Mobil Uygulama Marketlerinin Güvenlik Modeli İncelemeleri

Security Model Investigations of Mobile Application Markets

Selma BÜYÜKGÖZE
Kırklareli Üniversitesi TBMYO
selma.bulut@klu.edu.tr

Öz

Akıllı cep telefonları mobil internetin de yardımıyla artık hayatımızın vazgeçilmez bir parçası haline gelmiştir. Çoğu kişi artık bilgisayarlarını kullanmadan her türlü işlerini akıllı telefonlar aracılığıyla yapabilmektedir. Örneğin e-postalarını kontrol etmek, haberleri okuyup gündemi takip etmek, alış-veriş yapmak, oyun oynamak, mobil bankacılık hizmetlerini kullanarak ödemeler yapmak, sosyal medya hesaplarını kontrol etmek, müzik dinlemek, video seyretmek gibi yapılabilecek daha bir sürü işlem sayılabilmektedir. Ancak bu cihazlarımızı kullanırken güvenliğin ne kadar farkındayız? Telefonumuzda yüklü olan işletim sistemimiz ne kadar güvenli? Uygulama indirdiğimiz uygulama marketleri ne kadar güvenli? Bu çalışmamızda bu konulara değinip son durum hakkında bir analiz gerçekleştirmek istemekteyiz.

Anahtar Sözcükler: *Mobil Güvenlik, Uygulama Güvenliği, Akıllı Telefonlar*

Abstract

Smart mobile phones have become an indispensable part of our lives with mobile internet. Most people can now do all kinds of work via smartphones without using their computers. For example, there are many more operations that can be done such as checking e-mails, reading news and following the agenda, shopping, playing games, making payments using mobile banking services, checking social media accounts, listening to music and watching videos. But how aware are we to be safe when using these devices? How secure is our operating system installed on our phone? How secure is the application market we downloaded the application? We would like to refer to these issues in this study and carry out an analysis on the latest situation.

Key words: *Mobile Security, Application Security, Smart Phones.*

Gönderme ve kabul tarihi: 26.05.2018-16.02.2019
S. Büyükgöze: orcid.org/0000-0002-6559-7704
Makale türü: Derleme

1. Giriş

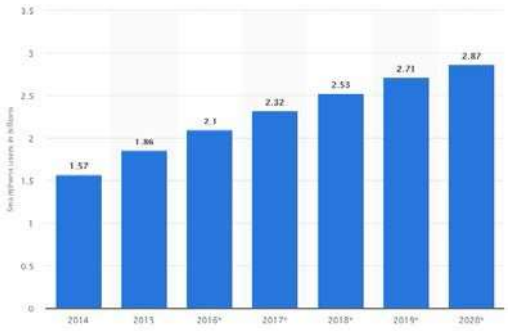
1990'lı yıllarda hayatımıza girmeyi başaran cep telefonları sadece konuşmak ve mesajlaşmak için üretilmişti. Ancak telefon teknolojilerinin gelişimi ile cep telefonları akıllı telefonlara dönüşmüş ve mobil internetin varlığı ile hayatımızda vazgeçemeyeceğimiz bir noktaya gelmiştir. Akıllı telefon nedir? diye baktığımızda; "temel telefon yetenekleri ile kısıtlı telefonlara oranla daha ileri seviyede işlem yapma kapasitesi bulunan, gelişmiş bağlantı seçenekleri sunan ve üzerinde mobil uygulamaları çalıştırabildiğiniz gelişmiş mobil iletişim cihazlarına "**akıllı telefon"** denilmektedir. Akıllı telefonlarda bulunması gereken özelliklere baktığımızda ise;

- Telefon görüşmesi yapılması ve kısa mesaj gönderilebilmesi,
- GPS, WiFi, 3G, 4G, Bluetooth gibi gelişmiş bağlantı seçenekleri sunması,
- Mobil internet bağlantısı yapabilmesi,
- Mobil uygulamaların yüklenebileceği bir uygulama marketine sahip olması,
- Üzerinde uygulama geliştirilebilen bir mobil işletim sisteminin yüklü olması,
- Dokunmatik ara yüz ekranı,
- Birden fazla uygulamayı aynı anda çalıştırabilme imkanı,

- Dahili ya da eklenebilir bellek imkanı,
- Görüntü ve ses kaydına imkan sağlaması gelmektedir [1].

Akıllı telefonların hayatımızdaki rolüne bakabilmek için önce bazı istatistiklere bakmak gereklidir. Satista.com verilerine göre 2007'den 2016 yılına kadar tüm dünyada satılan akıllı telefon sayısı 122 320 000 dan 1 495 360 000'a çıkmıştır. Piyasa araştırması şirketi International Data Corporation'a göre ise 2017'de dünya genelinde toplam 1 milyar 472 milyon akıllı telefon satılmıştır [2].

Satista.com'a göre 2014'deki akıllı telefon kullanıcı sayısı 1,57 milyardan 2016 yılında ise 2,1 milyara çıkmıştır, 2020 yılında ise bu rakamın 2,87 milyar kullanıcı olması beklenmektedir [3].

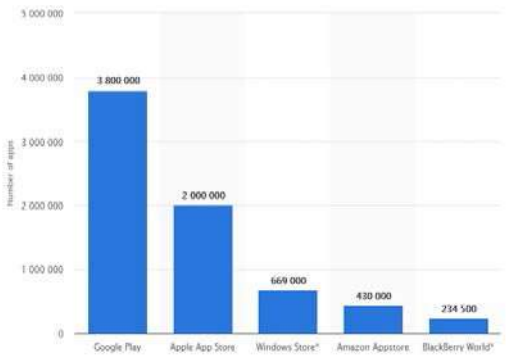


Şekil-1: Akıllı telefon kullanıcı sayısı 2014-2020 [3].

