TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ANDROID ÖN YÜKLÜ UYGULAMALARDAKİ MAHREMİYET VE GÜVENLİK SORUNLARININ ANALİZİ

YÜKSEK LİSANS TEZİ

Abdullah ÖZBAY

Bilgisayar Mühendisliği Anabilim Dalı

Tez Danışmanı: Dr. Öğr. Üyesi Buğra ÇAŞKURLU

ARALIK 2021

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, alıntı yapılan kaynaklara eksiksiz atıf yapıldığını, referansların tam olarak belirtildiğini ve ayrıca bu tezin TOBB ETÜ Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırlandığını bildiririm.

Abdullah ÖZBAY

ÖZET

Yüksek Lisans Tezi

ANDROID ÖN YÜKLÜ UYGULAMALARDAKİ
MAHREMİYET VE GÜVENLİK
SORUNLARININ ANALİZİ

Abdullah ÖZBAY

TOBB Ekonomi ve Teknoloji Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Tez Danışmanı: Dr. Öğr. Üyesi Buğra ÇAŞKURLU

Tarih: Aralık 2021

Android açık kaynak kodlu bir işletim sistemi olduğu için, sistemler üreticiler tarafından değiştirilebilir ve sistemlere yeni yazılımlar eklenebilir. Bu durum kullanıcı mahremiyeti ve güvenliği açısından endişe verici olmasına rağmen, sistemlerde bulunan ön yüklü uygulamaları kapsayıcı bir şekilde inceleyen çalışmalar sınırlı sayıdadır. Bu tez çalışmasında, bu alandaki boşluğu doldurma amacıyla oluşturulan ve herkese açık hale getirilen ön yüklü uygulamalardan oluşan bir veri kümesi tanıtılmaktadır. Ayrıca, bu veri kümesinde bulunan uygulamalardaki İzleyici Yazılım Geliştirme Kitleri, izinler, bazı manifest dosyası özellikleri ve uygulamalar tarafından kullanılan bulut servislerinin analizi gerçekleştirilmiştir. Bu analiz sonucunda, kullanıcı mahremiyetini ve güvenliği tehdit ve ihlal eden birçok durum tespit edilmiştir. Bununla birlikte, yapılan kullanıcı anketi ile kullanıcıların ön yüklü uygulamalar ve bunların aktiviteleri hakkındaki bilgi ve algıları ölçülmüştür. Bunun sonucunda, kullanıcıların ön yüklü uygulamalar hakkındaki bilgi seviyesindeki eksiklikler görülerek, kullanıcıları ön yüklü uygulamalar hakkında bilgilendirmek ve ön yüklü uygulamalar üzerinde daha fazla araştırmacının dikkatini çekmek amacıyla, analiz sonuçları oluşturulan bir web sitesi üzerinde yayınlanmıştır. Ayrıca, bu web sitesi üzerinde yayınlanan cihazlar, yapılan analizler sonucunda oluşturulan skorlama sistemi ile değerlendirilmiş ve cihazların kullanıcı mahremiyeti ve güvenliğine etkileri hakkında fikir vermesi amacıyla skorlanmıştır.

Anahtar Kelimeler: Android, Uygulama, Ön yüklü uygulama, Mahremiyet, Güvenlik

ABSTRACT

Master of Science

ANALYSIS OF PRIVACY AND SECURITY ISSUES IN ANDROID PRE-INSTALLED APPLICATIONS

Abdullah ÖZBAY

TOBB University of Economics and Technology
Institute of Natural and Applied Sciences
Department of Computer Engineering

Supervisor: Dr. Öğr. Üyesi Buğra ÇAŞKURLU

Date: December 2021

Since Android is an open-source operating system, systems can be modified by manufacturers and new software can be put to systems. Even if, this is a disquieting situation in terms of user privacy and security, number of studies that comprehensively analyze pre-installed applications on systems is limited. In this thesis, a dataset of pre-installed applications has been created and made publicly available to fulfill the gap in this area is introduced. Also, Tracker SDKs, permissions, some manifest attributes in applications and cloud services that are used by applications have been analyzed. In consequence of this analysis, many circumstances that threaten and violate user privacy and security have been detected. Moreover, with the user survey that has been made, users' knowledge and perceptions about pre-installed applications and their activities were measured. As a result, by seeing the deficiencies in the knowledge level of users about pre-installed applications, to inform users about pre-installed applications and to attract more researchers attention on pre-installed applications, the analysis results have been published on a website that has been created by author. In addition, devices that are released in this website have been evaluated with the scoring system that has been created as a result of the analyzes, and have been scored in order to give an idea about the effects of the devices on the user privacy and security.

Keywords: Android, Application, Pre-installed application, Privacy, Security

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren hocam Prof. Dr. Kemal BIÇAKCI, kıymetli tecrübelerinden faydalandığım TOBB Ekonomi ve Teknoloji Üniversitesi Bilgisayar Mühendisliği Bölümü öğretim üyelerinden Dr. Öğr. Üyesi Buğra ÇAŞKURLU ve diğer öğretim üyelerine ve destekleriyle her zaman yanımda olan başta yakın zamanda kaybettiğim annem ve anneannem olmak üzere, aileme ve arkadaşlarıma çok teşekkür ederim.

