen ve bir tür sosyal mühendislik saldırısı olan SmiShing ile özellikle güvenlik bilinci ve farkındalığı yeterli düzeyde olmayan mobil kullanıcıların gizli ve kişisel bilgilerinin yetkisiz kişilerin eline geçmesi mümkün olabilmektedir. SmiShing ataklarında genellikle, gelen mesajda kullanıcıya acil bir durum bilgisi verilerek, kullanıcıdan bir web linkine bağlanarak veya verilen bir telefonu arayarak müdahale etmesi istenmektedir. Gerçekte bağlanılacak web linki sahte ve saldırganın kullanıcı kişisel bilgilerini topladığı bir site, veya aranacak telefon numarası kişisel bilgilerin kayıt edildiği bir insansız telefon yanıtlama sistemi olmaktadır [33].

### 4.2.8. MobiSpy Atakları

MobiSpy son yıllarda ortaya çıkan ve bazı özel işletim sistemleri için tehdit oluşturan, mobil cihazlara yüklenen bir saldırı yazılımıdır. Bu yazılım sayesinde mobil cihazın telefon, mesaj trafiği yetkisiz ve kullanıcıdan habersiz olarak kayıt edilerek daha sonra merkezi bir saldırgan sunucusuna GPRS İnternet bağlantısı ile iletilmektedir [34].

### 4.2.9. Elektronik Dinleme

Günümüzde birçok kullanıcı özel telefon görüşmelerinin dinlenmemesi veya duyulmaması için etrafını kontrol etmeye dikkat etmektedir. Benzer şekilde, elektronik ortamda da dinlenmemek için yazılım ve donanım korunmasının önemini anlamak gerekmektedir. Özellikle casus yazılımlara, gerek dönemsel olayların gerekse de medyadaki haberlerin etkisi ile daha dikkat eder hale gelmiştir. Mobil cihazlar, casus yazılımların bir

şekilde cihaza alınmasına ve yüklenmesine elverişli güvenlik açıklarına sahiptir. Söz konusu casus yazılımlar, mobil cihaza yüklendikten sonra, tüm bilgileri toplayarak bir başka cihaza veya sunucuya gönderebilecek yetenektedir. Ayrıca, cihazın mikrofonunu dinleyerek konuşmaları eş zamanlı yönlendirmek için de kullanılabilmektedir.

Dolaylı olarak elektronik dinleme yapabilen bir çok yazılım ve yöntem mevcuttur. Hatta bunlara erişmek için İnternette yapılacak küçük çaplı bir araştırma bile yeterli olabilmektedir. Bilgisayar ve kablo şebekesi dünyasında, cihazların şebekeye erişimi belirli yetkilendirme çerçevesinde çalışmaktadır. Kablosuz iletişim teknolojisi ile sabit bir şebekeye erişmekte farklı güvenlik önlemleri (IP kontrolü, APN, VPN vb) alınabilmektedir. Bu yapı özellikle kurumsal iletişimde mobil teknolojiyi kullananlar için mutlaka inşa edilmesi gereken bir konudur.

Örneğin, mobil iletişim teknolojisinde; mobil cihaz ile baz istasyonu arasındaki iletişim hava ara yüzü üzerinden sağlanmaktadır. Hava ara yüzünde alınan önlemler bu anlamda çok önemlidir. Kore'de yapılan bir araştırmada, farklı üreticilerin ürettiği ürünlerin birleştirilmesi ile çalışan CDMA sistemi üzerinde gözlemler yapılmıştır [35]. İsrail ve Amerikalı araştırmacılar, şebekenin şifrelerini çözerek elektronik dinlemeyi gerçekleştirmiş [36], özel bir engelleme yöntemi geliştirerek tüm şebekedeki mobil cihaz trafiğini gözlemlemişledir.

### 4.2.10. Elektronik Takip

Kablosuz iletişim teknolojisi yardımı ile, kullanıcının hizmet aldığı hücreden yola çıkılarak farklı konum tabanlı servis senaryoları gerçekleştirilmiştir. Mobil cihazın korunmasızlığından kaynaklı sebeplerle (unutma, çalınma vb) cihaz açık bir hedef haline gelmektedir. Bazı konum tabanlı servisler belirli periyotlarla cihazla haberleşerek konum güncellemesi yapmaktadırlar. Bir takım servisler ise herhangi bir haberleşme olmadan doğrudan hizmet alınan hücre bilgisinden yola çıkarak çalışmaktadırlar. Bu tür servislerde hizmet alınan hücredeki radyo sisteminde hatalar oluşabilmektedir. Ayrıca ortamdan kaynaklı olarak cihaz Faraday kafesinde kalıp, radyo istasyonu ile tüm iletişimi kesebilmektedir. Ayrıca, cihaz radyo istasyonu ile sürekli temasa geçmek isteyeceğinden pil ömrünü de önemli ölçüde kısaltmaktadır.

Sonuç olarak, ilk dönem konum tabanlı servisler göstermiştir ki, çeşitli yöntemlerle bu servise farklı kişiler entegre olabilmekte ve servis bilgilerini izleyebilmektedir. Bu durum, büyük oranda cihazın korunmasızlığından ve servisin SMS v.b. bir yöntemle cihazla haberleşmesinin ve kimlik doğrulama özelliğinin olmamasından kaynaklanmaktadır.

### 4.2.11. Klonlama

Mobil cihazlar, üzerinde tek bir kimlik numarası ile üretilmektedirler. Başka bir mobil cihaza çeşitli nedenlerle bu cihazın kimlik numarası ve programları yüklenerek aynı cihazın yazılımsal olarak bir eşi oluşturulmaktadır. Bu işleme klonlama denmektedir. Örneğin, radyo frekans dalgasının yayılması gözlemlenerek, *analog* mobil cihaz şebekesi üretim sırasında aldığı *Elektronik Seri Numarası* (ESN) ve *Mobil Tanımlama Numarası* (MIN) bilgileri klonlama yapılmak için kolaylıkla elde edilebilir. Sayısal mobil cihaz şebekesinde bu anlamda güvenlik konusunda geliştirmeler yapılmıştır. Şebekeye bağlanma parolaları ile cihaz kimlik doğrulması yapılabilmektedir. Bu şekilde cihaz kimlik bilgilerinin şebeke üzerinden alınması engellenmektedir. Buna rağmen cihazın korunmasızlıktan kaynaklı riskleri yok edilememektedir.

### 4.2.12. Üçüncü Taraf Sunucu Hizmetleri

Son dönemlerde çoğunlukla tercih edilen, içerik ve uygulamanın farklı firmalarda tutulan sunucular üzerinden çalıştırılması çok ciddi güvenlik risklerine yol açmaktadır. Elektronik posta, çeşitli servis ve iletişim gereksinimlerinin dışarıdaki bir sunucuda olması kullanıcı bilgileri açısından da bir tehdit içermektedir. Bu durumun bir benzeri mobil cihaza yüklenerek çalıştırılan uygulamalarda da söz konusudur. Mobil cihazın korunmasızlığı ilgili yazılıma ve önemli bilgilere erişimde son derece büyük bir risktir.

Dolayısıyla, sunucuların farklı bir firma denetiminde olması ile cihaz üzerindeki (kurumsal vb) yazılımların ve bilgilerin taşınması aynı riski içermektedir. Bu nedenle, mobil cihazların üzerinde yazılım bulundurulmadan sadece bilgilerin çevrimiçi (online) alınıp sonrasında cihazda veri kalmamasının sağlanması gerekmektedir.

### 4.2.13. Hırsızlık

Mobil cihazların kolay taşınabilir olması bu cihazların çalınma riskini arttırmaktadır. Özellikle PDA, mobil telefon gibi üzerlerinde kişisel ve hassas veriler bulundurabilen cihazların çalınması, kullanıcıya olduğu kadar çalıştığı kurum için de zararın boyutu kestirilemeyecek bir tehdit oluşturmaktadır. Cihazların üzerindeki bilgiler şifreli olarak korunmuş olsa bile yerine koyma maliyeti ve cihazın kendi maliyeti önemli bir zarar olarak ortaya çıkmaktadır.

## 4.3. Mobil Uygulamalara Ait Güvenlik Önlemleri

Günümüzde taşınabilir cihazlar artık yaşamın tanımı olmaya başlamıştır. Bilgiye anında, konumdan ve kablodan bağımsız ulaşma isteği, eğlence servislerinin (oyun, kumar, sohbet vb.) artması, mobil ödeme gibi hizmetlerin özellikle web sayfalarından verilmeye başlanması, bireysel kullanıcıların mobil uygulamalara yönelmesini sağlamıştır. Bununla

birlikte çalışma koşulları da mobil uygulamaların tercihini artıran en önemli nedenlerden biri olarak karşımıza çıkmıştır. Sahada çalışma, satış ve teknik birimlerin kurum ile iletişimini güçlendirme, sahadan kurumsal uygulamalara ve e-postalara erişme, saha otomasyon servisleri gibi servisleri kullanma ve raporlama süreçlerinin anlık olması, kurumları hem kendi uygulamalarını geliştirmeye hem de PDA, Blackberry vb cihazları tercih etmelerine neden olmuştur. Gerek bireysel gerekse de kurumsal kimlikle mobil uygulamalara erişirken alınan risklere karşı önlem alma zorunluluğu bu noktada büyük önem arz etmektedir. Aslında her ne kadar bireysel ve kurumsal kullanım olarak ayırmaya çalışılsa bile, özellikle sahada çalışanlar mobil cihazları hem bireysel hem de kurumsal olarak kullanmaktadırlar. Bu durum, oluşacak risklere karşı her iki yapı için de önlemler alınmasını gerektirmektedir.

Mobil uygulamalarda oluşacak risklere karşı alınan önlemleri iki ana bölümde toplayabiliriz:

- Kullanıcı önlemleri
- Kurumsal önlemler

### 4.3.1. Kullanıcı Önlemleri

Özellikle mobil cihazların korunmasızlığı göz önüne alındığında bireysel kullanıcılara çok büyük görevler düşmektedir. Hem uygulamadan hem de cihazdan doğacak riskleri en aza indirmek durumunda kalan kullanıcı aşağıdaki önlemleri almalıdır:

**a. Fiziksel Kontrol**

Mobil cihazlar taşınması kolay boyutlarda üretilmektedirler. Bu cihazlarla son derece önemli bilgiler de taşınabilmektedir. Ayrıca cihazlarda, birinci derecede kullanıcıyı ilgilendiren uygulamalar da bulunabilmektedir. Bu nedenle, mobil cihazın korunması ve kontrolü kritik bir öneme sahiptir. Adeta bir kredi kartının korunmasında ve kullanılmasındaki kontrol, mobil cihazlar ve uygulamaları için de söz konusu olmalıdır. Mobil cihaz kullanılmadığı durumlarda otomatik olarak belli bir parola ve PIN ile kilitlenmesi sağlanmalıdır.

**b. Kullanıcı Kimlik Denetimi**

Gerek mobil cihazların açılması sırasında gerekse de mobil uygulamalara erişimde kullanıcılar PIN ve özel parolalar kullanmalıdırlar. Bu sayede çalınma ve kaybolma durumunda gereksiz servis kullanımının önüne geçilebileceği gibi, servis özelinde bilgilerin de çalınma riski en aza indirilmiş olacaktır.

**c. Veri Yedekleme**

Kullanıcılar, belirli aralıklarla cihazların ve uygulamalarının yedeklemesini yapmalıdırlar. Bu sayede cihazın korunmasızlığından doğacak risklerin oluşması ile meydana gelebilecek veri kayıplarının önüne geçilmiş olacaktır.

**d. Kablosuz İletişimde Dikkat Edilmesi Gerekenler**

Bluetooth, Wi-Fi, kızılötesi, WIMAX, GSM gibi kablosuz iletişim teknolojilerine olan gereksinimlerimiz artmaktadır. Ancak bu teknolojileri kullanırken havadan giden bilgilerin ele geçirilebilme riskleri de göz önünde bulundurulmalıdır. Zararlı yazılımların cihaza gönderilmesi güvensiz kablosuz iletişim teknolojilerinde kolayca mümkün olabilmektedir. Özellikle kullanım yoğunluklarının yaşandığı, havaalanı, konser gibi etkinliklerde açık olan bluetooth, kızılötesi gibi iletişim araçları potansiyel ataklar için bulunmaz fırsattır. Ayrıca, özellikle GPRS, Wi-Fi gibi teknolojilerden yararlanılarak yapılan bağlantılardan sonra mutlaka ilgili servisler kapatılmalıdır.

**e. Cihaz Tercihi**

Kullanıcılar kaybolma ve çalınma durumunda uzaktan cihaz üzerindeki servisleri kapatabilmeli, cihazı kilitleyebilmeli ve hatta cihazın üzerindeki tüm bilgileri silebilmelidirler. Günümüzde GSM teknolojisi sayesinde cihazların IMEI numarası üzerinden GSM operatörleri cihazları kullanılamaz hale getirebilmektedirler. Örneğin, Blackberry kurumsal Blackberry Sunucusu ile cihazı kilitleyebilmekte ve hatta cihazın üzerindeki tüm bilgileri silebilmektedir.

**f. Doğru Fonksiyon ve Doğru Uygulamaları Kullanma**

Kullanıcılar, ihtiyaçlarından fazla uygulamayı cihazlarına yüklemeleri sonucunda çeşitli sorunlar yaşamaktadırlar. Örneğin, fazla sayıda yüklenen uygulama, cihazın kapasitesi ve performansını olumsuz etkileyebilmektedir. Aynı zamanda özellikle İnternetten cihaza indirilmiş uygulamalarda, casus yazılımların veya virüslerin olma ihtimali yüksektir. Bunun yanı sıra kullanıcılar, ihtiyaçlarını mümkün olduğunca giderecek işlevleri üzerinde barındıran cihazları tercih etmelidir.

**g. Güvenlik Yazılımları ve Kontrol Sistemleri Kullanma**

Bilgisayar kullanıcıları; anti virüs programları, yabancı şebekelere bağlanmama, İnternetten temiz olduğuna emin olmadan program indirmemek gibi alışkanlıkları yeni yeni kazanmaktadır. Günümüzde kullanıcılar mobil cihazlarında ve mobil uygulamalarında da aynı hassasiyeti göstermek zorundadır. Aksi taktirde mobil uygulamalardaki riskleri yaşayabileceklerdir. Cihazlarının kapasitesine ve kullandıkları uygulamalara bağlı olarak kullanıcı,

- Kullanıcı kimlik denetimi yapmalı veya kişisel şifreleme kullanmalıdır,
- Cihazın içindeki veya harici hafızadaki bilgileri şifrelemelidir,
- Ağ geçidi yazılımı kullanmalıdır,
- Antivirüs programları kullanmalıdır,
- Antispam programları kullanmalıdır,
- Uygulamalara VPN gibi güvenli iletişim yöntemleri üzerinden erişmelidir.

Kullanıcılar, kurumsal bir yapı üzerinden mobil uygulama ve cihazları kullanıyorlarsa,

- Cihaz girişi kurumsal sistem tarafından kontrol edilmelidir,
- Kullanıcı yazılımı, güvenlik kuralları, güvenlik politikaları cihaza merkezi olarak kurumsal sunuculardan güvenilir ortamdan yüklenmelidir,
- Uzaktan güvenli olarak cihaz sıfırlaması (resetleme) erişilebilirliğin sağlanması için özel durumlarda yapılabilmelidir,
- Cihazın üzerindeki bilgiler erişilebilirlik ve acil durumlarda kurum merkezinden uzaktan silinebilmelidir,
- Cihaz üzerine çeşitli dosya indirmelerine karşı engellemeler yapılmalıdır,
- Kablosuz erişim ayarları güvenli olmalı ve bunların açık olup olmadığı kontrol edilmelidir,
- Mutlaka, VPN ve ağ geçidi gibi güvenlik araçları devrede iken uygulamaya bağlanılmalıdır,
- Uzaktan kurumsal ağdan güvenlik yama güncellemeleri yapılabilmelidir,
- Cihaz ve uygulama ile ilgili durumlar periyodik olarak güvenlik kontrolleri yapılmalıdır.

### 4.3.2. Kurumsal Önlemler

Günümüzdeki mobil uygulamalar ve işlevsel cihazlar daha çok kurumsal yapılarda tercih edilmektedir. İhtiyaçlara göre, saha ekipleri için satış otomasyonu, tüm işleri e-posta ile yapanlar için mobil cihazlar kurumlar tarafından temin edilip çalışanlarına verilmektedir. Bu kullanıcıların karşılarına çıkabilecek risklerle ilgili önlemler yukarıda sıralanmıştır. Ancak sadece kullanıcının önlem alması yeterli olmamaktadır. Kurumların da bir takım önlemler alması gerekmektedir. Bu önlemlerin büyük bölümü sabit uygulamalar için de geçerlidir.

**a. Mobil Uygulamalar için Güvenlik Politikalarının Devreye Alınması**

Kurumsal Güvenlik Politikalarında, mobil uygulama ve güvenli kullanımına yönelik politikalar yer almalıdır. Düzenli aralıkla gözden geçirilmesi gereken Mobil Uygulama Güvenlik Politikaları güncel teknolojilere ve değişimlere göre güncellenmelidir. Hazırlanan Mobil Uygulama Güvenlik Politikaları ilgili hedef kullanıcılara sorumluluklar yüklenmeli ve hedef kullanıcılara etkin bir şekilde duyurulması sağlanmalıdır.

Mobil Uygulama Güvenlik Politikaları en az aşağıdaki konuları içermelidir:

- Mobil uygulama kullanıcılarının yapmaması gerekenler (güvenlik ürünlerinin devre dışı bırakılmaması, kullanılan uygulamanın istemcisindeki güvenlik ayarlarının değiştirilmemesi gibi),
- Mobil Uygulama için kullanılan kimlik denetleme ve yetkilendirme bilgilerinin gizliliğinin sağlanması,
- Mobil ortamda tutulan ve iletilen bilginin hassasiyetine göre gizliliğinin sağlanması (sayısal şifreleme gibi yöntemler),
- Mobil cihazlara yönelik tehdit ve risklerin iyileştirilmesi yönelik önlemler (yama yönetimi, değişim yönetimi, güvenlik ürünlerinin devreye alınması, mobil yazılım modüllerinin güvenli tasarımı gibi).