We are Social ve Hootsuite tarafından hazırlanan "Digital in 2018 Western Asia" istatistiklerine göre de Dünya'da 4,021 milyar internet kullanıcısının 5,135 milyarı ise mobil internet kullanıcısından oluşmaktadır. Bu da demek oluyor ki; Dünya popülasyonun %53'ü internet kullanırken; bu oranın %68'i ise mobil interneti kullanmaktadır. Verilen sonuçlarda bir önceki yıla göre mobil internet kullanım oranı ise %4 oranında yani 218 milyon kişi artmıştır. Türkiye'de ise nüfusun %67'sine tekabül eden 54,33 milyon kişinin internet kullanıcısı, 51,45 milyon kişinin de mobil kullanıcı olduğu verilmektedir ve bu rakamın son 1 yıl içinde %5 artışla 3 milyon kişi arttığını görülmektedir. Yetişkin insanların %98'i cep telefonu kullanırken, bunların %77'si ise akıllı telefon kullanmaktadır. Son olarak da Akıllı telefonlarda kullanılan işletim sistemi oranlarına bakalım. Dünya çapında kullanılan akıllı telefonların %73,5'i Android işletim sistemli telefonlar ve %19,9'unu ise IOS işletim sistemli telefonlar oluşturmaktadır [4]. Counterpoint den alınan 2018'in ilk çeyreği akıllı telefon satış istatistiklerine bakıldığında ise Samsung marka akıllı telefonların 78.0 milyon adet satışla %21,6'yı, Apple marka akıllı telefonların 52,2 milyon adetle %14,5'i oluşturduğu görülmektedir [5]. Verilen istatistikler ciddi anlamda akıllı telefon kullandığımızı ve mobil internetten vazgeçemediğimizi göstermektedir.

Akıllı telefonların en popüler özelliklerinden biri uygulama marketlerinden uygulama indirip telefona kurmaktır. İndirilen bu uygulamalar ile oyunlar oynayabilir, alışveriş sitelerine kolayca bağlanabilir, tarayıcılar ile web sayfalarında gezinebilir, sosyal medya hesaplarına erişebilir, güvenlik uygulamaları ile akıllı telefonumuzun güvenliğini sağlayabiliriz. Haber sitelerinden bildirimler alabilir, canlı yayınlar yapabilir, müzik dinleyebilir, film izleyebiliriz. Aslında daha bir sürü işlemi bu uygulamalar ile kolayca yapabilmek mümkün olmaktadır. Her türlü işlemi cep telefonumuzla yapabilme durumu bilgisayarlardan uzaklaşıp akıllı telefonlara olan bağımlılığımızı arttırmaktadır.

Akıllı telefonlarımıza uygulamaları ise kullandığımız mobil işletim sisteminin uygulama marketinden indiririz. Bazen de telefonumuzun işletim sistemi imkan tanıyorsa web sitesi linklerini ya da aracı platformları (güvenli olmayan) kullanırız. Akıllı telefonumuz Android işletim sistemine sahip bir telefon ise Google Play, IOS işletim sistemine sahipse App Store, Windows Phone işletim sistemine sahip ise Windows Phone Store uygulamasını kullanırız. Statista.com'un verilerine göre; 2017 yılında 178.1 milyar uygulama indirilmiş durumdadır [6]. Bu rakamın 2018'de 205,4 milyar, 2022 de ise 258,2 milyar olması beklenmektedir [7]. Bu uygulamaların 2018'in ilk çeyreğinde 3,8 milyarı Google Play de iken, 2,0 milyarı ise Apple App Store'da, 669 bin uygulama ise Windows Store'da bulunmaktadır [8]. Google Play'de %94,24 Android uygulamasının ücretsiz olduğu, AppStore da %88 IOS uygulamaların ücretsiz olduğu verilmektedir [9]. Verilen rakamlar da uygulamaları ne kadar çok kullandığımızı net olarak göstermektedir.



Şekil-2: 2018 ilk çeyreğinde uygulama marketlerinde bulunan uygulama sayısı [8].

2. Akıllı Cep Telefonlarında Güvenlik

Akıllı telefonlara uygulama indirip; bu uygulamaların kullanımlarının artmasıyla birlikte güvenlik de sorun olmaya başlamıştır. Önceden sadece bilgisayarlarda karşılaştığımız kötücül yazılımlar şimdi ise indirip kurduğumuz uygulamalar, açtığımız eklenti dosyalar ya da tarayıcılar ile akıllı telefonlarımızı da kontrol altına almaktadır. Akıllı telefonlara bulaşan kötücül yazılımlar; kullanıcıların kişisel bilgilerine erişilmesi, etkinliklerinin ya da konumlarının saklanması, sosyal medya hesaplarına sızılması, banka hesaplarına erişilmesi, izinsiz mesaj gönderilmesi, bellek ve pil ömrünün kısaltılması gibi istenmeyen sonuçlara neden olabilmektedir. Kaspersky Lab'in uzmanları mobil cihazlar için 2017'nin ilk çeyreğinde 1.333.605 [10], ikinci çeyreğinde ise 1.319.148, 2018'in ilk çeyreğinde ise 1.322.578 [11] adet zararlı yazılım tespit etmişlerdir. Bu zararlı yazılımlardan maddi olarak en çok zarar veren, mobil bankacılık işlemlerine saldırı yapan uygulama sayısı 32.038 iken, ikinci çeyreğinde 28.976, 2018'in ilk çeyreğinde ise 18,912 adet olmuştur.