İÇİNDEKİLER

ŞEKİL LİSTESİ

ÇİZELGE LİSTESİ

Sayfa

KISALTMALAR

OEM : Orijinal Ekipman Üreticisi (Original Equipment Manufacturer)
SDK : Yazılım Geliştirme Kiti (Software Development Kit)
PHA : Potansiyel Zararlı Uygulama (Potentially Harmful Application)
PII : Kişi Tanımlayabilir Bilgi (Personally Identifiable Information)
FOTA : Uzaktan Aygıt Yazılımı Güncelleştirme (Firmware Over-The-Air)
GMS : Google Mobil Servisleri (Google Mobile Services)
VTS : Üretici Test Paketi (Vendor Test Suite)
CTS : Uyumluluk Test Paketi (Compatibility Test Suite)
GTS : GTS Test Paketi (GMS Test Suite)
STS : Güvenlik Test Paketi(Security Test Suite)
BTS : Dahili Test Paketi (Built Test Suite)
API : Uygulama Programlama Arayüzü (Application Programming Interface)
GPS : Küresel Konumlama Sistemi (Global Positioning System)
TPL : 3. Parti Kütüphane (Third Party Library)
GDPR : Genel Veri Koruma Düzenlemesi (General Data Protection Regulation)
CCPA : Kaliforniya Tüketici Mahremiyeti Yasası (California Consumer Privacy Act)
COPPA : Çocukların Çevrimiçi Mahremiyetini Koruma Kuralı (Children's Online Privacy Protection Rule)
XML : Genişletilebilir İşaretleme Dili (Extensible Markup Language)
AOSP : Android Açık Kaynak Projesi (Android Open Source Project)
SELinux : Geliştirilmiş Güvenlikli Linux (Security Enhanced Linux)
CDD : Uyumluluk Tanımı Belgesi (Compatibility Definition Document)
AWS : Amazon Ağ Servisleri (Amazon Web Services)
APK : Android Uygulama Paketi (Android Application Package)
MAC : Medya Erişim Kontrolü (Media Access Control)
IMEI : Uluslararası Mobil Cihaz Kodu (International Mobile Equipment Identity)
IMSI : Uluslararası Mobil Abone Kimliği (International Mobile Subscriber Identity)
REGEX : Düzenli İfade (Regular Expression)
SKU : Stok Tutma Birimi (Stock Keeping Unit)
S3 : Amazon Basit Depolama Servisi (Amazon Simple Storage Service)
OOBE : İlk Çalıştırma Deneyimi (Out-of-box Experience)
SSL : Güvenli Soket Katmanı (Secure Socket Layer)
TLS : Taşıma Katmanı Güvenliği (Transport Layer Security)

1. GİRİŞ

Android iki ana sebepten dolayı dünya genelinde en çok kullanılan mobil işletim sistemidir [1]: (i) açık kaynak kodlu bir işletim sistemidir [2], (ii) yeni cihazlar üretmek ve yazılımlar geliştirmek için Android işletim sistemini tercih eden yazılımcıların ve üreticilerin işleri Google tarafından belirlenen standartlarla [3] kolaylaştırılmaktadır. Bu iki nedenden dolayı; üreticiler, üreticilere yardım eden ve onlarla iş birliğinde bulunan sağlayıcılar, bağlantılı mobil ağ operatörleri, yarı iletken üreticileri ve üçüncü taraf firmalar mobil cihazlardaki uygulamaları değiştirebilirler ve kendi uygulamalarını cihazlara koyabilirler. Android cihazlarını, cihazlardaki aygıt yazılımlarını ve ön yüklü uygulamaları denetlemek için Google çeşitli sertifikasyon programları sunmakta ve uygulamaktadır.

Android Uyumluluk Programı'na göre cihazlar ve aygıt yazılımları Android Uyumluluk Tanımı Belgesi'ne [4] uyumlu olmalıdır. Bu gereksinimler Uyumluluk Test Paketi [5] kullanılarak kontrol edilebilir. Ancak Android Uyumluluk Programı'nda, Android cihazlara herhangi bir güvenlik ve mahremiyet denetimi uygulanmamaktadır.