**b. Mobil Uygulamalarda Güvenliğe İlişkin Farkındalık Faaliyetlerinin Uygulanması**

Kurumsal Mobil Güvenlik Politikalarına paralel olarak mobil uygulama kullanıcıları mobil uygulama kullanımı, mobil ortam tehditleri, mobil ortamda kullanılan kurumsal bilgilerin korunması, mobil operatörlerle ve mobil sunucularla güvenli iletişimin kurulması konularında düzenli olarak farkındalık eğitimi ve bilinçlendirme faaliyetlerine tabi tutulmalıdır.

**c. Kurumsal Güvenlik Risk Yönetiminin Uygulanması**

Diğer sabit uygulamaları, kurumsal verileri de içine alan Kurumsal Bilişim Risk Yönetimi süreci sürekli olarak uygulanmalıdır. Mobil Güvenlik Risk Yönetimi kurum ve mobil operatörleri tarafından uygulanmalı ve Kurumsal Bilişim Risk Yönetiminde aşağıdaki iş adımları takip edilmelidir.

- Mobil uygulama, teknoloji, cihaz, telsiz ortamlara ait güncel tehditlerin belirlenmelidir. Tehditler günden güne değişen teknikler içerdiğinden, kullanılan mobil cihazlara ve mobil ortamlara göre farklı tehditler söz konusu olduğundan tehdit analizlerinde otomatik araçların kullanılması önerilmektedir.

- Korunmasızlıklar tespit edilmelidir.
- Korunmasızılıktan yararlanacak tehdit eşleştirmesi yapılmalıdır.
- Riskler hesaplanmalı ve derecelendirilmelidir.
- Derecelendirilmiş risklere karşı alınması gereken önlemler tespit edilmelidir.
- Önlemlerin uygulanması planlanmalı ve alınan önlemlerin verimliliği ölçülmelidir.
- Yukarıda belirtilen iş adımları sürekli olarak uygulanmalıdır.

Mobil Uygulamalara ait Güvenlik Risk Yönetiminin, diğer Güvenlik Risk Yönetimlerinden farkı mobil uygulamalarda tehdit, korunmasızlık ve önlemlerin farklı ve çeşitli olmasıdır.

**d. Kurumsal Güvenlik Ürünlerinin Kullanılması**

Tek başına yeterli olmasa da risklerin azaltılması günümüzde mobil bileşenlerinde kullanılacak değişik güvenlik ürünlerinin kullanılması ve doğru yapılandırılması ile mümkündür. Mobil cihazlara kurulabilecek güvenlik ürünlerinden birkaçı aşağıda verilmektedir.

- Antivirüs ürünleri, kullanıcının virüslü dosyalara erişimini engellemekte, mobil tehditleri sezinleyerek mobil kullanıcı veri ve hizmetlerini korumaktadır.
- Anti Spam ürünleri, SPAM olarak iletilen istenmeyen kısa mesajları filtreleyerek tanımlı aksiyonlar almaktadır.
- Ağ geçidi ürünleri, mobil cihaza gelen ve çıkan ağ trafiğini denetlemekte ve tanımlı güvenlik kurallarına göre cihazı korumaktadır.
- *“Anti-spyware”, “anti-malware”* yazılımları, zararlı yazılımlara karşı mobil cihaz verilerini korumaktadır.

Mobil sunucu ortamlarında kullanılabilecek bazı güvenlik ürünleri ise şu şekilde sıralanabilir:

- Mobil Sunucu ortamlarındaki farklı uygulamalar için SSO Kimlik Denetim ve Yetkilendirme teknoloji ve ürünlerinin kullanılması.
- Kurumsal Mobil Sunucu ortamlarında uygulama, web sunucu ve verilerin tutulduğu Veritabanı ortamların ağ bölümlenmesi ve bölümlenen ağların sınır güvenliği için ağ geçidi kullanılması.
- Sunucu bileşenleri için antivirüs koruma ürünlerinin kullanılması.
- Sunucu ağlarında Saldırı Tespit ve Önleme sistemlerinin kullanılması.

- Sunucu ağında İçerik Filtreleme Sistemlerinin kullanılması.
- Sunucu bileşenlerindeki aktivitelerin Merkezi olarak toplanıp filtrelemesini temin eden Günlük Yönetim ve İzleme yazılımlarının kullanılması.
- Mesaj Sunucularda Anti SPAM ürünlerinin kullanılması.
- AAA Sunucularının kullanılması.
- Kablosuz ağ erişim noktalarının yönetim ve konfigürasyonun sağlandığı Kontrol Sunucu yazılımları kullanılması.
- Yama Yönetim Sistemlerinin kullanılması.

**e. Düzenli Korunmasızlık ve Sızma Testlerinin Yapılması**

Mobil istemci, mobil uygulama ve web sunucu bileşenleri, ağ bileşenleri, veri tabanı yönetim sistemleri, kablosuz ağ erişim noktaları, güvenlik ve sistem yönetim bileşenlerini, kullanıcıları, operasyon ve yordamları, mobil uygulamanın bellek taşması ve DoS ataklarına karşı, önlemlerinin sınanması, uygulama ve test geliştirme ortamlarını içeren düzenli güvenli korunmasızlık ve sızma testleri yapılması, olası tehditlere karşı korunmasızlıkların tespit edilmesi gerekmektedir.

Korunmasızlık ve sızma test ve analizlerine kimlik denetim, yetkilendirme, izlenebilirlik, mobil uygulamaya ait girdi, işlem ve çıktı kontrollerinin varlığı, kullanılan mobil teknolojilerinin duyurulmuş zafiyetlerinden ve eksikliklerden yararlanarak sızma, güvensiz iletişim protokol ve servislerinin varlığı, ürünlere ait varsayılan kimlik ve parolaları varlığı, konfigürasyon değerlerinin güvenli olup olmadığı, kullanıcıların güvenlik bilinç düzeyini tespit etme, yedekleme ve yönetim süreçleri mutlaka dahil edilmelidir.

Tehdit ve korunmasızlıklar zamanla değişkenlik göstereceğinden ve operasyon, süreç yazılım ve sistemlerde sürekli değişim söz konusu olduğu için korunmasızlık ve sızma analizleri belli aralıklarla yenilenmelidir.

**f. Kimlik Denetleme Teknolojilerinin Kullanımı**

Mobil cihazlara gelen bilginin kaynağının (kimden geldiğinin) doğrulanması için elektronik imza kullanılabilir. Güvenilir sertifika otoriteleri tarafından, güvenli elektronik imza oluşturma amacı ile verilen nitelikli sertifikalar sayesinde yapılan işlemlerde işlemin kimin tarafında yapıldığı bilgisine kesin olarak erişilebilir.

**g. Veri bütünlüğünün Sağlanmasına Yönelik Teknolojilerin Kullanımı**

Mobil cihazlara gelen verinin herhangi bir bozulmaya maruz kalmadan, gönderildiği andaki haliyle alıcı tarafa teslim edildiğinden emin olmak adına açık anahtar altyapısı (PKI)

veya elektronik imza kullanılabilir. Güvenilen sertifika otoriteleri tarafından, güvenli elektronik imza oluşturma amacı ile verilen nitelikli sertifikalar sayesinde yapılan işlemlerde taşınan bilginin herhangi bir bozulmaya maruz kalmadan alıcı tarafa aktarıldığından emin olunabilir.

**h. Diğer Kurumsal Güvenlik Önlemleri**

Mobil Uygulamaların kurumsal bileşenlerinin sabit uygulamalardan çok farklı olmaması nedeni ile aşağıda önerilen ek güvenlik önlemleri sabit uygulamalar için de geçerlidir:

- Konfigürasyon ve yama yönetim sisteminin uygulanması,
- Uygulama değişim yönetim sisteminin uygulanması,
- Uygulama geliştirme süreçlerinin ilk fazında güvenlik gereksinimlerinin belirlenmesi,
- Mobil uygulamada kalite standartlarına uyumun en az aşağıdaki koşullarla sağlanması:
    - Kodlama standartlarının yapılması ve bunun belgelendirmesi,
    - Doğrulama testlerinin yapılması,
    - Kritik kodların küçültülmesi,
    - Kullanıcı ara yüz uygulaması ile kullanıcı ara yüz uygulaması güvenlik kodunun izole edilmesi,
    - Mobil cihazın, tutarlığın sağlanması için uzaktan kontrollü ve güvenli açılmasının sağlanması,
    - Mobil uygulamanın veriye erişiminde güvenli kanalların kullanılması,
    - Uygulamaların üretim ortamına taşınmadan önce güvenlik testlerinin yapılması,
    - Uygulama sürüm kontrol sisteminin devreye alınması,
    - Düzenli izleme ve merkezi yönetimin devreye alınması,
    - Güvenli protokol ve servis kullanımı.

# 5 MOBİL UYGULAMALARDA GÜVENLİK YÖNTEMLERİ

Mobil uygulama, sadece istemcisi gezici olan, istemci ve ilk bağlantı noktası telsiz hat üzerinden gerçekleşen ve farklı şebeke bileşenlerine gereksinimi olan uygulama olarak tanımlanmaktadır. Mobil uygulamanın güvenliği sabit uygulamalı telli ortamlara göre daha karmaşık olmasına rağmen, sabit uygulamalarda olduğu gibi sabit sunucu ortamlarına gereksinim duymaktadır.

Bu bölümde, bir mobil uygulama için güvenliğin sağlanması uçtan uca ele alınmış olup, her bileşen ve iletişim ortamına ait endüstride uygulanan yöntemlere yer verilmiştir.

## 5.1. Mobil Uygulama Sunucu Ortamlarının Güvenliğinin Sağlanması

Mobil Uygulama için sunucu bileşenin koştuğu ortam genelde sabit bir ortamdır. Dolayısı ile bu bölümde verilen bilgiler sabit uygulamalar için de geçerlidir.

Aşağıda, mobil/sabit uygulamanın gereksinimi olan bileşenler ve bunlarla ilgili uygulanması önerilen güvenlik yöntemlerine yer verilmiştir.

### 5.1.1. Uygulama ve Web Sunucu Güvenliği

- Mobil uygulamanın koşacağı web ve uygulama sunucuları uygulamanın minimum gereksinimlerini taşımalı ve uygulama bileşenlerinin dışında başka uygulama ve servisleri sunucu üzerinde koşturulmamalıdır.
- Mobil uygulama istemci bileşeninin form, menü ve link bağlantıları mutlaka girdi değer doğrulamaları ve filtrelemesi uygulama tarafından yapılmalıdır.
- Uygulama ve web sunucu sistem yazılımlarındaki konfigürasyon değerleri varsayılan olarak bırakılmamalıdır.
- Uygulama ve web sunucu sistem yazılımı, güveneceği sistem ve uygulamalar dışında kalan uygulama ve sistemlere sertifika güvenleri kurulmamalıdır.
- Uygulama ve web sunucunun mutlaka test ortamı olmalı, duyurulmuş sistem güvenlik yamaları test ortamında test edildikten sonra üretim ortamına taşınmalıdır.
- Uygulama Açık Anahtar Altyapısı kullanıyor ise, sertifikasının geçerliliği düzenli olarak kontrol edilmelidir.
- Uygulama ve web kullanıcı güvenlik politikalarının doğrulaması yapılmalıdır.

- Uygulama ve web uygulama sistem yazılımının kullanımı, önemli dosyalara erişimi, başarılı, başarısız durumlar kayıt edilecek şekilde günlük izleri tanımlanmalı ve bu izlere erişim dizinleri kontrollü olmalıdır.
- Uygulama ve web sunucusu, düzenli olarak, yetkisiz ve yetkili kullanıcı kimlikleri ile güvenlik sızma ve korunmasızlık testlerine tabi tutulmalı, gerekli önlemler alınmalıdır.
- Uygulama ve web sunucunun konfigürasyon dosyaları kontrollü erişime tabi tutulmalıdır.
- Uygulama ve web sunucu konfigürasyon dosyalarının düzenli yedeği alınmalıdır.
- Hatalı login teşebbüslerine sınır getirilmeli ve belli bir sayıdan sonra otomatik kullanıcı kilitlemesi olmalıdır.

### 5.1.2. Veri Tabanı Yönetim Sistemi Güvenliği

- Mobil/Sabit uygulamanın kullandığı Veri Tabanı Yönetim Sistem (VTYS)'lerinin düzenli güvenlik yamaları test edildikten sonra üretim ortamına uygulanmalıdır.
- Varsayılan parola ve kullanıcılar değiştirilmelidir.
- Demo veritabanları sistemden kaldırılmalıdır.
- Varsayılan profiller yerine uygulamaya özel profiller yaratılmalı ve yetkiler kontrollü olarak bu profillere verilmelidir.
- VTYS'nin sistem nesnelerinin bulunduğu veritabanlarına sadece yetkili yöneticilerin erişimi sağlanmalıdır.
- VTYS'ne uzaktan bağlantı parametreleri güvenlikli olarak ayarlanmalıdır.
- VTYS içinden işletim sistemi çalıştırma komutlarına sınır getirilmelidir.
- VTYS günlükleri ayarlanmalı ve düzenli kontrol edilmelidir.
- VTYS yedekleri düzenli olarak alınmalıdır.
- Önemli tablo ve nesnelere erişim kontrollü olmalıdır.
- Önemli yöneticilerin Güvenli Parola Politikaları (parola uzunluğu, parolanın karmaşık karakterlerden oluşması, sınırlı parola ömrü, geçmiş parola atanmasına limit getirme gibi ) uygulanmalıdır.
- Hatalı login teşebbüslerine sınır getirilmeli ve belli bir sayıdan sonra otomatik kullanıcı kilitlemesi olmalıdır.

- Dışarıdan veri aktarma veya dışarıya veri alma komut ve hazır programlarına erişim kontrollü olmalıdır.

### 5.1.3. İşletim Sistemi Güvenliği

Uygulama, web, VTYS, sistem yönetim yazılımları, AAA sunucuları, RADIUS sunucuları, güvenlik sunucuları gibi değişik ürün ve yazılımların koştuğu işletim sisteminin güvenliği kritik bir öneme sahiptir. Bu nedenle, en az aşağıdaki hususlar göz önüne alınmalıdır.

- İşletim sistemlerine ait duyurulan güvenlik yamaları düzenli olarak test edildikten ve başarılı sonuç alındıktan sonra üretim ortamına uygulanmalıdır.
- Aktiviteler günlüklere işlenmelidir.
- İşletim sistemine ait ağ parametreleri atakları önleyici şekilde ayarlanmalıdır.
- İşletim sistemi yetkili kullanıcı kimlik adları değiştirilmelidir.
- İşletim sisteminde iş başlatma yetkisi yetkili kullanıcılara atanmalıdır.
- İşletim sisteminin parola dosyalarına erişim kısıtlı olmalıdır.
- İşletim sisteminin üzerinde güvensiz servis ve protokoller koşmamalıdır.
- Sistem yedekleri düzenli olarak alınmalıdır.

### 5.1.4. Diğer Bileşenlerin Güvenliği

- Uygulamanın kimlik denetim ve yetkilendirme sunucuları ile VTYS'ları özel ağ bölümlerine ağ geçitleri ile kontrollü erişim olacak sistem mimarisi tasarlanmalıdır.
- Ağ geçitlerinde iletişim yönüne bağlı kurallar oluşturulmalı ve güvensiz servislerin erişimi engellenmelidir.
- Tüm sunucular Anti Virus (AV) korumalı olmalıdır.
- Ağ bileşenleri erişilen port bazında kimlik denetimi yapılabilecek şeklinde ayarlanmalıdır.
- Uygulama kullanıyorsa mesaj sunucular anti-spam korumalı olmalıdır.
- Uygulama kullanıyorsa mesaj sunucular aktarıcı (relay) özelliğine kapatılmalıdır.
- Tüm bileşenlerin yedekleri düzenli alınmalıdır.
- Merkezi Günlük (log) sunucuları kullanılmalı ve izlenmenin kolaylaştırılması için filitreleme özelliği devreye alınmalıdır.

- Sistem Yönetim araçlarının güvenli protokollerle ve ağ geçitlerinde tanımlı kısıtlama kuralları ile bağlantısı sağlanmalıdır.
- Tüm diğer bileşenlerin güvenlik yamaları düzenli olarak uygulanmalıdır.
- Uzaktan bağlantılarda güvenli ve sertifika temelli bağlantı protokolleri kullanılmalıdır.

## 5.2. Mobil Uygulama Geliştirme ve Test Ortamlarının Güvenliği

Mobil/sabit uygulamaların geliştirildiği ortamların güvenliği için dikkat edilmesi gereken hususlar aşağıda verilmektedir:

- Geliştirme ortamaları için güvenlik yordamı oluşturulmalı ve bunun uygulanması sağlanmalıdır.
- Geliştirilen ortamda gereksiz servis ve portlar kapatılmalıdır.
- Geliştirilen ortamın üretim ortamına erişimi olmamalıdır.
- Geliştirme yapan kullanıcı sadece kendi geliştirdiği uygulamanın modül testlerini yapmalıdır.
- Geliştirme birden fazla geliştirici tarafından yapılıyorsa Geliştirme Sürüm Yönetim yazılımları kullanılmalıdır.
- Geliştirme yapılan ortak kütüphanelere erişim kontrollü ve kısıtlı olmalıdır. Geliştirme yapılan kaynak kodlara erişim kısıtlı ve kontrollü olmalıdır.
- Geliştirme sırasında tasarlanan güvenlik gereksinimlerinin testleri mutlaka yapılmalıdır.
- Geliştirme ortamının düzenli günlük yedeği alınmalıdır.
- Uygulamada taşınabilir kodlar ve program parçacıkları kullanılıyorsa bunun gizliliği ve bütünlüğünü sağlayıcı hedef ve kaynak kimlik denetim mekanizmaları (sayısal imzalı kodlar, “sandbox” gibi) kullanılmalıdır.

Mobil/sabit uygulamaların üretim ortamına taşınmadan önce test edilen ortamda dikkat edilmesi gereken güvenlik hususları aşağıda verilmektedir.

- Geliştirilen yazılım bölümlerinin modül, sistem, entegrasyon, regresyon testleri yapılmalıdır.
- Modül testleri hariç gerçekleştirilen tüm testler, bağımsız test ediciler tarafından yapılmalıdır.
- Test verisi olarak gerçek ortama en yakın veriler kullanılmalıdır.

- Bağımsız test ortamı, geliştirme ve üretim ortamlardan ayrı ve izole olmalıdır.
- Bağımsız test ortamından yapılan tüm test sonuçları, problem düzeltme bilgileri ile kayıt edilmelidir.
- Test araçlarına erişim kısıtlı ve kontrolü olmalıdır.