2017 yılında zararlı yazılımları kullanılarak saldırganlar tarafından en fazla saldırının yapıldığı 3. ülke olarak Türkiye gelmektedir. 2018'in ilk çeyreğinde ise 6. ülke konumundadır. Bu durum mobil bankacılık üzerinde güvenlik araçlarının daha fazla şekilde kullanılması gerektiğini göstermektedir. Bu güvenlik saldırılarının hangi araçlar ile yapıldığına bakıldığında ise ilk çeyrekte tarayıcıların %43,7 iken, ikinci çeyrekte %38,63'e indiği, Android işletim sisteminin ilk çeyrekte %32,01 iken, ikinci çeyrekte %22,30'a düştüğü görülmektedir. Ancak Office programlarının ilk çeyrekte %10,26 olan oranı ikinci çeyrekte %26,15'e çıkmıştır. 2018'in ilk çeyreğinde ise bu oran %47,15'e çıkmıştır [10,11]. Bu sonuç sadece işletim sistemi ya da tarayıcıların güvenlik için önemli olmadığını artık açtığımız her dosyanın daha da önem taşıdığını ve açarken dikkatli olunması gerektiğini göstermektedir.

En çok kullanılan mobil işletim sistemi Android olduğuna göre [5]; kötücül (zararlı) bir yazılımın, Android işletim sistemine bulaşabilme durumlarını inceleyelim.

- Uzaktan kurulum yoluyla: Android Market üzerinden uygulamayı yüklerken kullandığınız Gmail hesabınızın şifresini çalan bir kişi telefonunuza internet bankacılığına giriş yaparken kullandığınız tek kullanımlık SMS mesajlarını çalan bir truva atını yükleyebilmektedir.
- Uygulama marketi aracılığıyla: Android Market'e geliştirici hesabı olan herkes, geliştirmiş olduğu uygulamayı yükleyebilmekte ve kullanıcıların kullanımına sunabilmektedir. Google bu uygulamalar için Bouncer adında zararlı uygulama tarayıcı hizmetini kullanmaktadır. Ancak Apple gibi manuel olarak kod incelemesi yapmamaktadır.
- Android SDK aracılığıyla: SDK; Google tarafından uygulama geliştiricileri (developer) için hazırlanmış ve bünyesinde kütüphaneleri ve hata ayıklayıcı (debugger), öykünücü (emulator) gibi çeşitli araçları barındıran bir yazılım geliştirme kitidir. Bu kitte bulunan Android Debug Bridge (adb) ile emulatore veya bağlı olan cep telefonuna uygulama yüklemek mümkündür.
- Internet üzerinden: Web sayfası üzerinden, e-posta eklentisi veya QR kodu ile internet üzerinden indirilen APK dosyası ile Android işletim sistemine uygulama yüklemek mümkündür [12].

Üzerinde çalıştığı sisteme müdahale eden, erişimdeki cihazları devre dışı bırakan, kullanıcı bilgilerini elde eden veya mobil cihazları uzaktan kontrol etmek için tasarlanan kod parçalarına kötücül-zararlı yazılımlar denilmektedir. Akıllı telefonlara zarar vermek için kullanılan yaygın kötücül

yazılımların tanımları ve örnekleri Çizelge-1'de gösterilmektedir.

Çizelge-1: Akıllı telefonlara zarar vermek için kullanılan yaygın kötücül yazılımlar [13].

Tipi	Tanımı	Örnek
Truva atı	Bazı işlevleri gerçekleştiren kod parçaları gizlenmiş yazılımlardır	Andoid.P Japps Trojan, Rouge Apps, Hydraq
Virüs	Kendilerini çoğaltarak dosyalara bulaşırlar	Stuxnet
Robot	Uzaktaki bir saldırgana tam yönetim hakkı verir.	Opt-In Botnets, Aurora Botnet, Rustock
Avadanlık	İşletim sistemlerini etkileyerek uzaktaki saldırganlara yönetim yetkisi verirler.	Phoneıx Toolkit
Yanıltıcı	Yanlış sitelere yönlendiren reklamlardır.	Malicious ad on Social Network Apps, Tweetmeme
Kurt	Herhangi bir kullanıcı müdahalesi olmadan kendisini kopyalayarak ağda çoğalan programlardır.	Iphoneos.Ikee.B Iphoneos.Ekee

Virüsler, solucanlar, truva atı, casus yazılım, kök izni edinme, yükleyici ve botnet olarak gruplanan Android hedefli kötücül yazılımların tespit edilebilmesi için kullanılan birçok araç mevcuttur. Bu araçlar ve özelliklerinin karşılaştırması Çizelge-2'de gösterilmektedir.

Çizelge-2: Kötücül yazılım tespiti için kullanılan araçların özellik karşılaştırmaları [14].

Kötücül Yazılım Tespit Aracı	Makine Öğrenmesi	Manifest İncelemesi	API Analizi	İzin Analizi
Kirin	X	X	X	
SCanDroid	X			
TaintDroid	X	X		
DroidBox	X	X		
ComDroid	X			
Crowdroid		X		
DroidRanger				
Andrubis	X			
MADAM				
Andromaly		X		
RobotDroid		X		
TSructDroid		X		
STREAM		X		
A5	X			
Dendroid			X	X
DroidDoplhin				
DREBIN				
DroidMAt				

Kötücül yazılım tespiti için kullanılan araçlar ve yöntemler ayrı bir araştırma konusu olup burada sadece isimlerine değinilmiştir.

2.1. İşletim Sistemlerinin Aldığı Önlemler

Akıllı telefonlarda bulunan mobil işletim sistemleri de uygulama marketlerine bir uygulamayı dahil ederken bazı güvenlik önlemleri almaktadır. Zararlı yazılımın telefona en kolay buluşma şekli uygulama içinde gömülü vaziyette gelmesidir. Kullanıcı indirdiği uygulamanın; uygulama marketi tarafından güvenlik testlerinden geçirildiğini düşünerek; herhangi bir tereddüt duymadan uygulamayı telefonuna yüklemektedir. Hatta kendisine sorulan izin bildirimlerini de okumayacak, tamamen güvenlik kısmını uygulama marketinden bekleyecektir. Peki, gerçekte de bu durum bu şekilde mi işlemektedir? Uygulama marketleri gerçekten uygulama güvenliğini sağlayabiliyor mu? Kullanıcının dikkat etmesi gereken hususlar nelerdir? Bu sorulara cevap verebilmek için mobil işletim sistemlerinin güvenliği nasıl sağladıklarına derinlemesine bakmak gerekmektedir.