Bunun yanında Google tarafından cihaz geliştiricilerine Android Sertifikalı Ortak Programı [6] da sunulmaktadır. Bu program kapsamındaki cihazlar YouTube, Gmail, Google Play Store, Google Maps, Google Photos gibi GMS kapsamındaki uygulamaları ön yüklü olarak barındırırlar. Birçok kullanıcı bu uygulamaları cihazlarında istediği için, üreticiler de Android Sertifikalı Ortak Programı'na girmeye çaba göstermektedir. Android Sertifikalı Ortak [7] olmak isteyen cihaz üreticileri, bu programın gereksinimlerini sağlamak zorundadır. Bu gereksinimleri kontrol etmek için çeşitli test paketleri geliştirilmiştir ve uygulanmaktadır [8, 9]. Öncelikle üretici tarafından geliştirilen aygıt yazılımı parçalarının uyumluluklarını kontrol etmek amacıyla Üretici Test Paketi (VTS [10]) uygulanmaktadır. Mobil cihazlardaki yazılımların uyumluluklarını kontrol etmek için Uyumluluk Test Paketi (CTS) uygulanmaktadır. Bunun yanında cihazda bulunan Google uygulamalarının uyumluluklarını kontrol etmek için GMS Test Paketi (GTS) uygulanmaktadır. Yine bu programın parçası olarak, mobil Dahili Test Paketi (BTS), Güvenlik Test Paketi (STS) gibi daha çok cihaz güvenliğini kontrol eden test paketleri uygulanmaktadır. Dahili Test Paketi ile Potansiyel Zararlı Uygulamalar (PHA) ve diğer zararlı aktiviteler güvenlik bakış açısı ile gözden geçirilmektedir. Ek olarak Güvenlik Test Paketi ile güvenlik yamalarının uygulanıp uygulanmadığı ve ön yüklü uygulamaların güncel olup olmadıkları kontrol edilmektedir. Buna rağmen hem Android Uyumluluk Programı hem de Android Sertifikalı Ortak Programı kullanıcıların mahremiyetini ve güvenliğini tam anlamıyla garanti edememektedir.

Günümüz dünyasında kullanıcıların mahremiyet ve güvenliğini tehdit eden birçok ön yüklü uygulama tespit edilmiş durumdadır. Bunlardan en bilinenlerinden birisi, Kryptowire firması tarafından tespit edilen [11] ve üreticilerin aygıt yazılımlarını güncellemesine yardımcı olan Adups isimli uzaktan aygıt yazılımı güncelleme (FOTA) uygulamasıdır. Yapılan analize göre, bu uygulama BLU R1 HD akıllı telefonlarda bulunmakta

olup, Kişi Tanımlayabilir Bilgileri (PII) toplama ve kullanıcıların cihazlarında uzaktan yetkili bir şekilde kod çalıştırma kabiliyetlerine sahiptir.

Bunun yanında Google'ın Android Security & Privacy 2018 Year In Review [12] isimli raporunda belirtildiğine göre, Potansiyel Zararlı Uygulama geliştiricileri tedarik zincirinde bulunan Orijinal Ekipman Üreticileri (OEM) veya firmalar ile anlaşarak veya bunları kandırarak kendi uygulamalarını cihazlara kurdurabilmektedir. Böylece çok fazla çaba göstermeden binlerce telefona bulaşabilirler. Ayrıca yine raporda belirtildiğine göre, Hindistan, Brezilya ve Endonezya gibi büyük Android marketlerinde satılan akıllı telefonlarda, birden fazla sayıda ön yüklü potansiyel zararlı yazılım tespit edilmiştir. Bunun yanında, Oversecured firması tarafından yapılan araştırmaya göre [13, 14], Android Sertifikalı Ortak Programı'nın bir üyesi olan Samsung'a ait telefonlarda bulunan ön yüklü uygulamalar birden fazla tehlikeli zafiyet barındırmaktadır. Son olarak, Android akıllı telefonlarda OEM'ler ile bağlantılı ön yüklü uygulamaların dışında, sosyal ağlar, arama motorları, haberler, telekomünikasyon vb. ile bağlantılı ön yüklü uygulamalar da bulunmaktadır. Örneğin, Bloomberg tarafından yapılan habere göre [15], akıllı telefonlarda ön yüklü gelen Facebook uygulamaları, daha sonra cihazlardan silinememektedir. Üçüncü parti uygulamalar ve bunların bağlı ortakları telefon üreticileri ile işbirliği yapmaktadırlar [16].

1.1 Araştırma Amaçları

Son birkaç yıl öncesine kadar, ön yüklü uygulamalar araştırmacıların fazla ilgisini çekmemiştir ve yukarıda bahsedildiği gibi, ön yüklü uygulamalar üzerine yapılan çalışmaların birçoğu sadece seçilmiş birkaç uygulamayı kapsayacak şekilde yapılmıştır. Ancak yakın zamanda Android cihazlardaki ön yüklü yazılımlar üzerine yapılan ilk kapsayıcı çalışma [17] ile birlikte bu alandaki boşluk kapatılmaya başlamıştır. Bu tez çalışmasında önceki çalışmada belirlenen önemli bazı eksik noktaların giderilmesi amaçlanmaktadır. İlk olarak, Android cihazlardaki ön yüklü uygulamalardan oluşan herkese açık bir veri kümesi olmadığı için, böyle bir veri kümesinin oluşturulması amaçlanmıştır. Böylece bu önemli alanda gelecekteki araştırmaların daha rahat şekilde yapılabileceği düşünülmektedir. Bu amaçla bir Android uygulama geliştirilmiş ve bu uygulamayı kitle kaynak kullanımı yöntemi ile yayılmıştır. Bu uygulama yardımı ile veri toplanıldıktan sonra, toplanılan ön yüklü uygulamalar mahremiyet ve güvenlik açısından analiz edilmiştir. Ayrıca toplanılan ön yüklü uygulamalar, Kaggle [18] üzerinden araştırmacıların erişimine açılmıştır.