## 5.3. Mobil Cihaz/ İstemci Güvenliğinin Sağlanması

Mobil ya da kablosuz uygulamaların en savunmasız bileşeni mobil cihazdır. Mobil cihazların çalınma ve kaybolma riski kurumların hassas verileri ve müşteri bilgilerinin çalınması anlamına gelebilmektedir. 2007 yılı için yapılan tahminlerde dünya çapında 8 milyon telefonun çalıntı ya da kayıp olarak değerlendirildiği ve bunlardan 700.000 adedinin smartphone ya da PDA olduğu belirtilmektedir. Ortalama kullanım rakamları göz önüne alındığında ise akıllı telefon ya da PDA kullanıcılarının diğer cep telefonu kullanıcılarına göre %40 daha fazla kayıp veya çalıntı riski taşıdıkları değerlendirilmektedir. Bu riski en aza indirmek ve mobil cihazlarda bulunan verinin güvenliğini temin ederek sadece yetkili kişilerin erişimini sağlayabilmek için aşağıda belirtilen bir dizi güvenlik yöntemi önerilmektedir.

**a. Şifre Koruması**

Kurumda kullanılan tüm mobil cihazlar şifreli şekilde yapılandırılmalıdır. Şifre yetkilendirmesi ile yetkili kişilerin hassas verilere erişimi sağlanmalıdır. Bu yetkilendirme sayesinde kullanıcı yalnızca erişim yetkisine sahip olduğu verilere erişebilecektir.

**b. Şifreleme Desteği**

Eğer kurum, bazı dosyaları ve ayarları mobil cihazda saklamak isterse bunlar şifrelenmiş olarak tutulmalıdır. Bu şekilde şifrelenmiş olarak tutulan dosyalar sadece geçerli anahtara sahip yetkili kullanıcılar tarafından erişilebilecektir.

**c. Uzak Cihaz Yönetimi**

Uzak mobil cihazlar; uzak PC yönetimine benzer şekilde bir yönetim ile kurumun ağına bağlanmak istediklerinde, gerekli olan özelliklerin kontrolü yapılarak cihazların ağa bağlanması sağlanmalıdır. Bu şekilde ağa bağlanmış olan cihaz üzerinde zararlı uygulamaların olmaması sağlanır.

**d. GSM ve UMTS Mobil Telefonlarına ait IMEI Numarası Güvenliği**

GSM ve UMTS Mobil telefonların uluslararası biricik tanımlayıcı numarası olan IMEI'nin başkaları tarafından bilinmesi bir güvenlik riski oluşturmaktadır. Herhangi bir şekilde çalınan veya kaybolan kilitli mobil telefonların kilidi IMEI numarası ile açılabilmektedir. GSM Mobil Telefon operatörleri IMEI numaralarının bulunduğu listeyi güvenli ve erişim kontrollü bir ortamda tutmak zorundadır. Bu liste mobil operatörler tarafından erişilebilen ortak bir

veritabanında yer alıyorsa bu liste kara liste olarak değerlendirilir ve bu listede geçen IMEI numaraları hiçbir şekilde herhangi bir GSM operatörüne kayıt edilemez, mobil iletişimi sağlanamaz.

**e. GSM Mobil Cihazların Ek Güvenliği**

GSM mobil cihazlarında başlıca üç fiziksel dış erişim yolu (dış ara yüzü) bulunmaktadır. Bunlar, ağ bağlantı ara yüzü (anten aracılığı ile bluetooth, IR, GSM, 3G gibi ağ erişim teknolojileri), SIM kartı fiziksel ara yüzü ve tuşlamanın yapıldığı kullanıcı ara yüzüdür. Bu dış ara yüzlerinin güvenliğinin sağlanıyor olması bir gereklilik olup bunun için aşağıdaki yöntemlerin kullanılması söz konusudur.

Ağ bağlantı ara yüzü ile kayıt olunan operatörün kullandığı GSM ve 3G teknolojisi vasıtasıyla, mobil cihaz IMEI numarasını operatöre iletir ve operatör bu numaraya bakarak, duruma göre, bu mobil cihazın GSM ve 3G servislerini kullanılmasına kısıtlama getirir. Bu yöntem mobil cihaz kullanıcısının yetkilendirilmesinden öte mobil cihazın yetkilendirilmesidir.

Diğer bir yöntem ise, mobil cihazın kullanıcısının mobil cihaz tarafından denetimidir. Bu durumda, kullanıcı öncelikle kendini mobil cihaza PIN, parola, gizli şifre ve/veya biyometrik (parmak izi gibi) metotlarla tanıtır ve doğru girilen değere göre kullanıma izin verilir.

Bir başka yöntem olarak, akıllı kart kullanılarak kullanıcının mobil cihaz tarafından kullanıcı denetiminin yapılmasıdır.

## 5.4. Mobil Uygulama Güvenlik Yöntemleri

Mobil uygulama güvenliğini sağlamak için kritik öneme sahip işlemler aşağıda sunulmuştur.

**a. Kimlik Denetimi**

Uygulama katmanı kimlik denetimi, yazılım geliştirme sürecinde uygulanması gereken oldukça önemli bir güvenlik yöntemi olarak tanımlanmaktadır. Geliştirilen uygulama, ister yerel ağ üzerinde yer alan bilgisayar, ister İnternet üzerindeki bir bilgisayar, isterse GSM şebekesi ile kurumsal ağa bağlanan bir mobil cihaz ile kullanılıyor olsun kimlik denetimi mutlaka uygulanması gereken bir yöntemdir. Bu sayede, geliştirilen uygulama üzerinde bulunan verilere yetkisiz kişiler tarafından erişimi önlenir. Bunun yanında, yine bu yöntemin kullanımı ile uygulama üzerinde yapılan işlemlerin sadece yetkilendirilmiş kişiler tarafından yapılması sağlanmış olur.

**b. Uzak Uygulama Yönetimi (Remote Applet Management)**

Uzak uygulama yönetimi geliştirilen uygulamalar ile mobil uygulamalara bağlanacak cihazların gerekli güvenlik özelliklerine sahip olup olmadığı kontrol edilerek güvenli olmayan cihazların uygulamaya erişimi engellenebilmektedir. Bunun yanında, söz konusu uzak uygulama ile mobil cihazlar üzerinde gerekli bağlantı ve güvenlik ayarlarının otomatik olarak yapılması sağlanabilir.

Ancak, uzak uygulama yönetiminin dezavantajları da bulunmaktadır. Bunlar, öncelikle uzak cihaz üzerinde kullanılacak olan uygulamanın işletim sistemi ya da program bağımlılığı gibi nedenlerle geliştirilme zorluklarıdır. Bu dezavantajların aşılması kurumsal olarak tek tip mobil cihaz kullanımı ya da sistem bağımsız yazılımlar geliştirilebilmesi durumunda gerçekleşebilir. Kurumsal hizmetlerin ya da uygulamaların diğer kullanıcıların kullanımına sunulması durumunda ise sistemden bağımsız uzak uygulama geliştirilmesi bir güvenlik önlemi olarak değerlendirilebilir.

**c. İçerik depolama/şifreleme (Content Storage/Encryption)**

Mobil cihazlarda en büyük risk olan çalınma ya da kaybolma riski göz önüne alındığında mobil cihaz üzerinde saklanacak verilerin şifrelenmiş olarak tutulması bilgilerin ele geçirilme riskini azaltmaktadır. Ancak, bu işlemin yapılabilmesi için uygun şifreleme desteğine sahip bir mobil cihaz kullanımı gerekmektedir.

Bu çözüme alternatif olarak geliştirilen bir başka çözüm ise cihaz üzerinde hiçbir verinin tutulmadığı ve ancak uygulama ile bağlantı kurduğu anda verilere ulaşabildiği bir sistem olarak değerlendirilebilecek *Blackberry* ürünüdür.

**d. Sertifika depolama/yönetimi (Certificate Storage/Management)**

Sertifika yönetimi ile oluşturulan sertifikalarla ulaşılan uygulamanın doğruluğu garanti edilebilmektedir. Bu garanti, sahte ya da tuzak uygulamalar kullanılarak mobil cihaz kullanıcısının ulaşmaya çalıştığı uygulamaya ilişkin parola ve erişim bilgileri gibi bilgilerin çalınmasını engellemektedir.

**d. Parola/PIN Koruması (Password/PIN Protection)**

Parola koruması, cihaz kullanımı için yetkilendirme yapılması, cihaz üzerinde bulunan dosyalara erişim yetkilendirmesi ve, uygulama düzeyinde yetkilendirme için kullanılabilmektedir. Ayrıca, PIN koruması diğer kimlik doğrulama araçları için de çok önem taşıyan bir güvenlik unsurudur. Ek olarak, parola koruması ile mobil cihaz üzerinde şifrelenmiş olan verilere erişim daha güvenli hale gelmektedir.

**e. Tek Kullanımlık Parola**

Bir tür kimlik denetim yöntemidir. Tek kullanımlık parola uygulaması şu anda birçok İnternet bankacılığı uygulamasında da kullanılanbir yöntemdir. Bu yöntem ile uygulama üzerinde yapılacak işlem için gerekli kimlik doğrulaması daha önceden sisteme tanımlanmış cihaza uygulama tarafından oluşturulan tek kullanımlık parolanın gönderilmesi ve işlemin tamamlanması için bu parolanın uygulamaya girilerek kimlik doğrulamasının yapılması şeklinde uygulanmaktadır. Ülkemizde bu uygulamanın kullanım alanları tek kullanımlık parolanın SMS ile iletilmesi ya da tek kullanımlık parola oluşturucu cihazlar kullanılması şeklindedir.

**f. Elektronik İmza**

Elektronik imza; başka bir elektronik veriye eklenen, kimlik doğrulama amacıyla kullanılan ve elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlara verilen isimdir. Elektronik imza, sayısal imzayı da içine alan bir üst kavram olup genel bir anlama sahiptir. Bir tarayıcıdan geçirilerek bilgisayara aktarılan ve elektronik metinlerin altında kopyalama yoluyla kullanılan imza gibi en basit yöntemden, kişilerin göz retinası, parmak izi ya da ses gibi biyolojik özelliklerinin kaydedilerek kullanıldığı biyometrik önlemleri içeren elektronik imzaları veya bilginin bütünlüğünü ve tarafların kimliklerinin doğruluğunu sağlayan sayısal imzalara kadar karmaşık yöntemleri içermektedir.

**g. Sayısal İmza**

Sayısal imza, elektronik ortamdaki verilerin doğruluğunun ve güvenilirliğinin kanıtlanması amacıyla geliştirilmiş bir elektronik imza uygulamasının adıdır. Sayısal imza, imzalanan metin ile göre farklılık gösterir ve içeriğin matematiksel fonksiyonlardan geçirilerek eşsiz olduğu düşünülen bir değer bulunması sureti ile elde edilir. Dolayısı ile, sayısal imza ile imzalanan metin arasında mantıksal bir ilişki bulunmaktadır. Diğer bir deyişle, kişilerin, elle atılan imzada olduğu şekilde tek bir imzası yoktur; bunun yerine imzalamada kullanılan anahtarları vardır. Sayısal imza, bir kullanıcı ya da bir kurumdan gönderilen bilgilerin kesinlikle o kuruma veya kişiye ait olduğunu doğrulayarak, verinin başkası tarafından gönderilmediğini garanti eder. Islak imzanın elektronik ortamdaki karşılığı olarak değerlendirilebilecek sayısal imza, aşağıda belirtilen 3 temel işlevi yerine getirmektedir:

- *Kimlik tanıma*: Bir kişinin ya da kurumun kimliğinin onaylanması.
- *Veri bütünlüğü:* Oluşturduğu özet bilgi ile kasten veya kazayla verinin değiştirilemediğini onaylayarak bütünlüğünün korunduğunu ve doğruluğunu garanti eder. Sayısal imza veri gizliliğini sağlamaz.

- *İnkar edilememezlik:* Sayısal imza ile imzalanmış bir belgeyi yollayan kişi, onu yolladığını, alıcı da aldığını inkar edemez.

5070 sayılı Elektronik İmza Kanunu'nda geçen "elektronik imza" kavramı ile sayısal imza işaret edilmektedir. Bu nedenle, hazırlanan bu belgede, elektronik imza ile kastedilen anlam sayısal imza olarak dikkate alınmalıdır.

**h. Elektronik Sertifika ve Nitelikli Elektronik Sertifika**

Elektronik sertifika, sayısal imzanın (5070 sayılı Elektronik İmza Kanununa göre elektronik imza) doğrulanması için gerekli olan veriyi ve imza sahibinin kimlik bilgilerini içeren elektronik kaydı ifade etmektedir. Atılan imzanın doğruluğunun teyit edilebilmesi için gerekli olan elektronik sertifikalar, sözkonusu kanuna uygun olarak faaliyette bulunan elektronik sertifika hizmet sağlayıcılarından temin edilebilmektedir. Elektronik sertifika hizmet sağlayıcısının sertifika üzerindeki elektronik imzası, sertifikanın bütünlüğünü ve doğruluğunu garanti etmektedir.

Nitelikli elektronik sertifikalar; Kanunun 9. maddesinde belirtildiği şekilde "nitelikli sertifika" olduğuna dair bir ibareyi, sertifika hizmet sağlayıcısının kimlik bilgilerini ve kurulduğu ülke adını, imza sahibinin teşhis edilebileceği kimlik bilgilerini, sertifikanın geçerli olduğu süreyi ve sertifikanın seri numarasını barındıran elektronik sertifikalardır. Elle atılan imza ile aynı hukukî sonucu doğuran güvenli elektronik imza oluşturmak için nitelikli elektronik sertifikalara sahip olunması gereklidir.

**i. Mobil İmza**

23 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza (e-imza) Kanunu ile birlikte e-imza uygulamalarının yaygınlaşması e-imzanın bir gereklilik haline gelmesine yol açmıştır. Bununla birlikte, hem e-imza sahip olma hem de okuyucu maliyeti, kullanım, uyum ve taşıma zorlukları gibi sorunlar nedeniyle e-imza sahip olma oranları düşük kalmıştır. Mobil imza (m-imza) ile düşük maliyetli, kullanımı kolay güvenli bir altyapı sağlanarak bu tür zorluklar aşılmaya çalışılmıştır.

M-imza, 5070 sayılı söz konusu kanuna uygun olmak üzere, ıslak imza ile aynı hukuki sonucu doğuran e-imzanın cep telefonu vasıtası ile hızlı ve güvenilir olarak atılması sağlanmaktadır.

M-imza'ya sahip olabilmek için, m-imza hizmeti veren GSM operatörüne geçerli bir kimlik belgesi ile (nüfus cüzdanı, pasaport gibi) başvurulması gerekmektedir. GSM operatörü, m-imza için gerekli elektronik sertifikayı bir Elektronik Sertifika Hizmet Sağlayıcından elde ederek kullanıcının cep telefonu üzerindeki SIM karta yükler. Özel anahtarlar SIM kartta kalacak şekilde yapılan bu işlemve kişi doğrulaması yapıldıktan sonra

en az altı haneli bir m-imza şifresi belirlenerek kullanıma hazır hale getirilir. M-imza, cep telefonu ile çalıştığı, mobil olarak her uygulamada kimlik doğrulaması sağladığı ve düşük maliyetli olması nedeniyle tercih edilir hale gelmiştir. Banka uygulamalarında olduğu gibi, bankaya doğrudan müracaat ile kişinin şahsen doğrulanması da sağlanarak daha güvenli bir hale getirilebilir. Ayrıca uygulamaya erişim parolası, m-imza ve m-imza parolalarının kırılması çok mümkün olmadığından güvenli bir altyapı sağlanmaktadır.

M-imza, e-imzanın bir başka şekli olarak karşımıza çıkmakla beraber özellikle İnternet bankacılığı, e-devlet, e-belediye gibi uygulamalarında kullanışlı bir kimlik doğrulama ve imzalama aracı olarak kullanılmaya başlanmıştır. M-imza uygulama olarak tek kullanımlık parola yöntemine benzemekle beraber ayrıldığı noktalar vardır. M-imza için kullanılacak hattın m-imza sahibine ait olma zorunluluğu tek kullanımlık parola uygulamasında yoktur. Ayrıca, m-imza uygulaması sırasında kimlik doğrulamasının tam olarak sağlanması için imzalama işlemi bir PIN kodu ile yapılmaktadır. Bu sayede, telefon kaybolsa ya da çalınsa dahi imzalama işlemini sadece PIN kodunu bilen kişi tarafından yapılabilmektedir. Ek olarak, m-imza uygulamasında 5070 sayılı kanun kapsamında hukuki sonuçları belirlenmiş güvenilir e-imza kullanılmaktadır.

## 5.5. Mobil Uygulama İletişim Güvenliği

Mobil uygulamalarda güvenlik konusunda en önemli sorunlardan biri iletişim güvenliğinin sağlanmasıdır. Bu uygulamalar için iletişim güvenliğinin sağlanmasında zorluk yaşanmasının nedeni iletişim kanallarının uygulama sahibi kurum tarafından kontrol altında tutulamamasıdır. Çünkü, iletişim güvenliği pek çok noktada GSM operatörü tarafından sağlanan hizmetlere bağımlıdır. Bu bağımlılık, iletişim güvenliği konusunda alınabilecek önlemlerin sayısı oldukça sınırlı tutmaktadır.

### 5.5.1. Güvenli Veri Değişimi (Secure Data Exchange)

Güvenli veri değişimi iletişim sırasında mobil cihazdan uygulamaya ya da uygulamadan mobil cihaza gönderilen verilerin şifrelenmiş olarak iletilmesini sağlar. Bu şifreleme ile, veri iletişimi sırasında herhangi bir noktada ortaya çıkabilecek olan güvenlik eksikliği ya da saldırı nedeniyle veri sızması durumuna karşılık bir güvenlik katmanı oluşturulmuş olur.

Örnek olarak, IMEI numarasına bakılarak erişilen bir web sitesindeki uygulamanın yetkilerinin denetlenmesi için, web uygulaması gelen IMEI numarasının güvenli bir şekilde iletişimi sağlanmalıdır.

### 5.5.2. Sanal Özel Ağ (Virtual Private Network)

Sanal özel ağ, 2. kuşak GSM protokollerinden itibaren kullanılabilmektedir. Yeni kuşak teknolojilerin de devreye girmesi ile hızlanan ve gelişen ağ yapısı sanal özel ağ kullanımını kolaylaştıracaktır. İletişim güvenliğinin sağlanabilmesi için birden fazla ağın birbirine bağlanması gerekmektedir.