2.2. ANDROID Market Güvenlik Modeli

Google tarafından geliştirilmiş olan Android işletim sistemi, akıllı telefon işletim sistemlerinde en hızlı büyüyen pazar payına sahip olan açık kaynak kodlu ve tamamen özelleştirilebilir bir işletim sistemi yazılımıdır. Satış oranlarına bakıldığında; 2018'nin ilk çeyreğinde %85,9 oranıyla en fazla satılan işletim

sistemine sahiptir [15]. Bu nedenden, güvenlik tehditlerinin de hedefi haline gelmiştir.

Google Android Market, Android işletim sistemi tabanlı bir akıllı telefona yazılım dağıtmak için kullanılan resmi çevrimiçi mekanizmadır.

Android uygulaması geliştiricileri (3. Sınıf geliştiriciler), hazırladıkları uygulamalarının doğruluğunu kontrol etmeden Google Android Markete (Google Play) uygulamalarını yüklemektedirler. Uygulamalar, herhangi bir sertifika yetkilisinin müdahalesi olmadan, geliştiricilerinin kendileri tarafından kendiliğinden imzalanmaktadır. Geliştiricilerin, kırık uygulamalar veya truva atları da dahil olmak üzere uygulamaları yükleyebildiği resmi olmayan depolar da mevcuttur. Bu durum da, kötü niyetli saldırganların Market'e kötü amaçlı yazılım yüklemesine ve gayri resmi havuzlar aracılığıyla kötü niyetli yazılım yaymalarına izin vermektedir.

Android market güvenlik modelindeki temel Android platformu yapı taşları cihazın donanımı, işletim sistemi ve Android Application Runtime şeklindedir.

- **Cihazın Donanımı:** Android, akıllı telefonlar, tabletler, akıllı saatler, otomobiller, akıllı TV'ler, OTT oyun kutuları ve tv box (STB) gibi geniş bir donanım yelpazesiyle çalışmaktadır. Android, işlemci-agnostiktir yani farklı işleri farklı platformda çözer, ancak ARM eXecute-Never gibi donanıma özgü bazı güvenlik özelliklerinden yararlanmaktadır.

- **Android İşletim Sistemi:** Çekirdek işletim sistemi Linux çekirdeğinin üzerine inşa edilmiştir. Kamera işlevleri, GPS verileri, Bluetooth işlevleri, telefon işlevleri, ağ bağlantıları vb. gibi tüm donanım kaynaklarına işletim sisteminden erişilmektedir.

- **Android Application Runtime:** Android uygulamaları çoğunlukla Java programlama dili ile yazılmış ve Android çalışma zamanında (ART) çalıştırılmıştır. Bununla birlikte, çekirdek Android hizmetleri ve uygulamaları da dahil olmak üzere pek çok uygulama yerel uygulamalardır veya yerel kütüphaneleri içermektedir. Hem ART hem de yerli uygulamalar, Uygulama Sandbox'ında bulunan aynı güvenlik ortamında çalışmaktadır. Uygulamalar veri tabanları ve ham dosyalar da dahil olmak üzere özel verileri yazabilecekleri dosya sisteminin ayrılmış bir parçasını elde ederler.

Android uygulamaları çekirdeği Android işletim sistemine genişletirler. Uygulamalar için kullanılan iki ana kaynak vardır:

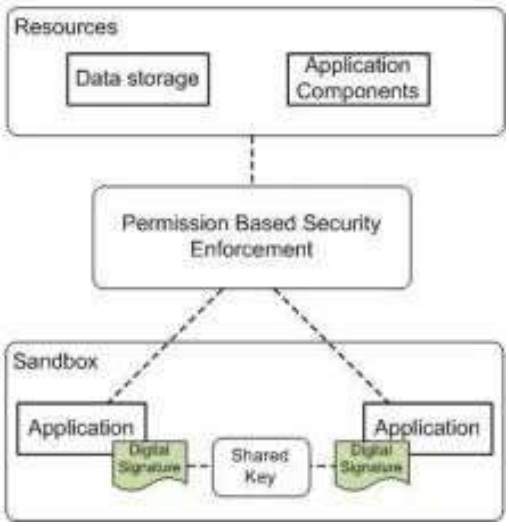
1. **Önceden yüklenmiş uygulamalar:** Android işletim sisteminde, telefon, e-posta, takvim, web tarayıcısı ve kişiler gibi önceden kurulmuş bir dizi uygulama bulunmaktadır. Bunlar hem kullanıcı uygulamaları olarak hem de diğer uygulamalar tarafından erişilebilen önemli cihaz yeteneklerini sunmak için kullanılmaktadır. Önceden yüklenmiş uygulamalar, açık kaynaklı Android platformunun bir parçası olabilmekte veya belirli bir cihaz için bir cihaz üreticisi tarafından geliştirilebilmektedir.

2. **Kullanıcı tarafından kurulan uygulamalar:** Android işletim sistemi, herhangi bir üçüncü parti uygulamayı destekleyen açık bir geliştirme ortamı sağlamaktadır. Google Play, bu şekilde kullanıcılara yüz binlerce uygulama sunmaktadır [16].

Android işletim sistemi bir Linux çekirdeğinin üzerine inşa edilmiştir. Linux çekirdeği, bellek erişimi, işletim, yönetim, sürücüler aracılığıyla fiziksel aygıtlara erişim, ağ yönetimi ve güvenlik çekirdek sistem hizmetlerini yürütmekten sorumludur.