Kullanıcı mahremiyeti ile ilgili olarak, uygulamalarda bulunan İzleyici (*tracker*) Yazılım Geliştirme Kitleri (SDK) yapılan çalışma ile çıkarılmıştır. Ardından, bu izleyicilerin analitik, reklam, konum takibi, profilleme, kimlik tanımlama vb. gibi amaçları analiz edilmiştir. Ek olarak, hangi tür uygulamaların (OEM uygulamaları, mobil ağ operatörleri, sosyal ağlar vb.) bu izleyicileri bulundurduğu belirlenmiştir. Sonuç olarak, Android ön yüklü uygulamalardaki İzleyici SDK ekosistemi keşfedilmiş ve bunların kullanıcıların mahremiyetine etkisi ortaya konmuştur.

Güvenlik bakış açısı ile bakıldığında ise, ön yüklü uygulamaların *manifest* dosyalarındaki kritik alanlar ile ilgili litaratürdeki ilk çalışma tarafımızca yapılmıştır. Bu kapsamda, *manifest* dosyalarındaki dışarıya açık uygulama bileşenleri, paylaşımlı UID

değerleri, *usesCleartextTraffic, allowBackup* ve *debuggable* gibi özellikler incelenmiştir. Burada ön yüklü uygulamaların güvenlik açısından en iyi uygulamaları takip edip etmediklerinin kontrolü amaçlanmıştır. Ek olarak, Android ön yüklü uygulamalar tarafından kullanılan bulut servisleri araştırılmıştır. Böylece, bu uygulamaların, bu servisleri ne kadar güvenli bir şekilde kullandıklarının tespiti hedeflenmiştir.

Bununla birlikte, geliştirilen uygulamayı [19] indiren ve yükleyen kullanıcılarla, kullanıcıların ön yüklü uygulamaların güvenlik ve mahremiyete etkisi hakkındaki endişelerini ve algılarını anlamak amacıyla bir anket çalışması yapılmıştır.

Son olarak yapılan çalışmalar sonucun elde edilen analiz sonuçları, Android cihaz kullanıcılarını bilgilendirmek ve bilinçlendirmek ve daha fazla araştırmacının dikkatini çekmek amacıyla hazırlanan web sitesine [20] konulmuştur. Bununla birlikte, bu web sitesinde bulunan cihazlar oluşturulan skorlama sistemine göre derecelendirilmiştir.

1.2 Katkılarımız

Özet olarak, bu tez çalışması ile ön yüklü mobil uygulamaların mahremiyet ve güvenlik ile ilgili yeni gelişmekte olan literatürüne ve bilgi havuzuna aşağıdaki başlıklarda katkılar sağlanmıştır:

- Android cihazlarda bulunan ön yüklü uygulamalardaki izleyici ekosistemini keşfettik. Bu kapsamda, hangi tür uygulamalarda (Örneğin, OEM uygulamaları, mobil ağ operatörleri, sosyal ağ, haber vb. üçüncü parti uygulamalar), hangi tür izleyicilerin mevcut olduğunu ortaya koyduk. Ek olarak, bu izleyicileri ve amaçlarını kullanıcı mahremiyetine etkileri bakımından inceledik.
- Uygulamaların manifest dosyalarındaki paylaşımlı UID (sharedUID) değerinin yanında *usesCleartextTraffic, allowBackup* ve *debuggable* gibi özelliklerin en iyi uygulamaları takip edip etmediklerini analiz ettik.
- Uygulamaların kullandığı ve tanımladığı izinleri analiz ederek, aşırı yetkili uygulamaları tespit etmeye çalıştık. Ayrıca, izinlerden yola çıkarak üreticiler ile 3. parti firmalar arasından iş birliklerini ortaya çıkardık.
- Ön yüklü uygulamalar tarafından kullanılan bulut servislerini analiz ettik ve bu servislerde herhangi bir yanlış yapılandırma olup olmadığını ortaya koyduk.
- Geliştirdiğimiz uygulamayı [19] kullanarak, kullanıcıların ön yüklü uygulamaların güvenlik ve mahremiyeti ile ilişkili endişelerini ve algılarını anlamak amacıyla bir anket çalışması gerçekleştirdik ve bu çalışmanın sonuçlarını tartıştık.
- Daha fazla araştırmacının dikkatini çekmek amacıyla, bu alanda ilk olacak şekilde, oluşturduğumuz veri kümesini herkese açtık[1].
- Yapılan analiz sonuçlarını kullanıcıları bilgilendirmek ve bilinçlendirmek ve araştırmacıların dikkatini çekmek amacıyla oluşturduğumuz web sitesi üzerinden yayınladık [20].