Bu noktada yapılması gereken; kurum ağı ile operatör ağı arasında oluşturulacak bir sanal özel ağ ile bu iletişimin güvenliğinin sağlanması ve bunun yanında, mobil cihazın uygulama erişim sırasında operatör ile arasında sanal özel ağ bağlantısı kurulması olabilir.

Bir başka yöntem ise, uygulama erişimi başlatılmadan önce mobil cihazın kurum ağına sanal özel ağ bağlantısı kurmasının sağlanmasıdır. Bu sayede, operatör ağından bağımsız olarak güvenli ağ bağlantısı kurulması sağlanır.

## 5.6. Mobil Uygulama Güvenlik Mühendisliği Yöntemleri

Mobil uygulamalarda genellenebilecek ve tüm mobil cihazlara uygulanacak bir güvenlik yönteminden bahsetmek zordur. Bu durumun en büyük nedenlerinden biri mobil cihazlarda kullanılan farklı işletim sistemlerinin olması, farklı mobil operatörlerinde farklı güvenlik politika ve önlemlerinin devreye alınması, operatörlerin farklı sertifikasyon süreçlerine sahip olmasıdır.

Bu bölümde, herhangi bir mobil uygulama geliştirilirken dikkat edilmesi ve göz önüne alınması gereken güvenlik yöntemlerine yer verilmiştir.

### 5.6.1. Korunmasızlık Analizi

Hazır bir mobil uygulama kullanılması durumunda, mobil uygulama kaynak kodu üzerinde korunmasızlık analizi gerçekleştirilmesi önem taşımaktadır. Bununla beraber, mobil uygulamanın kullanıma yönelik korunmasızlık analizi yapılması gerekmektedir.

Korunmasızlıklar; hazırlanan ve/veya kullanılan mobil uygulamanın güvenlik kısıtlarından, bütçe ve zaman yetersizliğinden, işlevsellik gereksinimlerinin güvenlik gereksinimlerine aykırı düşmesinden, kullanılan teknoloji ve uygulama geliştirme araçlarının güvenlik zafiyetlerinden, mobil uygulama teknolojilerinden, mobil uygulama güvenlik gereksinimlerinin doğru belirlenememesinden kaynaklanabilmektedir.

Korunmasızlık Analizi öncesi mobil uygulamanın *güvenlik hedefleri* belirlenmelidir. Güvenlik hedefleri aşağıdaki şekilde gruplanabilir [37]:

**a. Uygulamanın Kimlik Hedefleri**

Uygulamanın yanlış ve kötü amaçlı kullanımları engellemesi, kullanıcının gerçek kullanıcı olup olmadığının doğrulanması bu hedefler arasındadır.

**b. Finansal Hedefler**

Uygulamadan ötürü olabilecek herhangi bir potansiyel finans kaybında, kurumun ne kadarlık bir riske tahammül edebileceği bu hedefler arasındadır.

**c. Mahremiyet ve Uyumluluk Hedefleri**

Uygulamanın kullanıcı özel ve gizli bilgisini hangi seviyeye kadar koruyabildiği, kullanılan uygulama türünden ve kurumsal olarak bağlı olunan yasa ve yönetmeliklerden kaynaklanan hedefler bu kapsama dahil edilebilir.

**d. Servis Seviyesi Hedefleri**

Uygulamanın süreklilik gereksinimleri, yüksek maliyetler gerektirmeyen ancak servis süreklilik seviyesini yükselten kontrol hedefleri bu kapsama dahil edilebilir.

**e. Kurumsal İtibar Hedefleri**

Uygulamanın kötü amaçlı kullanım ve/veya bir güvenlik saldırısına uğraması durumunda kurumsal itibarın zedelenmesi kriterleri bu kapsama dahil edilebilir.

İkinci aşama olarak mobil uygulama gözden geçirilmelidir. Bu aşamada, uygulama bileşenleri, uygulama iş akışları ve uygulamanın kurum dışı sınır bilgi alışverişi incelenmelidir. En verimli uygulama gözden geçirme yöntemlerinden biri uygulama tasarım ve mimari dokümanının incelenmesidir.

Üçüncü aşama, uygulamanın ayrıştırılmasıdır. Ayrıştırılma işlemi, uygulama mimarisi anlaşıldıktan sonra, güvenlik açısından etkilenecek özellik ve modüllerin ayrı ayrı ele alınmasıdır. Bir modül ayrıştırıldığında, bu modüle ne tür verilerin girildiği, ne tür işlemler yapıldığı, verinin nasıl işleme tabi tutulduğu gibi detay alt süreçler belirlenir.

Dördüncü aşamada tehdit analizi ve modellemesi yapılmalıdır (Bknz. 5.6.2)

Son aşama Korunmasızlık analizinin yapılmasıdır.

### 5.6.2. Tehdit Modelleme

Hazır veya geliştirilecek bir mobil uygulama için, mobil uygulamaya yönelik olası tehditler belirlenmelidir. Tehdit Modellemesi aşağıdaki aşamalardan oluşmalıdır [38].

- Mobil Uygulamaya ait olası saldırı ve tehditler tespit edilmelidir.
- Tespit edilen tehdit ve korunmasızlıkların kolay yönetilmesini sağlamak için gruplanmalıdır.

- Tespit edilen tehditlere karşılık gelen ve Bölüm 4.1'de yer alan Korunmasızlıklar belirlenmelidir (bir tehdit birden fazla korunmasızlıktan yararlanabilir veya bir korunmasızlık birden fazla tehditin yararlanmasına neden olabilir).
- Tehdit Modelleme için aşağıda listesi verilen uluslararası kabul görmüş yöntemler kullanılabilir:
  - AS/NZS 4360:2004 Risk Yönetimi
  - OWASP Kılavuzları
  - Microsoft Tehdit Modellemesi ( STRIDE/DREAD Modelleme)
  - NIST 800-30 Kılavuzları

Bilinmeyen tehditlerin belirlenmesi mümkün olmadığı için öncelikle bilinen tehditler tespit edilmelidir. Aşağıdaki iş adımları tehdit modellemede kullanılabilir:

**a. Saldırı Ağaçlarının Oluşturulması**

Mobil Uygulamalardaki bilinen ana saldırılar Bölüm 4.2'de verilmektedir. Her bir saldırının, alt saldırı aktiviteleri oluşturularak ve herbir alt aktivite için uygulamanın tasarımında yapılması gereken önlemler belirlenir veya hazır bir uygulaması durumunda alınması gereken önlemler belirlenir.

**b. Tehditlerin Belgelendirilmesi**

Tüm tehdit ve alt aktivetleri belgelendirilmelidir.

**c. Tehditlerin Puanlanması**

Tehditlerin zarar gücüne ve oluşma olasığına göre puanlanması gerekmektedir.

### 5.6.3. Tasarım

Tehdit Modelleme ve Korunmasızlık analizi yapılan mobil uygulamanın tasarımına özgü güvenlik gereksinimleri ve önlemleri oluşturulmalıdır.

Aşağıdaki maddeler bir mobil uygulamada bu amaçla yapılabilecek yetkili veya yetkisiz işlemlerdir. Bu işlemlerden hangilerine nasıl bir yetki verileceği gözden geçirilmelidir.

- Yerel Bağlantı
- Net Erişim
- Okuma Konfigurasyon Verisi
- Okuma SIM Verileri
- Çoklu Ortam Kaydı

- Okuma Kullanıcı Verileri
- Yazma Kullanıcı Verileri
- Yazma SIM Verileri
- Mesajlaşma
- Otomatik Uygulama Çağırma
- Telefon Çağrı
- Yazma Konfigürasyon Verileri
- SIM Dayalı Sayısal İmza/Seritifika
- Konum Bilgisi
- DRM (Güvenli Veri Dağıtımı)
- Okuma/Yazma Uygulama Verileri
- Süreç Yönetimi

Mobil uygulamalarda güvenlik tasarımına başlamadan önce korunmasızlık analizi ve tehdit modellemesi mutlaka yapılmalıdır. Her platformda çalışacak tek bir uygulamanın geliştirilmesi ve Operatörlerle beraber test senaryolarının ortaya çıkartılması gerekmektedir.

### 5.6.4. Uygulama Kodunun Gözden Geçirilmesi

Güvenlik açıklarını ve zaafiyetleri uygulama hizmete alındıktan sonra gidermeye çalışmak hem beklenmedik ek kaynak ve maliyet yükleri getirmekte hem de uygulama projelerinin devreye alınmasını geciktirmektedir. Bu nedenle, uygulama geliştirme yaşam döngüsü süresince uygulamanın güvenlik özellikleri açısından gözden geçirilmesi gereklidir.

Uygulamanın gözden geçirilmesi uygulamanın davranış şeklinin akıllı yazılımlar kullanılarak otomatik olarak incelenmesi şeklinde tanımlanır. Uygulama gözden geçirme yöntemleri iki farklı teknik yaklaşım altında gruplanmaktadır [39]:

**a. Statik Gözden Geçirme**

Uygulama çalıştırılmaksızın kaynak kodu ve/veya obje kodu özel olarak geliştirilmiş yazılımlar kullanılarak çoğunlukla bir uzmanın gözetimi altında analiz edilir.

**b. Dinamik Gözden Geçirme**

Uygulama gerçek veya sanal bir işlemcide çalıştırılarak işleyişi sırasında gözden geçirilir. Uygulama kontrollü bir ortamda tekrarlı olarak hata durumları ve açıklar için sınanır. Bu amaçla geliştirilmiş birçok açık kaynak kodlu ve ticari yazılımlar bulunmaktadır (örneğin,

Holodeck, Valgrind). Bu yazılımlar, uygulamadaki bellek sızıntılarını, kapasite sorunlarını ve güvenlik zaafiyetlerini ortaya çıkartabilmektedir.

Uygulama kodlarının gözden geçirilmesi esnasında özellikle tehdit ve açıklık analizi yapılmalıdır. Açıklık analizi için genel ve uygulamaya bağlı senaryoların tanımlanması gereklidir. Genel senaryolar bilinen saldırılar ve açıklıklar için yapılır. Uygulama özel saldırı zayıflıklarının bulunması için uygulama analiz ve tasarımıyla beraber kaynak kodları da incelenmedir. Uygulamanın gözden geçirilmesi işlemi, döngüsel olarak hedeflenen güvenlik seviyesi elde edilene kadar ve her kod iyileştirme adımında tekrarlanmalıdır [40].

### 5.6.5. Uygulamanın Güvenli Olarak Hizmete Alınması

Uygulamanın güvenli bir şekilde hizmete alınması, üretim ortamının korunması açısından önemlidir. Bu nedenle, uygulamaların güvenli olarak test edildikten sonra imzalanması için bir sertifikasyon süreci oluşturulmalıdır. Uygulamanın hizmete alınmasından önce üretim ortamlarındaki gereksinimler açık ve tam olarak tanımlanmalı ve son sürüm bu gereksinimler doğrultusunda düzenlenerek bütünlüğünün bozulmadığı garanti edildikten sonra hizmete alınmalıdır.

### 5.6.6. Mobil Uygulama Hayat Döngüsündeki Güvenlik Yöntemleri

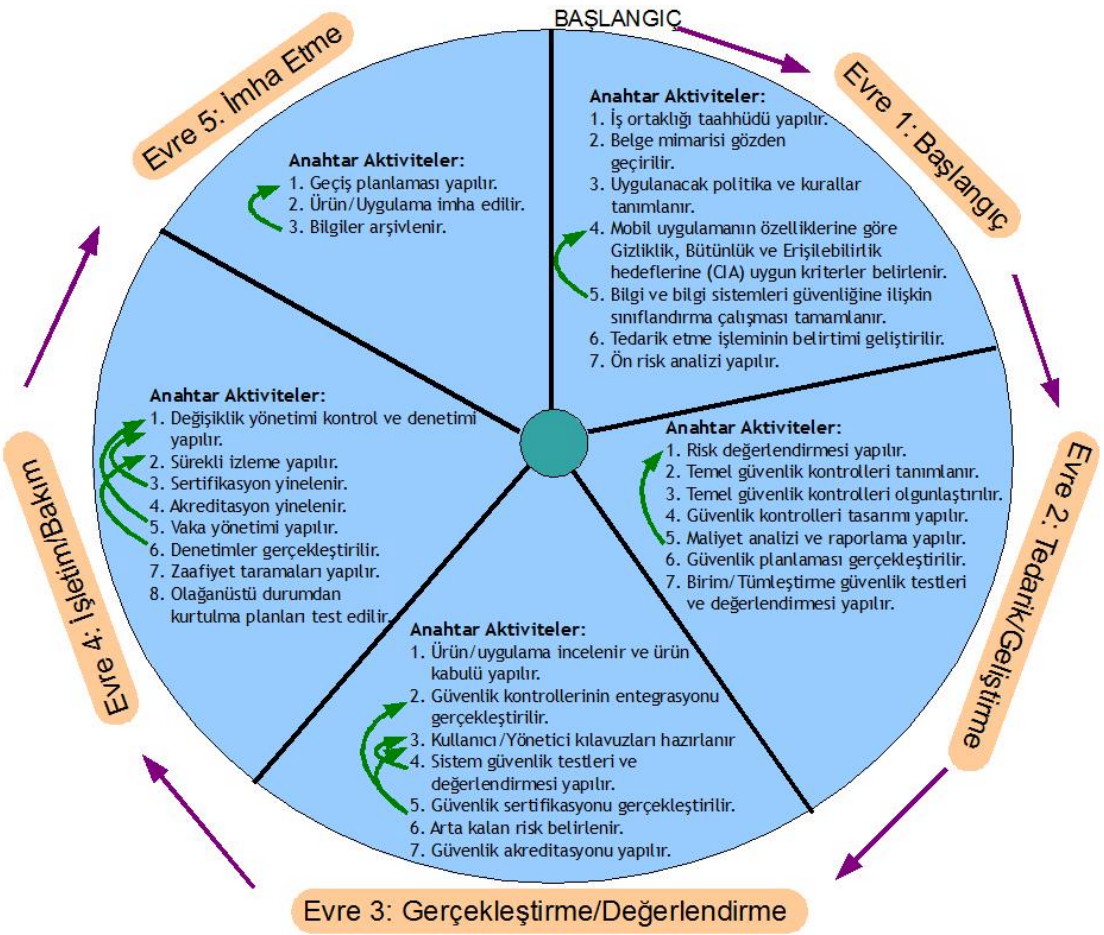
Mobil uygulama güvenliği, uygulama geliştirme yaşam döngüsü (SDLC: System/Software Development Life Cycle) içerisindeki tüm aşamalarda (planlama, analiz, tasarım, geliştirme, bakım ve iyileştirme) güvenlik politikasında saptanan ilkeler ve ilgili varlıklar doğrultusunda belirlenen tehditler ve saptanan zaafiyetlere göre mobil uygulamanın güncellenmesini amaçlayan yöntemleri kapsamaktadır. Uygulanan güvenlik yöntemleri kabul görmüş bilgi güvenliği standartlarına uygun olmalıdır [41, 42].

Güvenlik politikaları, yaşam döngüsü boyunca uygulanmadıkça güvenlik seviyesi konusunda gerçekçi ve güncel bilgi sahibi olmak mümkün değildir. Dolayısıyla mobil uygulama, tüm yaşam döngüsü boyunca tekrar eden bir şekilde zafiyet taramalarından geçirilmeli, tehdit analizleri sürekli olarak yinelenmeli ve risk faktörleri güncellenmelidir. Güvenlik boyutunun uygulama geliştirme yaşam döngüsünün tüm aşamalarına dahil edilmesine yaklaşımı güvenli uygulama geliştirme yaşam döngüsü (S-SDLC) olarak adlandırılmaktadır.

Mobil uygulama yaşam döngüsü klasik uygulama yaşam döngüsü ile temel olarak aynıdır. Ancak, mobil uygulamaların etkileşimli yapıları ve çok çeşitli ortamlarda hizmet vermeleri güncelleme ve iyileştirmelere çok daha açık olmalarına neden olmaktadır. Bu nedenle, mobil uygulamaların geliştirilmesinde son yıllarda oldukça popüler hale gelen çevik programlama (*agile programming*) yöntemlerinin kullanılması değerlendirilmektedir. Çevik

programlama yöntemlerinde uygulama geliştirme yaşam döngüsüne başlanırken kapsamlı bir ön tasarım çalışması ve uzun dönemli planlama yapılmamaktadır. Uygulama geliştirme yaşam döngüsü boyunca yinelenen çalışma bölümlerinde (*Sprint*) planlama, tasarım, geliştirme ve test aşamaları olgulaştırılarak tekrarlanır. Tasarım ancak uygulama geliştirme süreci tamamlandığında sonlandırılmış olur. Güvenlik gereksinimlerin karşılanması da bu yaklaşıma uygun olarak değerlendirilebilir. Buna göre, uygulama geliştirme döngüsünde her çalışma bölümünde zaafiyetler ortaya konulmalı, tehdit analizi yapılmalı ve gereksinimlere göre güvenlik önlemleri alınmalıdır.

Şekil 7'de, uygulama geliştirme yaşam döngüsünün güvenlik ilkelerine uygun şekilde yönetilmesine ilişkin olarak NIST tarafından önerilen yaklaşım gösterilmiştir.




**Şekil 7: Güvenlik İlkelerine Uygun Uygulama Geliştirme Yaşam Döngüsü**

# 6 MOBİL UYGULAMA GÜVENLİK TESTLERİ

## 6.1. Mobil Uygulama Güvenlik Testleri Giriş

Bilişim Teknolojilerinin her alanında güvenliğe en üst düzeyde önem verilmesine karşın, uygulama güvenliğine ilişkin testler az anlaşılmış ve tam olarak tanımlanmamış bir konu olarak görülmektedir. Uygulama güvenliği testleri, geleneksel uygulama testlerinden daha geniş ve çok yönlü alan uzmanlığı gerektiren oldukça kapsamlı ve farklı yaklaşımlar içeren bir çalışmadır. Mobil uygulamalarda güvenlik testleri ise, gerek kullanılan mobil aygıtların ve iletişim altyapılarının çeşitliliği gerekse kullanılan teknolojilerin karmaşıklığı nedeniyle daha fazla çaba ve özen gösterilmesi gereken bir konudur [43].