Linux çekirdeğinin en üstünde Dalvik Sanal Makinesi (VM) ve temel sistem kitaplıkları bulunmaktadır. Dalvik VM, Android uygulamalarını çalıştırmak için kullanılan kayıt defteri tabanlı yürütme alt yapısıdır. Daha düşük seviyeli sistem hizmetlerine erişmek için Android, C / C ++ sistem kitaplıkları aracılığıyla bir API sağlamaktadır. Temel sistem kütüphanelerine ek olarak, geliştirme çerçevesi içerik sağlayıcıları, konum yöneticisi veya telefon yöneticisi gibi üst düzey hizmetleri de sağlamaktadır. Bu, yerleşik web tarayıcısı veya posta istemcisi gibi temel uygulama kümesiyle aynı sistem kaynaklarını kullanan uygulamalar geliştirmek anlamına gelmektedir. Bununla birlikte, böyle zengin bir geliştirme çerçevesi, uygulamaların özel verileri çalmalarını, diğer uygulamaları kötü niyetle bozmalarını veya işletim sisteminin kendisini engellemesini önlemek için gerekli olduğundan, güvenlikle ilgili sorunları da ortaya çıkarmaktadır [17].

Güvenlik sorunlarını çözmek için Android platformu, Şekil-3'de gösterildiği gibi izin temelli bir güvenlik modeli uygulamaktadır [18].



Şekil 3: Android Güvenlik Modeli [16]

Android Market Güvenlik Modeli'nde Linux işletim sisteminin güvenlik modeli baz alınmıştır. Linux işletim sisteminde dosyalara verilen izinler kullanıcı bazlıdır ve bir kullanıcı başka bir kullanıcının dosyasını o kullanıcı izin vermediği sürece okuyamaz, değiştiremez ve/veya çalıştıramaz.

Android işletim sisteminde de her yeni kurulan uygulamayı yeni bir kullanıcı olarak düşünebilirsiniz. Bir uygulama, diğer bir uygulamaya ait dosyalara dosya sistemi üzerinden ulaşamaz. Uygulamaların kurulabilmesi için mutlaka dijital sertifika ile imzalanmış olması gerekmektedir. Uygulamalar çalıştıklarında kullanacakları kaynaklara, erişecekleri alanlara göre kurulum esnasında kullanıcıdan bir defaya mahsus olmak üzere izin istemek zorundadırlar. Örneğin bir uygulama, çalışabilmesi için internet bağlantısına ihtiyaç duyuyor ise kurulum esnasında bunu beyan etmek ve kullanıcıdan bu izni istemek zorundadır. İzinler APK (Android application package) içinde yer alan AndroidManifest.xml dosyası içinde tanımlanmaktadır. Kurulan her bir uygulama da ayrı bir Dalvik sanal makinesinde çalışmaktadır [12].

Android cihazlar için tehlikeli olarak tanımlanan bazı izin ve grupları mevcuttur. Bu izin ve izin grupları Çizelge-3'de gösterilmiştir.

Çizelge-3: Android cihazlar için tehlikeli olarak tanımlanan bazı izin ve izin grupları [19]

İzin Grubu	İzinler
CALENDAR	READ_CALENDAR (Takvimi oku) WRITE_CALENDAR (Takvime yaz)
CAMERA	CAMERA (Kamera)
CONTACTS	READ_CONTACTS (Rehberi oku) WRITE_CONTACTS (Rehbere yaz) GET_ACCOUNTS (Rehberi Edin)
LOCATION	ACCESS_FINE_LOCATION (Net Konum) ACCESS_COARSE_LOCATION (Yaklaşık Konum)
MICROPHONE	RECORD_AUDIO (Ses Kaydet)
PHONE	READ_PHONE_STATE (Telefon durunu oku) CALL_PHONE (Çağrı yap) READ_CALL_LOG (Çağrı kayıtlarını oku) WRITE_CALL_LOG (Çağrı Kayıtlarına yaz) ADD_VOICEMAIL (Sesli mesaj ekle) USE_SIP (SIP Oturum başlatma protokolünü kullan) PROCESS_OUTGOING_CALLS (Giden çağrıları işle)
SENSORS	BODY_SENSORS (Duyargaları kullan)
SMS	SEND_SMS (SMS gönder) RECEIVE_SMS (SMS al) READ_SMS (SMS oku) RECEIVE_WAP_PUSH (WAP mesajlarını oku) RECEIVE_MMS (MMS al)
STORAGE	READ_EXTERNAL_STORAGE (Harici belleği oku) WRITE_EXTERNAL_STORAGE (Harici belleğe yaz)

Tüm tehlikeli Android izinleri izin gruplarına aittir. Herhangi bir izin, koruma düzeyine bakılmaksızın bir izin grubuna ait olabilir. Cihaz Android 6.0 üstü ise, uygulamanız tehlikeli bir izin istediğinde aşağıdaki sistem davranışı geçerlidir:

Uygulamanın şu anda izin grubunda herhangi bir izni yoksa sistem, uygulamanın erişim istediği izin grubunu açıklayan kullanıcıya izin isteği iletişim kutusunu gösterir. İletişim kutusu bu gruptaki belirli izinleri açıklayamaz. Örneğin, bir uygulama READ_CONTACTS iznini isterse, sistem iletişim kutusu yalnızca uygulamanın cihazdaki kişilerin erişimine ihtiyacı olduğunu bildirir. Kullanıcı onay

verirse, sistem uygulamayı sadece talep ettiği izni verir.

Uygulamaya, aynı izin grubunda başka bir tehlikeli izin verilmişse, sistem, kullanıcıyla hiçbir etkileşimde bulunmaksızın derhal izni verir. Örneğin, bir uygulama daha önce READ_CONTACTS izni talep etmiş ve verilmişse ve daha sonra WRITE_CONTACTS izni istendiğinde, sistem kullanıcıya iletişim kutusunu göstermeden bu izni derhal vermektedir.