[1] [18]

- Bir skorlama sistemi geliştirerek, cihazların kullanıcı mahremiyeti ve güvenliği üzerindeki etkisini değerlendirdik.

1.3 Literatür Araştırması

Android uygulamaları ve ekosistemi birçok araştırmacının dikkatinin çekmiş ve bu alanda birçok çalışma yapılmıştır. Bu alandaki çalışmalar incelenirken ön yüklü uygulamalar ve 3. parti uygulamalar üzerinde ayrım yapılmalıdır. Çünkü bu uygulamalar birbirlerinden çeşitli temel konularda ayrılmaktadır. Bundan dolayı literatür araştırması yapılırken, bu farklılıklar göz önünde bulundurularak inceleme yapılmıştır.

1.3.1 3. Parti Uygulamalar

Android ekosistemi üzerindeki çalışmalarda, 3. parti uygulamalar üzerinde yapılan çalışmalar ön yüklü uygulamalara göre çok daha gelişmiştir. Bunun en temel sebeplerinden birisi 3. parti uygulamalara çoğunlukla [21–25] gibi uygulama marketleri üzerinden erişim sağlanabilmesidir. Bundan dolayı bu kapsamda yapılan çalışmalar ön yüklü uygulamalar üzerinden yapılan çalışmalara göre çok daha olgunlaşmıştır.

Uygulama İzinleri. Android ekosisteminde uygulama izinleri, cihaz üzerinde özellikle kullanıcı mahremiyeti ve güvenliğini etkileyen durumları en aza indirmek için büyük önem arz etmektedir. Bundan dolayı, bu konu birçok araştırmacının ilgisini çekmiş ve bu alanda birçok çalışma yapılmıştır.

Örneğin, bu konu üzerinde yapılan bir çalışma ile [26], Android kaynak kodları analiz edilerek, tanımlanan uygulama izinlerinin çıkarılması amaçlanmıştır. Bu kapsamda, 3.4 milyon satır Android kaynak kodu incelenerek 75 farklı izin tespit edilmiştir. Bu işlemleri gerçekleştirmek için bir araç [27] kullanılmış ve açık kaynak kodlu hale getirilmiştir.

Yine bir başka çalışmada [28], Android sistemlerde sunulan API çağrıları ile uygulama izinlerinin ilişkileri incelenmiştir. Android sistemlerde, uygulama geliştiricilere geniş bir API fonksiyonu havuzu sunulmuştur. Bu API fonksiyonlarının kontrolsüz kullanımı kullanıcı mahremiyetini ve güvenliğini etkileyebilir. Bundan dolayı, bu fonksiyonlara erişim çeşitli izinler ile kontrol altına alınmıştır. Bu çalışma kapsamında, uygulamalarda kullanılan API fonksiyonları ile izinlerin uyumu analiz edilmiştir. Böylece ihtiyacından fazla izin tanımlayan ve en az yetki prensibine uymayan uygulamaların tespiti amaçlanmıştır.

Bu API fonksiyonlarına erişim uygulama izinleri ile kontrol edilse bile, uygulamaların gerekli izinleri aldıktan sonra da gerçekleştirdikleri işlemler kullanıcı mahremiyeti ve güvenliği açısından önemlidir. Bilindiği üzere Android cihazlar kullanıcılar tarafından yaygın bir şekilde kullanılmakta ve birçok kullanıcı verisini içerisinde barındırmaktadır. Yapılan bir çalışma [29] ile, Android uygulamalarının sızdırdığı telefon bilgisi, GPS konumu, Wi-Fi verisi gibi özel bilgiler tespit edilmiştir.

Android sistemlerde, sistem tarafından sunulan izinlerin yanı sıra uygulama geliştiricilerin kendi izinlerini tanımlamalarına da olanak sağlanmıştır. Bu özel izinlerin (*custom*

permissions) kasti veya hatalı olarak yanlış kullanımı, kullanıcı mahremiyeti ve güvenliğini tehlikeye atan durumların ortaya çıkmasına neden olabilir. Yapılan bir çalışmada [30], Android özel izin tanımlama ve yönetim mekanizması incelenerek burada bulunan açıklıklar ortaya çıkarılmıştır. Böylece platform kaynaklarına çeşitli şekillerde yetkisiz erişim sağlanmış ve popüler Android uygulamalarında zafiyetler bulunmuştur.

Ayrıca, sistem kaynaklarına erişim çeşitli izinler yardımı ile sınırlandırılsa bile, bu izinlerin yönetimi kullanıcılara bırakılmıştır. Uygulamalar bu durumdan faydalanarak kullanıcıları yanlış yönlendirebilir ve sistem kaynaklarına çeşitli şekillerde erişebilir. Kullanıcıların izin yönetimi konusundaki davranışlarını anlamak ve kolaylaştırmakla ilgili çeşitli çalışmalar da [31] yapılmıştır. Ancak, örneğin bu durum ön yüklü uygulamalar konusunda eksikliklere sahiptir. Kullanıcılar birçok durumda ön yüklü uygulamaların kullandığı izinler ve bu izinlerin yönetimi konusunda bilgi sahibi değildir.