Açık platformları destekleyen mobil aygıtların sayısı ve oranı her geçen gün artmaktadır. Açık platformlar bir yandan mobil uygulamaların daha esnek ve hızlı bir şekilde geliştirilmesini sağlarken bir yandan da açık kaynak kodlarına ve uygulama yazılımı geliştirme ara yüzlerine (API) sınırsız erişim imkanı sunmaktadır. Bu nedenle mobil uygulamalar, bu uygulamaları kullanan aygıtlar ve/veya iletişim ağları için her geçen gün artan bir tehdit unsuru olarak ortaya çıkmaktadır. Açık kaynak kodlu işletim sistemi kullanan bir çok mobil aygıtta mobil uygulama güvenliğine ilişkin önlemler endüstri çalışma grupları (GSM Association ve Open Mobile Terminal Platform) tarafından oluşturulan tavsiyeler uyarınca bir şekilde sağlanmış olsa da mobil uygulamalardan kaynaklanan güvenlik zafiyetleri giderek artmaktadır.

## 6.2. Uygulama Güvenliği Testleri İçeriği

Uygulama güvenlik testleri uygulamalardaki zafiyetleri, eksiklikleri ve güvenlik açıklarını ortaya çıkarmayı amaçlayan sürecin genel adıdır. Güvenlik testleri uygulama ve uygulama verisinin sadece yetkilendirilmiş kişilere ve yetkilendirildikleri işlemler için erişilebilir olup olmadığını denetlemektedir. Güvenlik testlerini uygulama geliştirme yaşam döngüsünün (software development life cycle, SDLC) tüm evrelerinde uygulanmalı ve bu şekilde zafiyetlerin zamanında ve tam olarak tespiti sağlanmalıdır. Buna karşın, güvenlik testleri çoğunlukla uygulama geliştirme yaşam döngüsü tamamlandıktan sonra gerçekleştirilebilmektedir [44, 45].

Uygulama zafiyetlerinin tespitinde kullanılan araçlar temel olarak iki grupta değerlendirilir: Penetrasyon testleri (Kara Kutu Testleri), uygulama zafiyet tarama testleri olarak bilinen ve güvenlik birimleri tarafından en çok uygulan test yöntemidir. Kaynak kodu analiz testleri (Beyaz Kutu Testleri) ise uygulama kaynak kodundaki zafiyetlerin *otomatik* ve/veya *manuel* olarak tespitini gerçekleştiren test yöntem ve araçlarını kapsamaktadır.

İnsan beyni belirli bir büyüklük üzerindeki yazılımların karmaşık iş akışlarını analiz ederek olası tüm uygulama yollarındaki zafiyet noktalarını tespit edemeyeceğinden kaynak kodu analiz testlerinde çeşitli yazılımlar kullanılmaktadır. Çoğunluğu açık kaynak kodlu olan bu yazılımlardan bazıları Codenimicon [46], FlawFinders, Rats, Gnu Profiler, Valgrind vb.'dir. Hem Siyah Kutu Testleri hem de Beyaz Kutu testlerinde zafiyet tespitleri, dünya çapında web uygulama güvenliğini arttırmayı amaçlayan Açık Web Uygulama Güvenliği Projesi (The Open Web Application Security Project - OWASP) [47] topluluğu tarafından yapılan uygulama hata kodları sınıflandırmasına uygun şekilde gerçekleştirilmektedir.

Mobil uygulamalarda güvenlik testleri, uygulama güvenlik testlerinin özelleşmiş bir alt kümesini oluşturduğundan kullanılan test araçlarının uygulamaya göre uyarlanması gerekmekle beraber izlenmesi gereken test süreci temel olarak aynıdır. Mobil uygulamalarda kullanılan XHTML standardı, XHTML standardının daha az sayıda ve özelleşmiş formda etiketini (*tag*) içeren bir alt kümesidir. Mobil XHTML kullanmakta olan bir uygulamanın zafiyet tarama işleminde kullanılan güvenlik sızma test aracının uygulamaya göre düzenlenmesi gerekebilmektetir. Bunun yanında, uygulamanın geliştirildiği platformun teknik özellikleri ve mobil cihazların teknik özellikleri de test araçlarının seçilmesi ve uyarlanması konusunda doğrudan etkilidir. Örneğin, Symbian işletim sistemi için geliştirilen mobil uygulamanın güvenlik testiyle Windows Mobile işletim sistemi için geliştirilen mobil uygulamanın teknik özellikler kapsamında farklı olarak ele alınması uygun olmaktadır [48].

Mobil sistemler için en önemli risk unsurlarından birini çok çeşitli kaynaklardan indirilebilen ve platform bağımsız olarak kolaylıkla çalıştırılabilen programcıklar (*Applet*) oluşturmaktadır. Çoğunlukla Java programlama dili ile geliştiriilen ve HTML sayfası içinden çağrılabilen programcıklar, sunucundan istemci cihaza transfer edilerek istemci üzerinde web tarayıcı tarafından sanal java makinesi üzerinde çalıştırılmaktadırlar.

Mobil uygulamalar için çok uygun olan java programcıkları "bir kere yaz her yerde çalıştır" (write once run verywhere) yaklaşımıyla geliştirilmiştir. Programcıklar farklı ortamlar ve sanal makineler (java virtual machine) ile değişik web tarayıcılarında çalışabildiğinden belirlenmiş kısıtlı sayıda ortam için geliştirilen ve çoğunlukla tek bir test ortamında sınanan geneksel uygulamalardan farklı olarak çok çeşitli test ortamlarında test edilmeleri gerekmektedir. Web tarayıcılar geometrik taleplere farklı yanıt verebilmekte (örneğin. uygulama menülerini farklı gösterebilmekte) ve kullanılan güvenlik modeli tarayıcıdan tarayıcıya değişebilmektedir. Bu nedenlerle, programcıklar için her yerde test (*test every where*) yaklaşımına ek olarak tüm tarayıcılarda çeşitli kullanıcı konfigürasyonlarında test (*test on every browser, in various user set configurations*) yaklaşımı benimsenmelidir [49, 50].

Programcıklar çoğunlukla grafik arayüzü olan görsel programlardır ve kullanıcının veri girişi yapabilmesi için pencere araçları (Widget) kullanırlar. Programcıklar "sandbox" adı verilen güvenlik modeline uygun olarak yazılmalıdırlar. Bu güvenlik modelinde, programcık istisnai işlemler dışında yerel sistem kaynağına erişememektedir. Ancak, yerel diske okuma/yazma ve yerel süreçler (process) çalıştırma olarak tanımlanan bu istisnai işlemler çok ciddi güvenlik zafiyetleri oluşturmaktadır. Programcıkların güvenlik testlerinde, olası tüm kullanıcı davranışları, veri girişleri ve sistem kaynağına erişim durumları için uygulama açıklarını test edecek otomatik test programları (test harness) kullanılmalıdır. Bu test programlarına örnek olarak, java dili ile yazılan programların grafik kullanıcı arayüzlerinin test edilmesinde kullanılan JavaStar [51] verilebilir. Test programının tasarımı ve geliştirilmesi veya hazır bir program kullanılacaksa seçimi güvenlik testinin başarısı açısından çok önemli bir unsurdur.

## 6.3 Mobil Uygulama Güvenlik Test Süreci

Uygulama güvenliği test süreci, tehdit ve zafiyetlerin belirlenmesi ve analizlerinin yapılmasının ardından güvenlik risk ve ihtiyaçlarına göre uygulamanın işlevselsellik ve kullanıcı açısından kritik bölümlerinde veya tümünde güvenliğinin geliştirilmesini hedefleyen çalışmaları kapsamaktadır.

Güvenlik test sürecinin adımları şunlardır:

- Tehdit ve zaafiyet analizi kapsamında varlık temelli olarak tehdit profilleri ve zaafiyetler belirlenir.
- Güvenlik test gereksinimlerinin belirlenmesi amacıyla erişilmek istenen uygulama güvenlik düzeyi, uygulamanın teknik ve işlevsel özellikleri, ilgili standartlar ve çevresel faktörler, maliyet-kazanç ve risk analizleri yapılır.
- Belirlenen güvenlik test gereksinimleri uyarınca öncelikler, test araçları ve özellikleri, test zaman planı ve en önemlisi testin amaçları tanımlanır.
- Test kriterleri ve metodu belirlenir. Kullanılacak test metodundan çıkan sonuçlarının ne şekilde değerlendirilerek kabul edileceği saptanır.
- Kullanılacak test metodu hazırlanır, uygulanır ve sonuçları değerlendirilir.
- Son iki adımın, güvenlik öncelikleri tekrar tekrar değerlendirilerek döngüsel bir şekilde hedeflen güvenlik düzeyi sağlanana kadar uygulanır. Hedeflenen güvenlik düzeyi sağlandığında test sonuçlandırılır. Test sonuçlar raporlanır ve daha sonraki uygulamalarda yararlanılmak üzere derlenir.

# 7 MOBİL UYGULAMALARDA ÇALIŞMA GRUPLARI, İYİ UYGULAMA ÖRNEKLERİ VE ULUSLARARASI STANDARTLAR

## 7.1. Güvenlikte Standart Kullanmanın Yararları

Günlük hayatta standartların yararlarından ve öneminden bahsedilir, peki bunlar nelerdir? Standart kullanılmaz ise ne tür kayıplar söz konusudur?

Standart kullanmanın en önemli yararı kullanıcıya güven vermektir. Standart bir ürünün amacına uygun çalışacağı, belirli bir kaliteye sahip olacağı, başka ürünlerle uyumlu, sağlıklı ve esnek olduğu bilinir. Standart ürünler ve servisler genel olarak güvenilir ve kabul görmüş ürünler olarak algılanmaktadırlar. Teknoloji açısından bakıldığında ise, mevcut kazanımların paylaşılması ile üst düzey kalitede yeni ürünlerin geliştirilmesinde önemli rol oynamakta, birlikte çalışabilirliği artırmakta ve toplam maliyette düşüşe neden olmaktadır. Ek olarak, hukuki süreçlerin ve politikaların belirlenmesinde standartlar esas alınır veya standartlar ile desteklenir.

Güvenlik, özelde mobil güvenlik, konusunda da standart kullanmak yukarıda belirtilen avantajları da beraberinde getirmektedir. Mobil cihazların ve platformların güvenliğinin sağlanmasında karşılaşılan kısıtlar ve problemler, karşı karşıya kalınan tehditlerin boyutu bu sürecin daha sistemli dolayısı ile belli bir standart altında yönetilmesini gerektirmektedir. Özetle, güvenlik alanında standartlaşmanın getirdiği temel avantajlar şu şekilde sıralanabilir [52]:

- Mobil cihazlar ve platformlar arasında birlikte çalışabilirlik ve dolayısı ile araştırma ve geliştirme maliyetlerinin düşürülmesi,
- Özellikle mobil teknolojide kısıtlı olan uzman kaynağının etkin bir şekilde kullanılmasını, anahtar kelimlerin önceliklendirilmesinin sağlanması,
- Cihazların amacına uygun kullanımına yönelik güven, bunun sonucunda mobil cihaz kullanımının ve servislerinin yaygınlaştırılmasının sağlanması,
- Geliştirilen yöntemlerin yeni teknolojilere uyarlanmasının daha hızlı ve düşük maliyetle sağlanması,
- Hukuki süreçlerin ve politikaların belirlenmesinde temel oluşturması.

Günümüz iletişim ortamında mobil kullanımın yaygınlaştırılmasının ana hedef olarak belirlendiği göz önüne alındığında, son kullanıcının güveninin kazanılması kritik bir öneme sahiptir. Kullanıcıdan bağımsız, güvenilir, düşük maliyetli, esnek ve standart bir güvenlik altyapısı tesisi bu hedefe ulaşılması yolunda büyük katkı yapacaktır.

## 7.2. Uluslararası Standart, Grup ve Organizasyonları

Mobil güvenliğini tüm yönleri ile ele alan standart bir çalışma henüz bulunmamaktadır. Ancak, mobil platformlarda güvenliğin ve güvenin artırılmasına yönelik olarak küresel boyutta önemli kuruluşlar ve gruplar çalışmalar yapmaktadır. Yapılan çalışmaların sonuçları tavsiye niteliğinde önerileri içeren yayın ve belgeler şeklinde olmakta birlikte standartlaşmaya gidebilecek gereksinim ve belirtimleri de içermektedir. Aşağıda bu konuda çalışmaları sürdüren organizasyonlar ile uluslararası kuruluşların kısa tanıtımları ve çalışmaları yer almaktadır.

### 7.2.1. GSM Association (GSMA)

GSM Association (GSMA), dünya çapında faaliyet gösteren 850 civarında mobil telefon operatörü ile 200 civarında üretici ve sağlayıcıdan oluşan küresel bir organizasyondur [53]. Temel faaliyet alanı kablosuz servislerin mümkün olduğunca verimli ve yaygın şekilde küresel kapsamda çalışmasının sağlanmasına odaklanmış olup, gerek kişisel kullanım gerek de ulusal kullanımda yeni olanakların yaratılmasına önayak olmaktadır. Bu kapsamda, özellikle mobil uygulamalarda güvenilir bir ortam oluşturmak amacıyla bir grup (Mobile Application Security – MAS) kurulmuş ve proje başlatmıştır. Bu grup, uygulamaların sertifikasyonunu temel alan yaklaşımları ile mobil uygulamalarda 4 seviyeli bir güven sınıflandırması önermiştir:

- *Güvenilmez:* Uygulamanın için herhangi bir sertifikasyon yoktur, düşük güvenlik seviyesine sahiptir.
- *Güvenilir:* Üçüncü taraf sertifikasyonu sağlanmaktadır (Java verified gibi), orta derece güvenlik seviyesine sahiptir.
- *Yüksek derecede güvenilir:* GSM operatörü tarafından yönetilen sertifikasyon sağlanmaktadır, yüksek derece güvenlik seviyesine sahiptir.
- *Üretici:* Üretici firma tarafından sertifikasyon sağlanmaktadır, yüksek derece güvenlik seviyesine sahiptir.

Grup, mobil uygulama sertifikasyon süreci ile ilgili tavsiye ve bulgularını içeren, tüm tarafların yararlanabileceği bir belge hazırlamış ve yayınlamıştır.

### 7.2.2. The Trusted Computing Group (TCG)

TCG, birçok platformda cihaz ve ek donanımları için donanım ve yazılım destekli güvenlik teknolojileri tasarlayan ve geliştiren, açık standartlar oluşturan kar amacı gütmeyen bir organizasyondur [54].

TCG bünyesinde IT güvenlik alanları için özel çalışma grupları oluşturulmuştur. Bu çalışma gruplarından bir tanesi de mobil cihazların güvenliğine yönelik çalışmalarda bulunan Mobil Telefon Çalışma Grubudur. Mobil cihazların sınırlı kapasite, bağlanabilme çeşitliliği gibi kendine has özelliklerin ele alan grup, mobil güvenilir modüller için özellik, şartname, belirtim ve standartlar geliştirmektedir. BT altyapısı, yedekleme, sunucular, güvenlik gibi birçok alanda belirtimler geliştiren TCG, bu tecrübesini ve bilgi birikimini mobil dünyaya uyarlamaya çalışmaktadır. 2006 yılında çıkardığı belirtim belgesinden [18] sonra Haziran 2007'de mobil platformlar için ilk açık güvenlik standardını oluşturmuştur.

TCG, pazarda liderlik yapan üretici firmalarla da işbirliği yaparak mobil güvenlik alanında aşağıda belirtilen hususları hedeflemektedir:

- Mobil telefonlar başta olmak üzere tüm mobil cihazlarda genel güvenlik özelliklerini artırmak,
- Donanım ve yazılımlarda birlikte çalışabilirliği sağlamak,
- Son kullanıcılara güvenilir bir mobil ortam sağlamak.

TCG geliştirdiği belirtim belgesinde güvenliğin 5 temel prensibi olan kimlik denetimi, veri bütünlüğü, gizlilik, inkar edilemezlik ve güvenlik politikasına yönelik olarak aşağıda belirtilen 11 adet kullanım senaryosu belirlemiş ve mobil güvenliği bu senaryolar üzerinden incelemiştir [55]:

- Kullanıcı veri koruması ve gizliliği
- Platform bütünlüğü
- Cihaz kimlik tanınması
- Sayısal Hak Yönetimi (DRM)
- SIM kilidi ve cihaz kişiselleştirilmesi
- Güvenli yazılım indirimi
- Cihaz ve üzerindeki bilgilerin korunmasını sağlayan UICC kartı arasındaki güvenli kanal
- Mobil ödeme
- Yazılım kullanımı
- Son kullanıcıya bütünlüğün ispat edilmesi
- Mobil bilet

TCG tarafından üretilen belirtim belgeleri kamuya açıktır [55].

### 7.2.3. Open Mobile Terminal Platform (OMTP)

Open Mobile Terminal Platform (OMTP) 2004 yılında kurulmuştur. Güvenlik, kullanıcı deneyimleri ve cihaz yönetimi konularında çalışmalar yapmaktadır. Donanım ve yazılım üreticileri, mobil şebeke operatörleri gibi alanlardan Nokia, Samsung, Motorola, Sony Ericsson gibi üyeleri bulunan grup, güvenlik ve donanım konusunda tavsiye niteliğinde belgeler üretmekte ve yayınlamaktadır. Uçtan uca mobil kullanıcı servislerinin geliştirilmesi ve mobil iş olanaklarının büyümesini ana amaç edinen organizasyon, daha çok mobil güvenlik konusunda yaptığı çalışmalarla tanınmaktadır [56].

OMTP'nin mobil güvenlik alanında yaptığı çalışmalar son kullanıcı, uygulama geliştiricileri ve iş dünyasına yönelik güvenlik önlemlerini ve tavsiyelerini içermektedir.

OMTP'in güvenlik çerçevesinde, Mobil uygulamaların bütünlülüğünün ve doğruluğunun kontrol edilme durumuna göre 5 farklı güven seviyesi belirlenmiştir [17]. Kontrol mekanizması için Açık Anahtar Altyapısı (PKI) esas alınmıştır. İmzalanmamış veya uygulama geliştiricinin kendi oluşturduğu imza ile imzalanmış bir uygulama en düşük güvenlik seviyesi sınıfına girerken, cihaz üreticisinin imzaladığı ve onayladığı uygulamalar yüksek güvenli kategorisinde yer almaktadır. Bu çerçeve ile son kullanıcılar mobil cihazlarına uygulama yüklenmesi esnasında uygulamaların güvenliği konusunda karar verme aşamasından önemli ölçüde bilgiye sahip olabilmektedir. Uygulama geliştiriciler açısından bakıldığında ise, imzalama altyapısının kullanımı ile birlikte geliştiriciler mobil cihazların fonksiyonlarını daha fazla kullanabilmekte ve yaratıcı çözümler üretebilmektedir.