2.3. IOS Uygulama Güvenlik Modeli

2007 yılında Apple tarafından geliştirilen IOS, Linux tabanlı kapalı bir işletim sistemi yazılımıdır. Satış oranlarına bakıldığında; 2018'nin ilk çeyreğinde %141 oranıyla varlığını hala sürdürebilen ikinci en çok satan mobil işletim sistemine sahiptir [15]. Kapalı bir işletim sistemi olmasına rağmen, güvenlik tehditleriyle uğraşmak durumundadır.

IOS işletim sistemine kurulacak olan uygulamalar normalde Apple tarafından kontrol edilen App Store aracılığıyla dağıtılmakta ve sıkı kurallara uyduklarından emin olmak için bir inceleme sürecine tabi tutulmaktadır. İnceleme, yalnızca yayınlanmış API yöntemlerinin kullanılmasını sağlamaktadır. Bunun için uygulamaların statik analiz ve uygulamaları kontrol eden çalışma zamanı analizi ile sanal alanın dışında okumaya teşebbüs etmemesini sağlamaktadır.

Apple'ın App Store'da ve IOS platformunda kontrol ettiği kontrol seviyesi bazı tartışmaların bir noktasını oluşturmaktadır. Bir uygulamanın App Store'da dağıtılabilmesi için geliştiricilerin Apple SDK' sında yalnızca yayınlanmış API' leri kullanmaları veya reddedilen uygulama riskini almaları gerekmektedir. Buna alternatif olarak, Apple' ın kurallarının dışında işlev gören uygulamaların dağıtımını da destekleyen alternatif dağıtım kanalı Cydia Market popüler hale gelmiştir. Cydia Mağazasındaki uygulamalar, Apple'ın kod imzalama gereksinimini ortadan kaldıran jailbreaking adlı bir işlemi kullanmaktadırlar.

IOS uygulamaları Objective-C ile yazılmıştır ve bir dizi yayınlanmış API aracılığıyla donanımla iletişim kurabilirler. IOS kullanıcı, 2D ve 3D grafikler, konum hizmetleri ve iş parçacıkları ve ağ yuvaları gibi çekirdek işletim sistemi işlevleri ile etkileşimli ekran menüleri oluşturmak için birkaç soyutlama katmanı sunar. IOS'ta uygulama ayrımı ve izolasyonu, bir politika dosyasının bazı cihaz özelliklerine ve verilere erişimi kısıtladığı Mac OS X ile benzer bir sanal alan oluşturma mekanizması ile sağlanmaktadır [18]. Varsayılan olarak hiçbir üçüncü parti uygulama, kendi dizininin dışındaki sistem dosyalarını, kaynakları ve çekirdeği içeren verileri okuyamaz veya yazamaz. Uygulamaları bu şekilde kısıtlamak, geliştiricilerin korunan kaynaklara erişmek için kayıtlı API' leri kullanmalarını gerektirmektedir [19].

Android güvenlik mimarisinin aksine, IOS güvenlik modeli, mobil cihaz güvenliği ve kullanıcının korunması için farklı bir felsefe sunmaktadır. IOS uygulama platformu, geliştiricilere yeni uygulamalar oluşturmalarını ve uygulama mağazalarına katkıda bulunmalarını sağlamaktadır. Bununla birlikte, bir üçüncü taraf geliştirici tarafından gönderilen her başvuru revizyon işlemine gönderilmektedir. Revizyon işlemi sırasında uygulama kodu, uygulama deposundan çıkmadan önce uygulamanın güvende olduğundan emin olan profesyonel geliştiriciler tarafından analiz edilmektedir. Böyle bir uygulama yüklendiğinde bir mobil aygıt üzerindeki tüm izinler alınmış olunur. Uygulama yerel kameraya, 3G / 4G, Wi-Fi veya GPS modülüne kullanıcı bilgisi olmadan erişebilmektedir. Android platformu her kullanıcının kendi güvenliğini kendi sorumluluğunda ele almasına izin verirken; IOS platformu geliştiricilerini IOS güvenliği API' lerini kullanarak güvenli kod yazmaya zorlamakta ve bu şekilde zararlı uygulamaların uygulama mağazasına girmesini engellemektedir.

IOS güvenlik API'leri, işletim sisteminin Çekirdek Hizmetleri katmanında bulunur ve işletim sisteminin Çekirdek katmanındaki hizmetlere dayanmaktadır [20]. Bir ağ görevini yürütmesi gereken uygulama, Çekirdek Hizmetleri katmanında bulunan CFNetwork API'si aracılığıyla güvenli ağ işlevleri kullanabilmektedir. IOS güvenlik uygulaması, zincir anahtar (keychain) öğelerine erişim ve kök sertifika güven yönetimi gibi çeşitli güvenlik protokollerini uygulayan Güvenlik Sunucusu adlı bir arka plan programı içermektedir. Güvenlik Sunucusu'nun hiçbir genel API'si yoktur. Bunun yerine, uygulamalar Güvenlik Sunucusuna ulaşabilmek için Keychain Services API'sini, Sertifika, Anahtar ve Güven servisleri API'sini kullanırlar.

Zincir Anahtar Hizmetleri API'si şifreleri, anahtarları, sertifikaları ve diğer gizli verileri depolamak için kullanılır. Uygulaması, bu nedenle hem şifreleme işlevlerini (şifrelemek ve şifreleri çözmek) ve veri saklama işlevlerini (sırlar ve ilgili verileri dosyalarda saklamak için) gerektirmektedir. Bu amaçlara ulaşmak için, Anahtarlık Zincir Anahtar Hizmetleri Ortak Kripto dinamik kütüphanesini kullanmaktadır.