3. Parti Kütüphaneler. SDK'lar gibi 3. Parti Kütüphaneler, uygulama geliştiricilerin, geliştirme sürecini hızlandırdıkları ve kolaylaştırdıkları için geliştiriciler tarafından sıklıkla kullanılmaktadır. Ayrıca yine bu TPL'ler yardımı ile, geliştiriciler uygulamaları üzerinden para kazanma, uygulamanın verdiği hataların tespiti gibi işlemleri gerçekleştirebilirler. Bu tür işlemler için reklam ve izleme servisleri çeşitli SDK'lar sunmaktadır. Ancak bu tür TPL'lerin kontrolsüz ve bilinçsiz kullanımı, kullanıcıların mahremiyetini ve güvenliği tehlikeye atmaktadır. Örneğin, bu kütüphanelerde bulunan bir zafiyet, kütüphaneyi kullanan uygulamaları da etkilemektedir. Ayrıca yine kütüphanenin kullanıcının gizli verilerine erişmesi ve bu verileri toplaması gibi durumlar ortaya çıkmaktadır. Bu sebeplerden dolayı, Android uygulamalarda kullanılan TPL'lerin kullanıcı mahremiyeti ve güvenliğine etkisi üzerinden çeşitli çalışmalar yapılmıştır. Örneğin yapılan bir çalışmada [32], Lumen Privacy Monitor isimli bir uygulama yardımı ile Android cihazların ağ trafiği gerçek zamanlı olarak incelenmiştir. Böylece cihazlarda bulunan uygulamaların kullandığı izleme ve reklam servislerinin tespit edilmesi amaçlanmıştır. Çalışma sonucunda 233 tanesi ilk olmak üzere, 2,121 izleme ve reklam servisi keşfedilmiştir. Daha sonra keşfedilen bu servislerin ve bağlı oldukları firmaların ilişkileri ve gizlilik politikaları incelenerek veri toplama ve paylaşma davranışları analiz edilmiştir. Bu çalışma sonucunda reklam ve izleme servislerini bağlı oldukları firmalar ve 3. parti firmalarla, topladıkları kullanıcı verilerini paylaştıkları tespit edilmiştir. Son olarak, çalışma kapsamında bu servisleri GDPR gibi regülasyonlarla uyumu incelenmiştir. Bu çalışmada belirtildiği üzere dinamik analiz yöntemleri ile ilgili servisler tespit edilmiş ve cihazlarda mevcut olan tüm servisler incelenmiştir. Başka bir çalışmada [33] ise, Amerika Birleşik Devletleri ve Birleşik Krallık'ta bulunan Google Play uygulama marketindeki 959,000 uygulamadaki 3. parti izleyici servisleri analiz edilmiştir. Bu kapsamda, kullanılan veri kümesi üzerinden, 3. parti izleyici servisleri ekosisteminin keşfedilmesi, hangi uygulama kategorilerinde hangi tür izleme servislerinin yoğunlaştığı, bu servislerin daha çok hangi firmalara ait olduğu gibi konular tespit edilmiştir. Bunun yanında, bir diğer çalışmada [34], 1,100 farklı uygulamanın 10 farklı şehirde çalıştırılması ile veri toplanmıştır. Toplanılan bu veri analiz edilerek konum tabanlı reklam ağlarının, konumların nüfus yoğunluğu, reklam ağlarının farklı konumlardaki davranışları gibi konular odak alınarak keşfedilmesi amaçlanmıştır. Yine bu çalışmada da 3. parti uygulamalar baz alınmıştır.

Bulut Servisleri. Bulut servisleri özellikle son zamanlarda Android uygulamalar tarafından yaygın bir şekilde kullanılmaktadır. Bu durum araştırmacıların da ilgisini çek-

miş ve konu üzerinden çeşitli araştırmaların odak noktası olmuştur. Zimperium tarafından yapılan araştırmaya göre [35], bulut servisleri kritik ve hassas kullanıcı bilgileri barındırmakta ve bu servislerin hatalı konfigürasyonu, bu bilgilerin tehlikeye girmesine neden olmaktadır. Checkpoint tarafından yapılan başka bir çalışmada [36] ise, gerçek zamanlı veri tabanı, bildirim gönderme ve bulut depolama gibi bulut tabanlı servislerdeki hatalı konfigürasyonlar 100 milyondan fazla sayıda kullanıcının kişisel bilgilerini tehlikeye atmaktadır. Her iki çalışmada uygulama marketlerindeki uygulamaların analizi üzerinde yoğunlaşmıştır.