OMTP'nin güvenlik konusunda yaptığı çalışmalara mobil şebeke operatörleri, mobil cihaz üreticileri ve sağlayıcıları katkıda bulunmaktadır. Bu sayede, mobil platform güvenliği konusunda kamuda bulunan tedirginliği yok edecek güvenli bir ortamın sağlanması dolayısı ile mobil iş dünyasının gelişimi hedeflenmektedir.

AT&T, T-Mobile, Vodafone gibi lider mobil operatörlerin de üye olduğu, mobil web servisleri için standart oluşturma çalışmaları yapan BONDI girişimi [57] OMTP tarafından desteklenmektedir. Girişimin temel amacı, mobil servis geliştiricilerine güvenli arayüz sağlama ve güvenli surf yapabilme yolunda, mevcut açık ve özel mobil teknoloji kapsamında çalışma yapan grup ve organizasyonların çalışmalarının derlendiği, farklılaşmaların en az düzeye indirildiği kaynaklar oluşturmak olarak açıklanabilir. Dolayısı ile mobil kullanıcıların mobil web servislerinin kullanımı kapsamında kendilerini ve hassas verilerinin güvenliğinden emin olabilecekleri bir ortam sağlama BONDI'nin temel hedefi olarak görülebilir. BONDI özelliklerini taşıyan mobil cihazların ilk üretiminin 2009'da başlayabileceği öngörülmektedir.

### 7.2.4. National Institude of Standards and Technology (NIST)

NIST 1901 yılında ABD'de kurulmuştur. Temel misyonu, yaşamı kolaylaştıran ve yenilikler sağlayan teknoloji, bilim ve standartların geliştirilmesine katkıda bulunmaktır [58]. Bu kapsamda, bünyesinde çalışma grupları oluşturmuştur. Bu gruplardan 2002 yılında kurulan Bilgisayar Güvenlik Grubu (CSD), tüm IT alanında olduğu gibi mobil platformlarda güvenlik ihtiyaçları, yönetimi ve standartları konularında çalışmalar yapmakta ve belgeler üretmektedir [59].

NIST CSD mobil güvenliği, hukuksal, cihaz türleri ve uygulamalar açısından olmak üzere 3 kategoride toplanmıştır. Bu kategorilerde ele aldığı güvenlik ihtiyaçlarını, önerilerini web sitesinden [60] erişebilen belgeler ve yayınlar ile kamuya sunmaktadır.

### 7.2.5. The European Telecommunications Standards Institute (ETSI)

ETSI, başta Avrupa olmak üzere küresel boyutta IT, iletişim ve İnternet teknolojileri konularında standardizasyon çalışmalarında bulunan, kar amacı gütmeyen, 60 ülkeden yaklaşık 700 üyeye sahip bir kuruluştur [70]. Mobil ve kablosuz platformlarda güvenli ortamların sağlanmasına yönelik çalışmalarda bulunana kuruluş gelişmeler ile ilgili yayın ve belgeler üretmektedir. GSM, GPRS, EDGE, UMTS gibi teknolojiler için güvenliği esas alan şifreleme algoritmaları ve protokolleri, akıllı kartlar için kimlik doğrulama ve gizliliğe yönelik standartlar geliştirmekte ve yaygınlaşmasını sağlamaktadır [76].

## 7.3. Mobil Güvenlikte Kullanılan Standartlar

### 7.3.1. TIA 1091

TIA 1091 IMS Security Framework, TIA tarafından yayınlanmış bir mobil güvenlik standardıdır [61]. Bu standart, İnternet Protokol (IP) çoklu ortam uygulamalarını sunmak amacıyla üçüncü nesil (3G) geniş bant teknolojilere erişim sağlamak için gerekli özellikleri ve mekanizmaları tanımlar.

### 7.3.2. ITU-T X.1122 Önerisi

Açık Anahtar Altyapısının (PKI) mobil uygulamalarda kullanımı ile ilgili öneriler içeren bir kılavuzdur [62]. Açık anahtar altyapısı pek çok güvenlik fonksiyonunu (şifreleme, sayısal imza, veri bütünlüğü v.b.) gerçekleştirmek için çok uygun bir güvenlik teknolojisi olmasına rağmen bu teknolojinin mobil uçtan uca veri iletişimi için uyarlanması gerekmektedir. Bu kılavuz, PKI teknolojisine dayanan güvenli bir mobil sistem inşa etmek için öneriler getirmektedir.

ITU-T Çalışma Grubu 17 tarafından 29 Nisan 2004 tarihinde onaylanmıştır. Kılavuzun kapsamı genel olarak mobil uçtan uca veri iletişiminde sertifikaların kontrolüdür.

Bir mobil düzenleme metodu tanımlayarak bir model oluşturma bu kılavuzun kapsamı dışındadır.

PKI teknolojisinin mobil uçtan uca iletişim için bir mobil kullanıcı ile uygulama servis sağlayıcısı arasında aşağıdaki şekillerde kullanımını tanımlar:

- Mobil terminal ile uygulama sunucusu arasında (Genel Model) *veya*
- Mobil terminal ile mobil güvenlik geçidi (mobile security gateway) arasında ve mobil güvenlik geçidi ile sunucu arasında (Gateway Modeli)

Kılavuzda, sertifikaların ömür döngüsü ile ilgili PKI işlemleri, telekomünikasyon servislerinde kullanım modelleri, sistem konfigürasyon örnekleri ve PKI ile ilgili diğer kullanım önerilerine yer verilmiştir[1].

### 7.3.3. ITU-T X.1121 Önerisi

Mobil uçtan uca veri iletişimi için güvenlik teknolojileri çerçevesidir [63]. Hazırlanan kılavuzda, mobil uçtan uca veri iletişimindeki güvenlik tehditlerini ve mobil kullanıcılar ile uygulama servisi sağlayıcılarının bakış açısından güvenlik gereksinimlerini tanımlamaktadır. Ek olarak, belli güvenlik fonksiyonlarını gerçekleştiren güvenlik teknolojilerinin mobil uçtan uca veri iletişimi modelinde nerede olduğunu göstermektedir. ITU-T Çalışma Grubu 17 tarafından 29 Nisan 2004 tarihinde onaylanmıştır.

Bu kılavuz, bir mobil ağda yer alan bir mobil terminal ile bir açık ağda yer alan uygulama sunucusu arasında mobil uçtan uca veri iletişimi için OSI Referans Modelinin üst katmanında mobil kullanıcı ve uygulama servisi sağlayıcısının bakış açısından güvenlik gereksinimlerini tanımlamaktadır.

Bu kılavuz, uçtan uca mobil veri iletişiminde güvenlik teknolojileri için bir çerçeve çizmektedir. Ancak bir açık ağa bağlıyken bir mobil terminale kablosuz network erişimi durumu dışında mobil ağ bileşenlerinin detaylarını içermemektedir.

Günümüzde veri iletişim yeteneğine sahip mobil terminaller oldukça yaygın olarak kullanılmaktadır. Özellikle e-ticaret uygulamalarının yaygınlaşması güvenlik konusunu daha da önemli bir hale getirmiştir. Bir mobil kullanıcı ve uygulama servis sağlayıcı açısından bakıldığında en önemli konulardan biri bir mobil terminal ile uygulama sunucusu arasındaki mobil uçtan uca veri iletişiminin güvenliğidir.

Kılavuzda mobil uçtan uca iletişimin özellikleri, mobil ortamdaki güvenlik tehditleri, veri iletişimi için güvenlik gereksinimleri, mobil güvenlik gereksinimlerini karşılayan güvenlik fonksiyonları ve güvenlik teknolojileri tanımlanmıştır[1].

[1] Kılavuz http://www.itu.int/rec/T-REC-X.1122-200404-I/en adresinden ücretsiz edinilebilir.

### 7.3.4. TCG Güvenilir Mobil Modül Şartnamesi *(Mobile Trusted Module Specification)*

TCG'nin yayınlamış olduğu açık güvenlik standardıdır [18, 55, 64, 65, 66]. Mobil telefonlarda bilgi güvenliğinin sağlanması amacıyla geliştirilmiştir. Standardın amacı, var olan TCG teknolojisini, gömülü sistem yapısını da dikkate alarak mobil telefonlarda da kullanılmak üzere uyarlamaktır.

Söz konusu standart aşağıda yer alan beş standardı referans almakta ve ihtiyaç duyulan durumlarda yeni komut ve yapılar tanımlamaktadır.

Standart, mobil telefonlarda TCG tabanlı bir güvenlik blok yapı çözümü sağlamak için ihtiyaç duyulan temel çerçeveyi, komutları ve kontrol tanımlanmalarını sağlar. Bu da, mobil chip, yazılım ve cihaz firmalarının ürünlerinin içine MTM (Mobile Trusted Module) fonksiyonlarını taşıyan tasarımlar eklemelerine imkan vermektedir.

Standart içerisinde iki tür MTM tanımlanmaktadır. Bunlar:

- "Mobile Local-Owner Trusted Module"
- "Mobile Remote-Owner Trusted Module"

### 7.3.5. OMTP Uygulama Güvenlik Çerçevesi *(Application Security Framework)*

Açık platform işlevselliği mobil eko-sistemin tüm taraflarına, ihtiyaç ve gereksinimlere göre farklılaşan çeşitli imkanlar sunmaktadır. Kullanıcılar çeşitli programları yüklemek, kaldırmak veya sunulan çevrimiçi servisleri yenileyerek kullanmak gibi imkanlara sahiptirler. Bununla birlikte, kaynağı bilinmeyen veya güvenilmeyen uygulamalarla mobil kaynaklara ve ara yüzlere sınırsız erişim sağlanması kullanıcının terminalin veya, eğer uygun bir güvenlik mimarisi ile yönetilmez ise ağın zarar görmesi ile sonuçlanabilir.

Bu belge, zararlı veya kötü yazılmış uygulamalar tarafından suistimal edilebilecek olan terminalde sunulan anahtar fonksiyonel grupları tanımlamaktadır. Ardından bu fonksiyonel gruplar bir takım güvenlik seviyeleri ile eşleştirilmişlerdir. Bir uygulama bu fonksiyonel gruplardan herhangi birine erişmek istediği zaman o uygulamaya OMTP tarafından uygun bir imza şeması ile verilen güvenlik seviyesine bakılır ve söz konusu işlevselliğe erişip erişemeyeceği belirlenir.

Anonim bir geliştirici tarafından yazılan ve hiçbir testten geçmeyen bir uygulama çok düşük bir güvenlik seviyesine sahip olacaktır. Bu düşük güvenlik seviyesi, uygulamanın

[1] Kılavuz http://www.itu.int/rec/T-REC-X.1121-200404-I/en adresinden ücretsiz edinilebilir.

terminale yüklenmesini engellememekle birlikte bazı fonksiyonel gruplara erişimi kısıtlanacak (kullanıcıya bir uyarı verilerek) veya o uygulama için tamamen engellenecektir.

Bu belgenin hedef kitleri operatörler, üreticiler ve sertifikasyon şema otoriteleridir. Bununla beraber, geliştiriciler de erişim şartlarını, uyarı rejimlerini ve uygulamaların sertifikalandırılmasının faydasını anlamak için bu belgeyi kullanabilirler.

Uygulamaların sertfikalanması operatörler, üreticiler veya üçüncü taraflar gibi farklı yapılarca gerçekleştirilebilir. Sertifikalama işlemini gerçekleştirebilen üçüncü taraflardan bazıları Tablo 3'de verilmektedir.

**Tablo 3: Sertifikasyon Çalışmaları**

| SERTİFİKASYON DÜZENİ | İŞLETİM SİSTEMİ/ ÇALIŞTIRMA ORTAMI | DÜZENİ KOŞAN FİRMA |
|---|---|---|
| Java Verified™ | Java(TM) Platform, Micro Edition | Sun |
| Mobile2Market | Windows Mobile | Microsoft |
| Symbian Signed | Symbian OS | Symbian |
| TRUE BREW | BREW | Qualcomm |

### 7.3.6. OMTP, Gömülü Tüketici Cihazlarında Güvenlik Tehditleri *(Security Threats on Embedded Consumer Devices)*

Bu belge, kullanıcı cihazlarını etkileyebilecek tüm tehditlerin bir listesini vermektedir. Aynı zamanda bu tehditlerin, oluşturulmasının, yayılmasının kolaylığı gibi potansiyel tehlikeleri ile her bir tehdidin nasıl engelleneceği tanımlanmıştır [68].

### 7.3.7. OMTP, Gelişmiş Güvenilen Ortamlar OMTP TR1 (*Advanced Trusted Environment OMTP TR1)*

Mobil terminal ve cihazlarının gelişen servis ve teknolojilere paralel olarak artan güvenlik risk ve tehditlerinin arttığı, mobil terminal ve cihazının bu servisleri kullanabilmesi için değişik ortam, şirket ve operatörlere güven kurarak iletişimini sağlayabildiği, güvenilen her ortam için alınması ve dikkat edilmesi gereken hususları içerir. Mobil cihazlarında güvenli depo ortamı, SIM kartı ve mobil cihaz arasındaki güvenli iletişim kanalları, mobil cihaz girdi-çıktı güvenliği, güvenli mobil terminalin açılması, mobil cihaz dosya ve veri bütünlük kontrolü ve bunların tehdit grupları, en iyi uygulama ve önlem örnekleri ile anlatılmaktadır [37].

### 7.3.8. OMTP, Cihaz Yönetiminde Anti-virus İstemci Gereksinimleri (*AV Client Requirements for Device Management)*

Mobil cihazların uzaktan anti virüs yönetiminin (yükleme, konfigürasyon, yama ve imza güncellemesi, günlük yönetimi vb.) güvenli olarak yapılmasını temin etmek için bir dizi gereksinim ve önlem içermektedir.

### 7.3.9. NIST SP 800-48, Telsiz Ağ Güvenliği, "802.11, Bluetooth ve El Cihazları"

Belgenin amacı kamu kurumlarına güvenli kablosuz ağlar kurabilmeleri amacıyla yol göstermektir [69]. Bu belge, iki temel kablosuz teknolojiyi işaret etmektedir: kablosuz yerel alan ağlar (WLAN) ve Bluetooth ağlar. Belge, aynı zamanda kablosuz el terminallerinin kullanımını da adreslemektedir. Bu belgede, IEEE 802.11 standardında yer almayan teknolojilere değinilmemekte, üçüncü nesil (3G) kablosuz telefonlar için güvenlik konusu işlenmemektedir.

Belge 5 ana bölümden oluşmaktadır:

- Amaç, kapsam, hedef kitle, kabuller ve belge yapısından oluşmaktadır.
- Kablosuz teknolojilere genel bir bakış sunmaktadır.
- 802.11 WLAN teknolojisi ve güvenliği incelenmektedir.
- Bluetooth teknolojisi incelenmektedir.
- Kablosuz el cihazlarının avantajları ve güvenlik riskleri incelenmektedir.

### 7.3.10. European Telecommunications Standards Institute (ETSI) Tarafından Geliştirilen Standartlar

"European Telecommunications Standards Institute" (ETSI), *mobil elektronik imza* (*me-imza*)'nın oluşturma, yönetme süreçleri ve kullanım alanlarındaki güvenlik altyapısını da dahil ederek standart kabul edilebilecek nitelikte teknik raporlar (TR) ve teknik belirtimler (TS) yayınlamıştır [70]. Genel olarak, "mobil bir cihaz kullanılarak oluşturulan ve haberleşme ortamından bağımsız bir konumda imza veya sertifikasyon servisinden destek alan e-imza" olarak tanımlanabilecek [71] me-imza'ya ilişkin ETSI tarafından yayınlanan standartlardan önemli olanları aşağıda sunulmuştur.

#### a. ETSI TR 102 203: Mobil Ticaret (m-commerce); Mobil Elektronik İmzalar; İş ve İşlevsel Gereksinimler

Mobil elektronik imza (M-imza) çözümlerinin tasarım ve uygulamasına yardımcı olmak amacıyla hazırlanmıştır. Mayıs 2003'de yayınlanan standardın içeriğinde; M-imza, M-imza Tasarım Kriterleri, M-imzanın Kullanım Durumu, M-imza Süreci, M-imza Hizmeti, M-

imza Uygulama Sorunları, Potansiyel Roller ve Sorumluluklar, Etkileşimler ve Arayüzler ile Gereksinimler bölümleri yer almaktadır. Belgede, me-imza süreçlerinin koordine edilmesini ve yönetilebilmesini içeren hizmetin iş ve işlevsel gereksinimler belirtilmiştir. Ayrıca bu standart ile, e-imza çözümlerini kolaylaştırmak ve yaygınlaştırmak amacıyla GSM SIM kart, akıllı kart ve şifreleme tekniklerinin kullanımı anlatılarak; birlikte çalışılabilirlik, güvenlik önlemleri ve arayüzlere ilişkin teknik özelliklerin belirtilmesi amaçlanmıştır [72, 71].

**b. ETSI TR 102 206: Mobil Ticaret (M-COMM) Mobil Elektronik İmza Hizmeti; Güvenlik Çerçevesi**

Ağustos 2003'de yayınlanan standartta, M-İmza Kavramı, Genel Güvenlik Analizi, M-imza Oluşturma Sistemi İçin Güvenlik Gereksinimleri ve M-imza Profili konuları değerlendirilmekte ve bu konularda öneriler sunulmaktadır [73, 71].

**c. ETSI TS 102 204: Mobil Ticaret (M-COMM); Mobil Elektronik İmza Hizmeti; WEB Servis Arayüzü**

Ağustos 2003'de yayınlanan standartta, M-imza hizmet fonksiyonlar, M-imza'ya ilişkin 7 farklı web servisi ve bu amaçla değişimi yapılan 13 adet mesajın biçimi belirtilmektedir [74, 71]. Bu kapsamda; M-imza, M-imza statü sorgulama, M-imza görüntü sorgulama, M-imza kaydı, M-imza alındısı, M-imza uyumluluğu, fatura sorgulama, kayıt, bildirim ve uyumluluk ile Genel ESHS ve uygulama hizmet sağlayıcı gibi destek tipleri, iletişim protokol kuralları ve web servisi (güvenlik ve gizlilik) konuları anlatılmaktadır.