CF-Network, güvenli veri akışları oluşturmak ve korumak ve bir iletiye kimlik doğrulama bilgisi eklemek için uygulamalar tarafından kullanılabilen üst düzey bir API'dir. CFNetwork, güvenli bir bağlantı kurmak için temel güvenlik servislerini çağırmaktadır.

Sertifika Anahtar ve Güven Hizmetleri API'si, sertifikalar oluşturmak, yönetmek ve okumak, bir Zincir Anahtara sertifika eklemek, şifreleme anahtarları oluşturmak, verileri şifrelemek ve şifrelerini çözmek, verileri imzalamak ve imzaları doğrulamak ve güven ilkelerini yönetmek için işlevler içerir. Tüm bu hizmetleri gerçekleştirmek için API, Ortak Kripto dinamik kitaplığını ve diğer Temel OS düzeyinde hizmetleri çağırmaktadır.

Randomizasyon Hizmetleri şifreli olarak güvenli rasgele sayılar sağlar. Rasgele sayılar, bir bilgisayar algoritması tarafından üretilir. Bu sayıları üretmek için Randomizasyon Hizmetleri, Çekirdek OS katmanında rastgele sayı üreteci çağırır. Geliştiricilerin sunulan API'yı doğru kullanması ve kötü amaçlı etkinlikleri uygulamaya entegre etmemesi durumunda, uygulama App mağazasına kabul edilir.

2.4. Blackberry OS Uygulama Güvenlik Modeli

Blackberry İşletim sistemi, Research in Motion (RIM) tarafından geliştirilmiştir. Satış oranlarına bakıldığında; 2016'nin dördüncü çeyreğinde %0 oranıyla varlığını sürdürememiştir [15].

Blackberry OS, Java ile yazılmış üçüncü taraf geliştirilmiş uygulamalarını desteklemektedir. İşletim Sistemi, Java Sanal Makinesi (JVM) aracılığıyla gerçekleştirilen çalışma zamanında uygulamaları izole etmek için sanal alan kullanmaktadır.

Geliştiriciler geleneksel olarak Blackberry için Java uygulamaları yazmış ve RIM onayı olmaksızın web siteleri aracılığıyla dağıtılmıştır. Bu durum, yeni Blackberry modellerinin kullanıcılarının erişebileceği Blackberry App World' un piyasaya sürülmesiyle değişmiştir. RIM, gönderilen her bir başvuruyu App World'e dahil etmek için onaylamasına rağmen, geliştiricilerin uygulamalarını diğer sunucularda barındırması da serbest bırakılmıştır [22].

2.5. Symbian OS Uygulama Güvenlik Modeli

İşletim sistemi 1990'lı yılların başından beri var olmuş ve şimdi bile yüzlerce akıllı telefon modelinde bulunmaktadır. Symbian, eskiden patentli bir platform iken Şubat 2010'da Symbian3 markası altında Nokia tarafından açık kaynağa bağlanmıştır. İşletim sistemi bütünlük, güvenlik ve düşük kaynakları göz önünde bulundurarak tasarlanmıştır.

Symbian platformu geçmişte kötü amaçlı yazılımlara hedef olmakla birlikte, çoğu saldırı, kullanıcıların sosyal mühendislik veya doğrudan manipüle edilmesiyle (örneğin, kötü amaçlı bir programın çalıştırılmasına izin vermek için kullanıcıların "evet" i tıklatması gereken Cabir3 solucanı) karşı karşıya kalmıştır.

Symbian tüm başvuruların dijital olarak imzalanmasını zorunlu kılmaktadır. Ancak tüm imzaların Symbian Foundation tarafından yayınlanması zorunlu değildir. Geliştiriciler, telefonla arama yapma, ağ bağlantılarını başlatma ve cihazın konum verilerine erişmeyi içeren "kullanıcı yeteneklerine" erişmelerine izin vererek uygulamaları imzalayabilirler. Sistem ayarlarını değiştirmeye veya temel işletim sistemine erişmeye ihtiyaç duyan uygulamalar onay için Symbian Signed4 programına gönderilmelidir. Kullanıcılar, çevrimiçi sunucuyu bir sertifikanın geçerliliği kontrol etmek için telefonlarını ayarlayabilirler. İmzasız uygulamalar gelişmiş işlevlere sınırlı erişime sahip olabilse de, pili boşaltmak ya da özel bilgileri sızdırmak için tekrar tekrar kod çalıştırarak kötü niyetli davranıp hizmet reddine neden olabilirler. Bazı taşıyıcılar Symbian olmayan imzalı sertifikaları tamamen devre dışı bırakarak, yalnızca imzalanmış uygulamaların bu taşıyıcılar tarafından kontrol edilen cihazlarda çalışmasına izin verirler [22].

Sonuç

Akıllı telefonlarımızda bulunan işletim sistemlerimizin uygulama güvenliğini nasıl sağladıklarını incelemek için yapılan bu çalışmada; Appstore'daki uygulamaların Apple tarafından kendi güvenlik kriterlerine göre değerlendirildiğini ve bu kriterleri yerine getirmeyen uygulamaları hiçbir şekilde Appstore'a yüklemedikleri görülmüştür. Ancak IOS'un kullandığı sıkı denetim politikasına karşın diğer işletim sistemleri güvenliği genelde kullanıcılarına bırakmıştır.

Uygulama yüklerken dikkat edilmesi gereken; verilen izinlerin ne amaçla verildiğinin kontrol edilmesidir. O uygulamanın çalıştırılabilmesi için verilen izin gerçekten kullanılması gereken bir araç için mi gereklidir; yoksa üçüncü parti uygulama geliştiricilerin farkına varmadan koyduğu bir izin midir? İzine onay vermezseniz muhtemelen kurulan uygulama ya düzgün çalışmayacaktır ya da hiç yüklenmeyecektir. Burada hem kullanıcının hem de uygulamayı hazırlayan uygulama geliştiricinin dikkatli olması gerekmektedir. Kullanıcı dikkatli davranıp izinleri tek tek kontrol edecek; geliştirici ise sadece gerekli olan aygıtlar için izin talep edecektir. Böylece dışarıdan akıllı telefonumuza olabilecek müdahalelerin önüne geçebiliriz.