Manifest Dosyası Analizi. Android sistemlerdeki Manifest(AndroidManifest.xml) dosyası uygulamalanın çalışması için gerekli konfigürasyon bilgilerini içinde barındıran XML formatındaki bir dosyadır. Manifest doyasındaki hatalı konfigürasyonlar, uygulamayı tehlikeye atarak kullanıcı mahremiyetini ve güvenliğini tehdit eden durumlara neden olabilir. Örneğin, manifest dosyası özellikleri (Örn., allowBackup, debuggable, usesCleartextTraffic) ve paylaşımlı UID (sharedUID) değerleri kılavuzlarda belirtildiği şekilde [37] ayarlamalıdır. Özellikle, paylaşlımlı UID değerlerinin kasıtlı veya kasıtsız hatalı kullanımı, uygulamaların aşırı yetkilerle (Örn., `android.uid.system` yetkisi ile.) çalışmasına neden olabilir [8]. Bunun yanında, aynı paylaşımlı UID değerine sahip olan ve aynı anahtarla imzalanmış uygulamalar birbirlerinin kaynaklarına erişebilirler. Bu durum kullanıcıların güvenlik ve mahremiyetini etkileyen durumların [38, 39] ortaya çıkmasına neden olabilir.

1.3.2 Ön Yüklü Uygulamalar

Daha önceden bahsedildiği gibi, önceki çalışmaların birçoğu Android uygulama marketlerindeki uygulamalar üzerinde yapılmıştır. Ön yüklü uygulamalar cihazlarla birlikte yüklü bir şekilde geldikleri için, 3. parti uygulamalardan büyük farklılıklar göstermektedir. Bu farklılıklar temel olarak Çizelge 1.1'de görülebilir. Bundan dolayı, ön yüklü uygulamaların analizi ve bu alandaki çalışmalar 3. parti uygulamalara göre farklılıklara sahiptir.

Son zamanlarda yayınlanan bir makaleye göre [40], batarya, disk alanı, hafıza gibi sistem kaynaklarını tüketen ve sistemlerde ön yüklü olarak gelen uygulamaların (*bloatware*), kullanıcıların mahremiyet ve güvenliğine etkisi araştırılmıştır. Bunun yanında, kullanıcıların bloatware uygulamalar hakkındaki bilgisini ve bakış açısını ölçen bir kullanıcı araştırması yapılmıştır. Ancak, bu çalışmada daha çok uygulama izinleri ve bu izinlerden kaynaklanan sonuçlar üzerine yoğunlaşılmıştır.

Ek olarak ön yüklü uygulamalarda yetki yükseltme zafiyetleri bulmayı amaçlayan bir çalışma [41] da yapılmıştır. Bu çalışma kapsamında 100 farklı cihaz üreticisine ait 2017 cihaz yazılımından (*firmware*) toplamda 331,342 ön yüklü uygulama analiz edilmiştir. Çalışma için geliştirilen *FIRMSCOPE* sistemi ile, uygulamaların statik olarak akış analizi yapılmıştır. Bu sistemde kullanılan akış analizi yöntemleri ile literatürdeki en gelişmiş (*state-of-art*) yöntemler hem başarım hem de hız olarak geride bırakılmıştır. Bu sistem ile birçoğu sıfırıncı gün açığı olan ve istismar edilebilen yetki yükseltme zafiyetleri tespit edilmiştir.

Başka bir güncel çalışmada [42] ise, Android sistemlerdeki uzaktan yazılım güncel-

leme uygulamaları analiz edilmiştir. Bu uygulamalar cihazların güvenli ve güncel kalmasında büyük rol oynamaktadır. Çalışma kapsamında ilk olarak 422,121 ön yüklü uygulama arasından 2,013 tane FOTA uygulaması tespit edilmiştir. Ardından, bu uygulamalar statik olarak analiz edilmiştir. Analiz sonucunda, bu uygulamaları konum toplama ve 3. parti izleyici barındırma gibi kullanıcı mahremiyetini tehlikeye atan faktörlere sahip oldukları görülmüştür. Ayrıca, uygulamalardaki geliştirme hatalarından kaynaklanan çeşitli zafiyetler tespit edilmiştir.

Bu konudaki güncel bir çalışma [17] ile birlikte, ön yüklü uygulamalar üzerine kapsamlı bir çalışma yapılmış ve büyük bir veri kümesi kullanılarak ön yüklü uygulama ekosistemi keşfedilmiştir. Ek olarak, 3. parti kütüphaneler, uygulama izinleri (özellikle özel izinler) ve uygulamaların ağ trafikleri mahremiyet temelli olarak incelenmiştir. Ancak, bu çalışmada incelenmeyen bazı önemli noktalar mevcuttur. Özellikle İzleyici Yazılım Geliştirme Kitleri (Tracker SDK'lar), bu çalışma kapsamında açıkta kalmıştır. Bunun yanında, çalışmanın ana odağı gizlilik problemleri olduğu için manifest dosyası en iyi uygulamaları ve bulut servislerinin güvenliği gibi güvenlik problemleri kapsam dışı kalmıştır. Son olarak, kullanıcıların ön yüklü uygulamalara bakış açısından ve bu konudaki algısından bahsedilmemiştir.