**d. ETSI TS 102 207: Mobil Ticaret (m-commerce); Mobil Elektronik İmza Hizmeti; Mobil Elektronik İmza Hizmetinin Dolaşım Şartları**

Ağustos 2003'de çıkan standart temel olarak mobil ticaret ile mobil elektronik imza hizmetinin dolaşım şartlarını içermektedir [75, 71]. Kullanıcı ile uygulama sağlayıcı arasındaki M-imza mesajlarının dolaşımını kolaylaştırmak ve belirli bir modelin oluşumunu sağlamak için SOAP ve http mimarisi üzerinden teknik arayüzleri belirlemeyi amaçlamıştır. Yayınlanan belge içeriğinde; Mobil Elektronik İmza Dolaşım Hizmeti, Dolaşım Konuları, Birlikte Çalışabilirlik, İşlevsel Gereksinimler; Dolaşım Çözümü (kullanıcının ilişkili olduğu MESH'nin bulunması, diğer bir deyişle, Uluslararası Mobil Abone Kimliği ve bir şebeke vasıtasıyla yol bulunması), bu amaçla oluşturulan 5 farklı senaryo, dolaşım hizmetinin teknik tanımı, veri formatları (SOAP başlık ve XML veri tipi) ve işleme talimatları yer almaktadır.

# 8 TÜRKİYE VE DÜNYADA MOBİL UYGULAMA KULLANIMI, GÜVENLİĞİ VE ÖNLEMLERİ

Günümüzde kablosuz alanların sayısının artması, GPRS/EDGE teknoloji ve 3G beklentisi, dizüstü ve mobil el terminallerinin kullanıcı sayısını ve kullanım alanlarını artırmıştır. Bunun yanı sıra, GPRS altyapısı üzerinden takip sistemleri ve veri iletişimi ile ilgili uygulamalar da geliştirilmiştir. Bu tür uygulamaların başında :

a. Takip sistemleri (araç, ekip, vb.),

b. Mobil istemci uygulamaları üzerinden veri iletişimi,

c. Saha otomasyon sistemleri üzerinden veri iletişim,

d. Bağlantı kartı gibi yapılar üzerinden sağlanan erişimler gelmektedir.

Yukarıda sıraladığımız dört ana uygulamanın arkasında çalışan yapıda birçok güvenlik önlemi alınmak zorundadır.

Gerek GPRS ile gerekse kablosuz iletişim alanlarında doğrudan İnternet erişimi olmakta ve bağlantı için cihazlar İnternet bulutundan IP almaktadırlar. Özellikle GSM üzerinden yapılan çalışmalar için APN altyapısı kullanılarak sistemlere erişmek son derece önemlidir. APN yapısının güvenlik konularında sağlayacağı faydalar aşağıda verilmektedir.

a. APN'e sadece belirlenen hatlar giriş yapabilir.

b. APN'i kullanacak uygulama ile GSM operatörü arasında özel tünelleme ve şifreleme yapılacağından verinin güvenli iletişimi sağlanır.

c. Konumlandırılabilecek RADIUS yazılımı ile,

- Kullanıcı adı ve parola ile ilave güvenlik (kimlik denetimi),
- Kullanıcılara seviyelerine göre yetkilendirme (yetki denetimi),
- Veri paketlerinin alışverişi sırasında trafik bilgisi (kimlik ve yetki takibi),
- IP yönetimi

sağlanır.

## 8.1. Mobil Devlet

İnternet ve mobil teknolojinin günlük hayatımıza etkisinin gün geçtikçe artması ile birlikte özel sektörde olduğu gibi kamu kurum ve kuruluşları da, vatandaşlarına verdikleri hizmet kalitesini artırmak ve birbirleri ile olan kurumsal ilişkilerinde ihtiyaçlara daha iyi cevap verebilmek amacıyla çalışmalar yapmaktadır. Bu kapsamda gerçekleştirilen e-devlet

süreçlerinin başarılı olabilmesinin temel anahtarı, vatandaşlar tarafından yaygın olarak kullanılabilmesi ve bu amaçla gerektiğinde erişim noktalarına ulaşabilmeleridir.

TBD'nin tanımına göre e-devlet; kamu kuruluşları, vatandaşlar ve ticari kurumlar arasındaki bilgi, hizmet ve mal alışverişlerinde bilgi teknolojilerinin kullanılarak performans ve verimlilik artışını hedefleyen devlet modelidir [88]. Son yıllarda ülkemizde yaşanan e-devlet dönüşümü ile elektronik ortamda sunulan servisler hızla artmıştır.

E-devlet uygulamalarına vatandaşlar tarafından erişim İnternet üzerinden sağlanmaktadır. Ülkemizde, yaklaşık 16 milyon İnternet kullanıcısı bulunmasına rağmen cep telefonu çok daha yaygın olarak kullanılmaktadır. Cep telefonu abone sayısı 66 milyona yaklaşarak %90'ı aşan bir kullanım oranına erişmiş, kayıtlı cep telefonu sayısı ise 100 milyonu aşmıştır [87]. Bu rakamlara ek olarak e-devlet hizmetleri kullanımı için cep telefonlarına göre daha maliyetli bilgisayar donanımı ve İnternet bağlantısı gerektirdiği gerçeği e-devlet uygulamalarının yaygınlaştırılmasında ve başarılı olmasında mobil cihazlardan yararlanılması gerekliliğini ortaya koymaktadır.

Cep telefonları, ilk dönemlerinde konuşma ve kısa mesaj gönderim amacıyla kullanılmaya başlanmış, daha sonra İnternet bankacılığı yapan bankalar tarafından kimlik tanıma ve onaylama mekanizması için kullanılmıştır. GPRS ve WAP teknolojisinin gelişimi ile birlikte bankacılık işlemleri de yapabilme yeteneği kazanan cep telefonları, günümüzde artık nitelikli elektronik sertifika kullanımını destekleyecek seviyeye ulaşmıştır. Bu sayede, nitelikli elektronik sertifika ile kamu hizmeti sağlayan kurumların servislerine cep telefonu ile erişebilme altyapısı oluşturulmuş ve işlemler için inkar edilemezlik özelliği elde edilebilmesi sağlanmıştır.

Mobil cihazlardaki bu yaygın ve işlevsel kullanım, kamu kurum ve kuruluşlarının daha verimli ve etkin hizmet verebilmek amacıyla mobil uygulamalar alanında çalışmalar yapmasını kaçınılmaz hale getirmektedir. Bu kapsamda, özel sektördeki başarılı mobil uygulamalar mobil devlet (m-devlet) uygulamalarının önünü açılmasına yardımcı olmaktadır.

Mobil teknolojinin gelişimi ve kolay kullanımı ile e-devlet çabaları yeni bir yöne, m-devlete doğru gitmektedir. E-devlet hizmetleri; mobil uygulamalar ve mobil teknolojileri kullanarak gelişmektedir. Bu süreçte devlette mobilite kavramı yerleşmektedir.

Mobilite, kullanıcılarına zaman ve mekandan bağımsız olarak, 7 gün 24 saat hizmete ve bilgiye mobil erişim imkanı sağlamakta ve günlük hayatın bir parçası olmaktadır. E-devlet hizmetlerinin mobil ortama taşınması ile ortaya çıkan m-devlet servisleri ile devlet vatandaşlara daha yakın hale gelmektedir.

Elektronik ve mobil devlet servislerinin yaygınlaşması ile beraber; kamu kurumuna vatandaşa, vatandaşın kamu kurumuna ve kamu kurumunun kendi içinde etkin, kolay yönetilir ve etkileşimli işleyişi sağlanmaktadır.

M-devlet, e-devlet uygulamalarının yerini almaktan ziyade, mobil cihazların yaygın kullanımı ve alınan hizmetler için farklı bir iletişim kanalının kullanılması açısından bakıldığında tamamlayıcı bir unsur olarak görülmektedir. Ancak, mobil cihazlarda hala var olan ekran boyutunun yetersizliği, veri girişindeki zorluklar m-devlet uygulamalarının arzu edilen hızlı gelişiminde engel teşkil edebileceğinden, mobil uygulamalarda kullanıcıya sunulan servisler tasarlanırken bu hususlar ve kısıtlar özellikle göz önünde bulundurulmalıdır.

Ülkemizde, m-devlet konusunda başarılı ve önemli çalışmalar bulunmaktadır. MOBESE gibi belediyeler düzeyinde yapılan çalışmaların yanında Vergi Dairesi Otomasyon Projesi (VEDOP) [87] gibi bakanlık düzeyinde projeler gerçekleştirilmiştir. Örneğin, VEDOP projesinin bir parçası olan e-dilekçe uygulaması ile, vatandaşlar TC Kimlik Numarası ve nitelikli elektronik sertifikasını kullanarak güvenli ve yasal bir şekilde başvurularını yapabilmektedir. Başvuruların elektronik olarak imzalanması cep telefonu ile de yapılabildiği için, gelecekteki mobil projeler için bir altyapı oluşturulmuştur.

Ulusal Yargı Ağı Projesi (UYAP) mobil hizmeti, vatandaş ve avukatlara ilgili Adalet Birimlerine gitmeden anlık sorgulama, dava dosyaları ile son durum bilgilendirmesi, dava açma, icra takibinin başlatılması gibi işlemlerin kısa mesaj servisi (SMS), sesli yanıt sistemi, WAP ve diğer mobil servisler kanalı ile yapılmasına olanak sağlayacaktır[89]. Adalet Bakanlığı bu konuda Türkiye'deki bazı Mobil Operatörlerle işbirliği protokolü imzalamış olup, kısa sürede bu hizmetlerin devreye girmesi beklenmektedir.

## 8.2. Türkiye'den Örnekler: İstemci Uygulamalarında Güvenlik

**a. Hassas Verinin Saklanmaması**

Türkiye'de pek çok banka (örneğin, İş Bankası, Türk Ekonomi Bankası, Garanti Bankası gibi) mobil bankacılık uygulamaları ile son kullanıcılara hizmet vermektedir. Bu uygulamaların ortak özelliği, SIM kart veya telefon hafızasında veri saklamamalarıdır.

**b. Tek Kullanımlık Parola Üretimi**

Son kullanıcılarına başka sebepler ile tek kullanımlık parola üreten donanımlar dağıtmış olan kurumlar mobil uygulamalarında da bu parolaları oturum güvenliği için kullanabilmektedirler. Örneğin, İnternet şubesinde tek kullanımlık parola üretimini

destekleyen bankaların mobil uygulamaları, oturum açma sürecinde tek seferlik parola üretimini desteklemektedir.

#### c. Mobil İmza Kullanımı

Mobil bankacılık uygulamalarında cep telefonunun SIM kartı üzerinde halihazırda bulunan mobil imza sertifikası ve parolası ile gerçekleştirilebilmektedir.

## 8.3. Dünya'dan Örnekler: Güvenli Eleman ile Güvenlik

#### a. Hassas Verinin Saklanması

Cep telefonu üzerinden temassız olarak ödeme gerçekleştirilmesini sağlayan uygulamaların bulunduğu telefonlarda son kullanıcıların kimlik ve ödeme bilgileri *Güvenli Eleman* adı verilen özel bir donanım üzerinde saklanmaktadır [77]. Bu verilere erişim cep telefonu üzerindeki uygulamanın doğrudan güvenli elemandaki bir hafıza bölgesi ile veya güvenli elemanda bulunan bir akıllı kart uygulamasıyla konuşması ile sağlanmaktadır [78].

Güvenli Eleman donanımı kurulan platforma göre farklı alanlarda olabilmektedir. Örneğin Toro ve ING Bank'ın 2009 Ocak ayında Romanya'da gerçekleştirmiş olduğu temassız ödeme denemesinde kullanılan cihazlarda Güvenli Eleman telefon üzerinde bir donanım olarak bulunmaktadır [79]. Tayland'da BenQ ve TaiwanMobile tarafından gerçekleştirilen deneme uygulamasında ise güvenli eleman SIM kart üzerinde yer almaktadır [80].

#### b. Donanım Adresleri ile Güvenlik

Değiştirilemez olduğu varsayılan donanım adresleri ile erişim denetlemesi gerçekleştiren mobil uygulamalar da mevcuttur. Bluetooth üzerinden ödeme çözümü üreten Rollpay adlı firma telefonun IMEI numarasını ve Bluetooth radyosunun MAC adresini kullanarak mobil uygulamada son kullanıcı tarafından sağlanan müşteri numarasının ait olduğu son kullanıcıyı doğrulamaktadır [81].

# 9 MOBİL UYGULAMA GÜVENLİK GELECEĞİ

Mobil uygulamalarda olabilecek güvenlik gelişimleri, mobil uygulamaların gelecekteki işlevsellik beklentilerine ve mevcut durumdaki güvenlik problemlerine bağlıdır.

Gelecek mobil teknolojileri, herhangi bir mobil cihazdan, herhangi bir zaman diliminde herhangi bir veriye erişmek ve bunu gereksinime göre kullanmayı amaçlamaktadır. Bu yönlü esnek bir kullanım gereksinimi ve mobil cihazların özelliklerinde görülen gelişmeler mobil cihazlara yönelik güvenlik risklerini de arttırmaktadır.

Mobil uygulamaları ilgilendiren gelecekteki olası güvenlik iyileştirme beklentileri aşağıdaki başlıklarda toplanmıştır.

**a. Kablosuz LAN Uygulamalarında Güvenlik İyileştirici Beklentiler**

Sabit ağı kullanmayan mobil uygulama çok azdır. Mobil uygulamalar bir şekilde kurumsal ağdaki sunucu bileşenleri ile iletişimde olmak zorundadır. Bu nedenle, bu bölümde mobil uygulamaların sabit ağla entegre olduğu topolojilerden Kablosuz LAN (WLAN) güvenlik geleceği konuları ele alınmıştır.

802.11p (IEEE 1609) [82] standardı, hızlı hareket eden ambülans, yolcu otobüsü, otomobil gibi cihazlardan akıllı ulaşım sistemleri uygulamalarının destekleneceği bir taslak standart olup Amerika Birleşik Devletleri ve Avrupa Birliğinin bu konudaki çalışmaları devam etmektedir. Yol kenarlarına yerleştirilen altyapı bileşenleri, hızlı hareket eden bir taşıtın kısa mesafeli veri iletişimini sağlayacak IEEE 1609.2 [83] protokol eklentisi (yayınlanmış), taşıt ve mobil ortam bileşenleri arasında güvenli mesaj iletişimini sağlayacaktır. Akıllı Ulaşım Sistemi uygulamaları; yolcuya, sürücüye, kurum ve şirketlere çok değişik mobil uygulamaların (çalınan taşıtın bulunması, uzaktan taşıtın muayenesi, yolculara İnternet servisi, trafiğin optimizasyonu gibi) daha güvenli bir şekilde sunulmasına imkan sağlaması beklenmektedir. Melez bir ağ yapısına gerek duyan bu uygulamaların güvenliğinde servis sağlayıcı bazında kimlik denetim ve AAA, kimlik doğrulama, mahremiyete özel sayısal sertifika ve güvenli gizli anahtar değişimi teknolojilerini kullanması beklenmektedir.

Hızlı dolaşım olanağının desteklendiği 802.11r (*Fast Roaming*) [84] standart eklentisi, 2008 yılının Temmuz ayında onaylanmış ve duyurulmuştur. Sabit erişim noktaları ile mobil cihazların kısa sürede (50 milisaniyeden az) dolaşımına imkan veren bu Orta Katman eklenti standardı, Wi-Fi ağından VOIP dolaşımını 802.11x kimlik denetimini sağlamaktadır. Sabit ve mobil yakınlaşmasına ivme sağlayacak bu standart, yakın gelecekte sürekli hareket halinde olan sağlık, üretim ve eğitim sektörü kullanıcılarınca ses haberleşmesinde yaygınca kullanılacaktır. Ayrıca gecikme süresine hassas mobil cihazlardan sabit yerel ağa bağlantı

gerektiren mobil uygulamalarda 802.11x kimlik denetimi ile daha güvenli kimlik denetimi sağlanacaktır.

Bilindiği gibi kablosuz ve sabit LAN bağlantı iletişiminde kullanılan *sistem yönetim çerçeve* bilgileri günümüzde güvenlik korumasız olarak iletilmektedir. Bu durum, diğer mobil cihazlardan gelen sahte bağlantı taleplerine ve bazı durumlarda uygulamaların kullandığı ağın kesintisine neden olmaktadır. Halihazırda, güvenli sistem yönetim çerçeve bilgisinin iletilmesine olanak verecek 802.11w [85] Korumalı Yönetim Çerçeve standardı oluşturulmaktadır. 802.11x kimlik denetimde yakın gelecekte kullanılması düşünülen bu standart, zararlı sistemler tarafından gelebilecek muhtemel güvenlik risklerini azaltmak için yönetim çerçeve bilgililerinin gizliliği, kaynağın doğrulanması, veri tutarlılığının sağlanması ve yeniden oynatma ataklarının önlenmesi gibi ek güvenlik olanaklarını sunacaktır. 802.11w standardına uyumlu cihaz ve uygulamalar yakın gelecekte (2010 yılı ve sonrası) standardın yürürlüğe girmesi ile birlikte yaygınlaşacaktır.

**b. 4G QoS Servisleri ve Gelişmiş Güvenlik Seçenekleri**

4G Mobil teknolojisinin yakın gelecekte kullanılmaya başlanacağı (2010), ve IP temelli paket anahtarlama mobil ağı üzerinde koşacağı bilinmektedir. 4G ile Mobil kullanıcılarına 100Mbps hızında veri transferinin sağlanacağı beklenmektedir.

4G ‘de video ve ses gibi zaman hassas verilerin servis kalitesinin (QoS) sağlanacağı ve mevcut telsiz teknolojilerine göre daha güvenli olacağı planlanmaktadır. Özellikle güvenliğin erişilebilirlik unsurunun öne çıkacağı 4G Mobil teknolojisinde yüksek verimli sayısal radyo modülasyonu olan OFDMA (*Orthogonal Frequency Division Multiplexing)* ile veri hatalarını azaltan çoklu girdi ve çoklu çıktı (MIMO) anten sistemleri kullanılacak, mobil operatör hücresel ağ bileşenleri ile umuma açık kablosuz LAN bağlantı bileşenleri “hot spot” arasında tam bir entegrasyon söz konusu olacaktır.