App Store Google Play gibi resmi uygulama marketlerinden indirmediğimiz uygulamaların yani web sitesi ya da aracı programlar yoluyla indirdiğimiz APK' ların telefonumuza zarar verebileceğini, diğer açık kaynak kodlu işletim sistemi uygulama marketlerindeki uygulamalarında güvenlik ile ilgili sıkıntılar barındırabileceğini unutmamak gerekmektedir. Buradan resmi uygulama marketlerindeki yazılımların tamamen güvenli olduğu sonucuna varılmamalıdır. App Store Google Play gibi resmi uygulama marketlerinde şayet güvenlik dolayısıyla sorunlu bir uygulama mağazaya şikayet edilirse; o uygulama ya yayından kaldırılır ya da revize edilip(güvenlik açığı kapatıldıktan sonra) tekrardan yüklenecektir.

Güvenliği sadece uygulama marketinden beklemek yerine mobil saldırılardan akıllı telefonunuzu korumak için yapılabileceklere baktığımızda;

- Yazılımınızı güncel tutmak,
- Alışkın olmadığınız sitelerdeki uygulamaları indirmekten kaçınmak ve yalnızca güvenilir kaynaklardan uygulamaları yüklemek,
- Uygulamalar tarafından istenen izinlere dikkat etmek ve bu izinleri anlamaya çalışmak,
- Cihazınızı ve verilerinizi korumak için uygun bir mobil güvenlik uygulaması yüklemek,
- Önemli verileri sık sık yedeklemek olduğunu görürüz.

Nasıl ki bir bilgisayar aldığımızda artık içinde bir virüsten koruma programı kurulu olarak geliyorsa; satın aldığımız akıllı telefonların içinde kurulu olarak bir virüsten koruma, bir güvenlik duvarı yazılımının da gelmesi ilerde olabilecek saldırı ihmalini düşüreceği düşünülmektedir.

Bu çalışmanın mobil işletim sistemlerinin uygulama güvenliğini nasıl sağlandığını merak edenlere bir yol gösterici olacağı düşünülmektedir. Ancak bu konuyla ilgili yeterince çalışma yapılmadığı ve bunun nedeni olarak da işletim sistemi üreticilerinin bu konuyla ilgili materyalleri paylaşmamasından kaynaklandığı düşünülmektedir.

4. Kaynakça

[1] B.Yurdagül, *Akıllı Telefon Nedir, Ne İşe Yarar? Dünyadaki Akıllı Telefon Kullanım Oranları ve Türkiye'deki Durum*, Android Türkiye, 2011.

[2] https://www.dunyahalleri.com/cep-telefonu-sektoru-doyuma-ulasmis-olabilir/ , Erişim tarihi: 25.09.2017.

[3] https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ , Erişim tarihi: 25.06.2018.

[4] https://wearesocial.com/blog/2018/01/global-digital-report-2018, Erişim tarihi: 25.06.2018

[5] https://www.counterpointresearch.com/global-smartphone-market-declined-yoy-second-successive-quarter-q1-2018/ , Erişim tarihi: 25.06.2018.

[6] https://www.statista.com/statistics/263797/number-of-applications-for-mobile-phones/, Erişim tarihi: 25.06.2018.

[7] https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/, Erişim tarihi: 25.06.2018.

[8] https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/, Erişim tarihi: 25.06.2018.

[9] https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/, Erişim tarihi: 25.06.2018.

[10] https://securelist.com/it-threat-evolution-q1-2017-statistics/78475/, Erişim tarihi: 25.09.2017.

[11] https://securelist.com/it-threat-evolution-q1-2018-statistics/85541/, Erişim tarihi: 25.07.2018.

[12] https://www.mertsarica.com/android-zararli-yazilim-analizi/, Erişim tarihi: 25.09.2017.

[13] Wright, J., Dawson Jr, M. E., & Omar, M. *Cyber security and mobile threats: The need for*

antivirus applications for smart phones. Journal of Information Systems Technology and Planning, 5(14), 40-60,2012

[14] Utku, A., & Doğru, İ. A. *Mobil Kötücül Yazılımlar Ve Güvenlik Çözümleri Üzerine Bir İnceleme.* Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji, 4(2), 49-64,2016.

[15] https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/, Erişim tarihi: 25.07.2018.

[16] https:/source.android.com/security/, Erişim tarihi: 25.09.2017.

[17] I., Burguera, U. Zurutuza, Nadjm-Tehrani, *Crowdroid: Behaviorbased Malware Detection System For Android*., In ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM), 2011.

[18] G. Delac, M. Silic, J. Krolo, *Emerging Security Threats For Mobile Platforms*, In MIPRO, Proceedings of the 34th International Convention, 1468-1473, 2011.

[19] https://developer.android.com/guide/topics/permissions/overview#perm-groups, Erişim tarihi: 25.07.2018.

[20] J. Anderson, J. Bonneau, and F. Stajano. *Inglorious Installers: Security in the Application Marketplace*, In Proceedings of the 9th Workshop on the Economics of Information Security, 2010.

[21] D. Barrera, P. Van Oorschot, *Secure Software İnstallation On Smartphones*. IEEE Security & Privacy, 9(3), 42-48, 2011.

[22] D. Barrera, H. G., Kayacik, P. C., Van Oorschot, A. Somayaji, *A Methodology For Empirical Analysis Of Permission-Based Security Models And Its Application To Android.* In Proceedings of the 17th ACM Conference On Computer And Communications Security, 73-84, 2010.