4G güvenliğinde AAA (Kimlik Denetim, Yetkilendirme ve İzlenebilirlik) kontrolünün sağlanması, İnternet anahtar değişimi, mobilite kaydı ve kaynak rezervasyonu gibi güvenlik kontrol ve işaretleşme bilgileri kullanılacaktır. Mobil düğüm noktaları hareket durumunda operatörlerin ve servis sağlayıcıların ağ bileşenleri tarafından kimlik denetimi ve yetkilendirmesi tabi tutulacak, Mobil Düğüm noktaları ve AAA bileşenleri arasında RADIUS, COPS ve DIAMETER gibi AAA protokolleri kullanılacaktır. Merkezi güvenlik politikaları (şifreleme, filtreleme ve şifre çözümleme gibi) Mobil düğümlere yüklenebilecektir. Böylelikle mobil uygulamalar arası uçtan uca güvenliğinin sağlanması mümkün olabilecektir.

**c. Mobil Cihazlardaki Güvenlik İyileştirici Beklentiler**

Geçmiş yıllarda başlayan ancak henüz yaygınlaşmayan spam önleyici (anti-spam), ağ geçidi, yazılım casuslarından koruyucu (anti-spy), zararlı yazılımlardan koruyucu (anti-malware) ve antivürüs koruma araçları, sabit uygulama ortamlarında olduğu gibi mobil cihazlarda da sıkça kullanılacaktır. Merkezi ve kurumsal ortamdan tanımlı güvenlik politikaları ile yönetilecek (yükleme, yama güncelleme, günlük yönetimi gibi) bu mobil güvenlik araçları yeni tehditlere ve risklere karşı mobil ortam veri ve trafiğini koruyacaktır.

Ayrıca mobil terminal ve cihazlarda gelişen yonga teknolojisi sayesinde mobil uygulamaların birbirinden izole koştuğu, bir uygulamanın diğerini etkilemediği, çok kritik uygulamalara olası güvenlik tehditli yazılımların erişemediği Sanal Etki Alan mimarileri yakın gelecekte yaygınlaşacaktır.

**d. Mobil Cihazlarda Sanal Ortam Güvenliği**

Sabit sunucularda olduğu gibi aynı mobil cihaz üzerinde birden fazla işletim sistemi, mobil servisi ve uygulamasının koştuğu sanal ortamlar gelecekte yaygınlaşmaya başlayacaktır. Mobil sanal ortamları, işletim sistemi çekirdeğinin önemli mobil servislerden izole edilmesi ve ek kontrol özellikleriyle güvenliğe olumlu katkı sağlayacaktır.

**e. Mobil Gömülü İşletim Sistemlerindeki Güvenlik**

Günümüzde yaygın kullanılan Symbian OS, Palm OS, Windows Mobile, Linux OS gibi mobil cihaz işletim sistemlerinde aşağıda planlanan ek güvenlik özelliklerinin kazandırılması beklenmektedir:

- Kullanılan servise bağlı fonksiyonların, işletim sistemi kesilse dahi devam etmesi,
- Gelişmiş erişim kontrol mekanizması ile işletim sistemi çekirdeğinin olası tehditlere karşı izole edilmesi,
- Otomatik sistemi başlatma ve işletim sistemi izleme fonksiyonlarının işletim sisteminden ayrılması,
- Güvenli sistem açılımı (Secure Boot) ve gerçek zamanlı cihaz kimlik doğrulması.

**f. Yeni Nesil Geniş Bantlı Mobil Teknolojileri ve Güvenlik**

Özellikle yüksek hızın egemen olduğu mobil teknolojileri HSPA (High Speed Packet Access), EVDO (Evolution Data Optimized), LTE (Long-Term Evolution) ve WIMAX2 söz konusudur [86].

GSM ve CDMA günümüzdeki hücresel mobil ana şebeke protokollerini oluşturmaktadır. Her iki hücresel ana şebeke protokolü, raporun diğer bölümlerinde

belirtildiği üzere daha çok iletişim hızını artıran yeni teknolojilerle desteklenmektedir. EV-DO, CDMA şebekelerinde, HSPA ve LTE ise GSM şebekelerinde yeni teknoloji olarak karşımıza çıkmaktadır. Özellikle 3G teknolojilerindeki radyo sistemleri için LTE, halihazırda 3GPP'nin 8.nci ve öncesi sürümlerinde mobil ağ etki alanı, IMS, kimlik denetleme mimarisi bir dizi güvenlik tanımlaması yapmış bulunmaktadır. Gelecek yıllarda radyo cihazları arasında kimlik denetimi, güvenlik mimarisi ekleri, şifreleme, işaretleme, sinyallerinin gizliliği ve bütünlüğü konularında yeni güvenlik eklentileri beklenmektedir.

# 10 SONUÇ

Gerek dünyada ve gerekse de ülkemizde cep telefonlarının kullanım oranlarının İnternet kullanım oranlarından daha yüksek oranda seyrediyor olması, vatandaşların mobil uygulama hizmetlerine her an, her yerden ulaşabilmesi noktasında yeni fırsatlar yaratmaktadır. Bir başka deyişle, bu olanak yardımıyla daha çok sayıdaki kullanıcının yer, mekan ve zaman kısıtlaması olmadan e-bankacılık, e-ticaret, e-eğitim, e-sağlık hizmetlerine ulaşabilmesi mümkün olabilecektir.

Mobilitenin sembolleştiği cep telefonlarına olan talebin yüksekliği bu alandaki teknolojinin de hızla gelişmesine neden olmaktadır. Gelişmenin hızlı oluşu, devam etmekte olan standartlaşma çalışmalarından yakın bir zamanda somut sonuç alınmasını güçleştirmektedir. Örneğin, web uygulaması çalışacak cihazlarda yüklü olan işletim sistemlerinin farklılığı, farklı tarayıcılar, yetersiz güvenlik önlemleri bilgi güvenliği açısından ciddi riskler oluşturmakta ve mobil uygulama güvenliği konusunda kişisel ve kurumsal önlemlerin alınmasını zorunlu kılmaktadır.

Şu an için gözlemlenen temel eğilim, mobil uygulamalarda işlevselliğin daha ön planda tutulduğu, güvenlik konusunda ise yeni yeni bilinçlenme işaretlerinin görülmekte olduğu yönündedir.

Bu raporun amacı bu noktaya dikkat çekmek üzerinedir. Esasen Mobil Uygulama Güvenliği, Genel Uygulama Güvenliği esasları altında değerlendirilebilecek iken; uygulamanın çalıştığı cihazın taşınabilir olması, haberleşmenin havadan yapılması ve bunun bir operatör vasıtasıyla gerçekleşmesi konunun farklı bir şekilde değerlendirilmesini zorunlu kılmaktadır. Mobil cihazların kolay çalınabilmesi, kaybedilmesi, havadan haberleşmenin dinlenebilmesi, iletişimin değişik GSM operatörleri aracılığıyla yapılması mobil uygulama güvenliğinin son yıllardan başlayarak önümüzdeki günlerde de en çok konuşulacak konulardan bir haline geleceğine işaret etmektedir.

Bunun yanında İnternet uygulamalarının cep telefonlarından erişilebilir olması sebebiyle sabit İnternet kullanıcılarının maruz kaldıkları virüsler ve ajan programlar gibi siber tehdit araçları mobil kullanıcılar için de tehdit oluşturmaya başlamıştır.

Mobil uygulama güvenliği konusundaki standartlaşma çalışması bir taraftan devam ederken ve bunun belli bir olgunluk seviyesine erişmesi beklenirken bir taraftan da operatörlerin ve uygulama hizmeti veren ya da verecek kamu kurum ve kuruluşlarının öncelikle alması gereken aksiyonların olduğu değerlendirilmektedir. Örnek olarak, operatör tarafında iletişimi başlatmak için kullanılan doğrulama mekanizmalarının güçlendirilmesi, güvenlik güncellemelerinin periyodik ve merkezi olarak yapılması sayılabilir.

Kurumsal uygulamalarda da benzer tedbirlerin alınması söz konusudur. Örneğin, kullanıcının VPN üzerinden kabul edilmesi, güçlü parola kullanılması, kullanıcı cihazındaki yazılımın merkezi kontrol edilmesi, virüs güncellemelerinin merkezi dağıtımı gibi.

Ancak bilgi güvenliği zincirinin en önemli halkasını insan faktörünün oluşturması nedeniyle öncelikle kullanıcıların bilinç seviyelerinin yükseltilmesinde ve muhtemel tehditlere ilişkin farkındalık eğitimlerine ağırlık verilmesinde fayda görülmektedir.

# KAYNAKÇA


**[1]** http://en.wikipedia.org/wiki/4G

**[2]** http://en.wikipedia.org/wiki/APN

**[3]** http://en.wikipedia.org/wiki/Base_Station_Subsystem

**[4]** http://en.wikipedia.org/wiki/CDMA

**[5]** http://en.wikipedia.org/wiki/Electronic_Serial_Number

**[6]** http://en.wikipedia.org/wiki/GPRS_core_network

**[7]** http://tr.wikipedia.org/wiki/IMEI

**[8]** http://en.wikipedia.org/wiki/Initialization_vector

**[9]** http://en.wikipedia.org/wiki/Mobile_Identification_Number

**[10]** http://www.javvin.com/wireless/NSS.html

**[11]** http://en.wikipedia.org/wiki/Personal_Communications_Service

**[12]** http://en.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System

**[13]** http:// en.wikipedia.org/wiki/WiFi

**[14]** http://tr.wikipedia.org/wiki/WiMAX

**[15]** Mobile Security, A primer on the security of mobile devices, and the implications for enterprise IT, Jon Collins and Dale Vile, June 2007

**[16]** Secure Mobile Working, Beyond the Technology, Dale Vile, February 2007

**[17]** Mobile Handset Security: Securing Open Devices and Enabling Trust, White paper, David Rogers, 2007

**[18]** The Trusted Computing Group: Mobile Specification: Securing Mobile Devices on Converged Networks, White paper, September 2006

**[19]** McAfee Mobile Security Report 2008

**[20]** http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

**[21]** http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

**[22]** http://en.wikipedia.org/wiki/802.11

**[23]** http://www.senza-fili.com/downloads/SenzaFili_WiMAXSupp08_Ecosystem.pdf

**[24]** http://en.wikipedia.org/wiki/IEEE_802.16

**[25]** http://www.wimaxforum.org/resources/frequently-asked-questions

**[26]** http://en.wikipedia.org/wiki/3G

**[27]** Chris Bennett Challenges of Mobile Security, SearchCIO.com, TechTarget, December 17, 2003

**[28]** Wayne Jansen, Karen Scarfone Guidelines on Cell Phone and PDA Security Recommendations of the National Institute of Standards and Technology

**[29]** SearchMobileComputing.com http://searchmobilecomputing.techtarget.com

**[30]** http://www.wikipedia.org

**[31]** War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics. Patrick S. Ryan, Vrginia Journal of Law & Technology, Vol. 9, No 7, Summer 2004

**[32]** 802.11 Denial of Service Attacks and Mitigation, GAWN Gold Certification. Stuart Compton. SANS Institute, May 2007.

**[33]** http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci1241308,00.html

**[34]** http://searchmobilecomputing.techtarget.com /topics/0,295493,sid40_tax299687,00.html

**[35]** Dae Hyun Ryu, Seung Ju Jang, A Security Weakness of the CDMA (Code Division Multiple Access) Cellular Service, International Journal of Computer Science and Network Security, Vol. 6, No. 5, May 2006, pp. 218-227

**[36]** Elad Barkan, Eli Biham, Nathan Keller, Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication, Proceedings of Crypto 2003

**[37]** OMTP Security Recommendations and the Advanced Trusted Environment: OMTP TR1. David Rogers. 4th ETSI Security Workshop, January 2009

**[38]** http://www.owasp.org/index.php/OWASP_Guide_Project

**[39]** Improving Software Security with Precise Static and Runtime Analysis. Benjamin Livshits, Doctoral dissertation Stanford University, Stanford, California, December, 2006. http://suif.stanford.edu/~livshits/papers/pdf/thesis.pdf

**[40]** Official Home Page for valgrind, a suite of tools for debugging and profiling. http://valgrind.org/

**[41]** NIST SP 500-1 53, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach http://ww.foundstone.com/us/pdf/ProgDev/fs_secure_software_dev_lifecycle.pdf

**[42]** Integral Business Solutions Secure Software Development Lifecycle (SSDLC). White Paper. http://www.go-integral.net/files/SSDLC%20Whitepaper.pdf

**[43]** Security testing and monitoring process (2008). Sami Noponen http://akseli.tekes.fi/opencms/opencms/OhjelmaPortaali/ohjelmat/CONE/fi/Dokumenttiarkisto/Viestinta_ja_aktivointi/Seminaarit/grp_2008/Esitykset/Noponen_VTT_TNT_GIGA_esitys01042008.pdf

**[44]** Esa Tikkala, Mikko Rapeli, Kaarina Karppinen, Hannu Honkanen. Security Testing OpenGGSN:a Case Study (2007). VTT Technical Research Centre of Finland, Oulu, Finland http://www.isy.vcu.edu/~gdhillon/secconf/secconf07/PDFs/50.pdf

**[45]** OpenGGSN (2006). http://sourceforge.net/projects/ggsn/.

**[46]** Codenomicon GTP Test Tool(2006) http://www.codenomicon.com/brochures/codenomicon-gtp-test-tool.pdf/

**[47]** The Open Web Application Security Project (OWASP). Web reference. http://www.owasp.org

**[48]** Jason Fuller. Windows Mobile 5.0 Application Security (May 2005). Microsoft Corporation. Web reference. http://msdn.microsoft.com/en-us/library/ms839681.aspx.

**[49]** Java Security Evolution and Concepts, Applet Security. Raghavan N. Srinivas; Reprinted from JavaWorld December 2000 http://java.sun.com/developer/technicalArticles/Security/applets/

**[50]** IEEE Security and Privacy. Building Security In Software Security Testing. Gary McGraw. September 2004 http://www.cigital.com/papers/download/bsi4-testing.pdf

**[51]** Testing Java GUIs. Alan Walworth. 1997. http://java.sys-con.com/node/35802

**[52]** Security in a Mobile World, Janne Uusilehto, IX Conference 2007, Singapore

**[53]** GSM Association Official Home Page. http://www.gsmworld.com

**[55]** The Trusted Computing Group Official Home Page. http://www.trustedcomputinggroup.org

**[55]** TCG Mobile Phone Working Group, Use Case Senarios, v 2.7, 2005

**[56]** Open Mobile Terminal Platform Official Home Page. http://www.omtp.org

**[57]** OMTP BONDI Project Home Page. http://bondi.omtp.org

**[58]** National Institude of Standards and Technology Home Page. http://www.nist.gov

**[59]** Guidelines on Cell Phonand PDA Security, Recommendations of NIST, Wayne Jansen and Karen Scarfone. NIST Special Publication 800-124, October 2008

**[60]** http://csrc.nist.gov/groups/SNS/mobile_security/publications.html

**[61]** http://electronics.ihs.com/news/2008/tia-mobile-security-1091.htm

**[62]** International Telecommunication Union: http://www.itu.int/itudoc/itu-t/aap/sg17aap/history/x1122/index-es.html

**[63]** International Telecommunication Union: http://www.itu.int/itudoc/itu-t/aap/sg17aap/history/x1121/index.html

**[64]** Trusted Computing Group, TPM Main Part 1 Design Principles, Specification version 1.2 Revision 103, July 2007

**[65]** Trusted Computing Group, TPM Main Part 2 TPM Structures, Specification Version 1.2 Revision 103, July 2007

**[66]** Trusted Computing Group, TPM Main Part 3 Commands, Specification Version 1.2 Revision 103, July 2007

**[67]** Application Security Framework. OMTP Limited Publication, June 2008.

**[68]** Security Threads on Embedded Consumer Devices. OMTP Limited publication, May 2008.

**[69]** Guide to Securing Legacy IEEE 802.11 Wireless Networks. Recommendations of the National Institute of Standards and Technology. Karen Scarfone, Derrick Dicoi, Matthew Sexton and Cyrus Tibbs. July 2008.

**[70]** The European Telecommunications Standards Institute Home Page. http://www.etsi.org

**[71]** Mobil Elektronik İmza: Senaryolar, Uygulamalar, Standartlar ve Ülkeler. Demet KABASAKAL, Şeref SAĞIROĞLU, Mustafa ALKAN. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, Kasım 2007

**[72]** ETSI TR 102 203 V1.1.1 (2003-05), Technical Report. Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements. European Telecommunications Standards Institute, 2003

**[73]** ETSI TR 102 206 V1.1.3 (2003-08), Technical Report. Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework. European Telecommunications Standards Institute, 2003

**[74]** ETSI TS 102 204 V1.1.4 (2003-08), Technical Specification. Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface. European Telecommunications Standards Institute, 2003

**[75]** ETSI TS 102 207 V1.1.3 (2003-08), Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services. European Telecommunications Standards Institute, 2003

**[76]** ETSI White Paper No.1: Security for ICT - the Work of ETSI, Carmine Rizzo, Charles Brookson, Second Edition, October 2008

**[77]** Security in Near Field Communication - Strengths and Weaknesses, Ernst Haselsteiner, Klemens Breitfuss, 2006

**[78]** MasterCard Paypass Güvenlik Modeli, http://www.mastercard.com/us/personal/en/aboutourcards/paypass/security.html

**[79]** Toro - ING Bank Romania NFC denemesi Blogu, http://www.toro-asia.com/blog/toro/romania-here-we-come

**[80]** Taiwan Mobile & Gemalto'nun SIM Tabanlı NFC Hizmetleri, http://www.cellular-news.com/story/29127.php

**[81]** RollPay Sistem Güvenlik Özet Dokümanı, http://www.rollcomm.com/downloads/ROLLPAY_System_Security_Overview_rev2.pdf

**[82]** http://en.wikipedia.org/wiki/IEEE_802.11

**[83]** http://nsl.csie.nctu.edu.tw/wivec2008.pdf

**[84]** http://en.wikipedia.org/wiki/IEEE_802.11r

**[85]** www.networkworld.com/columnists/2006/052906-wireless-security.html

**[86]** www.mobilesociety.typepad.com/mobile_life/2006/09/4g_overview_wim.htm

**[87]** Toward Mobile Revenue Administration in Turkey. A. Yıldırım, C. Özgün, Y. Göğebakan. The Third International Conference & Exhibitions on Mobile Government, September 2008.

**[88]** Türkiye Bilişim Derneği (2002), a.g.e, s.22

**[89]** http://www.uyap.gov.tr/sms/smsbilgi.html