Son olarak, 2021 yılında yapılan bir çalışmada [43], OEM'lerin AOSP üzerinde yaptıkları değişikliklere odaklanılmıştır. Çalışma kapsamında, ikili dosyaların güvenlik sıkılaştırmaları, SELinux politikaları, Android *init* betikleri, çekirdek güvenlik sıkılaştırmaları gibi konular ele alınmıştır. Çalışma sonucunda incelenen, 2,907 cihaz yazılım dosyasından 579 tanesinde CDD ile uyumsuzluklar tespit edilmiştir. Bu uyumsuzluklar cihazların güvenlik durumlarını olumsuz olarak etkilemektedir.

Çizelge 1.1: Ön yüklü uygulamalar ile uygulama marketlerindeki uygulamaların karşılaştırılması.

Ön Yüklü Uygulamalar	**Uygulama Marketlerindeki Uygulamalar**
Cihazda ön yüklü olarak gelir.	Cihaza kullanıcı tarafından uygulama marketleri üzerinden yüklenir.
Başta *system* kullanıcısı olmak üzere daha yetkili kullanıcılarla çalışır.	Her uygulama için özel oluşturulan yetkisiz kullanıcı ile çalışır.
Ön yüklü olarak geldikleri için, uygulama izinleri otomatik olarak verilir.	Kullanıcı tarafından yüklendiği için, izinler yükleme esnasında sorulur.
Kullanıcı tarafından sistem üzerinden kaldırılamaz, sadece devre dışı bırakılabilir.	Kullanıcı tarafından sistemden kaldırılamaz.
Birçoğunun güncellenmesi için sistem güncellemesi gerektiği için, daha az sıklıkla güncellenir.	Güncelleme yayınlandığı sürece uygulama marketleri üzerinden güncellenebilir.

Şu ana kadar belirtildiği (ve Çizelge 1.1'de özetlendiği) gibi, ön yüklü uygulamalar ile uygulama marketlerindeki uygulamalar önemli farklılıklar göstermektedir ve yine bahsedildiği gibi ön yüklü uygulama ekosistemini ve bunun güvenlik ve mahremiyet etkilerini anlamak için yapılması gereken çok fazla iş vardır. Bu çalışmadaki amacımız bu konuda katkı sağlamaktır.

2. VERİ KÜMESİ OLUŞTURULMASI VE DETAYLARI

Android sistemlerdeki ön yüklü uygulamalar üzerindeki kapsamlı çalışma sayısının düşük olmasının temel sebeplerinden birisi, bu alandaki veri kümesi eksikliğidir. Bilgimiz dahilinde, Android ön yüklü uygulamalardan oluşan herkese açık bir veri seti bulunmamaktadır. Bu konudaki güncel bir çalışmada [17] böyle bir veri seti oluşturulsa bile, mevcut durumda herkese açık hale getirilmemiştir. Bundan dolayı, bu çalışmayı gerçekleştirmek ve bu alandaki eksikliği kapatmak amacıyla bir veri kümesi oluşturulması amaçlanmış ve bunu gerçekleştirmek için bir sunucu-istemci yapısı kurulmuştur. Bu yapıda geliştirilen bir Android uygulama [19] istemciyi, bu uygulamanın haberleştiği web sayfası [44] ise sunucuyu belirtmektedir.

2.1 Android Uygulaması (Pre-App Collector)

Ön yüklü uygulamaları kullanıcıların cihazlarından toplamak amacıyla, bir Android uygulaması (Bu çalışma TOBB Ekonomi ve Teknoloji Üniversitesi İnsan Araştırmaları Değerlendirme Kurulu tarafından etik olarak onaylanmıştır [45].) geliştirilmiş ve bu uygulamayı Google Play Store üzerinden yayınlanmıştır [19]. Bu uygulamayı yaygınlaştırmak için, üniversitelerin mail gruplarında, sosyal medya gruplarında ve sosyal medya üzerinde paylaşılmıştır. Uygulama şu şekilde çalışmaktadır:

Uygulama ilk olarak başlatıldığında, kullanıcıları çalışma hakkında bilgilendirilmekte ve işlemlere başlamadan önce kullanıcıların onayını alınmaktadır Şekil 2.1 (a).

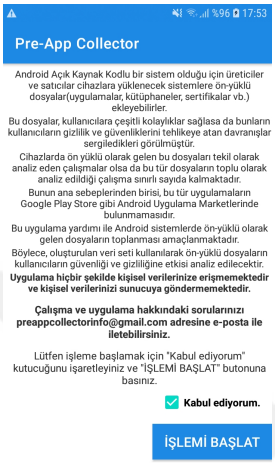
Ardından kullanıcılara, onların ön yüklü uygulamaların mahremiyeti ve güvenliği hakkındaki endişelerini ve algılarını ölçmek için birkaç soru sorulmaktadır. Kullanıcıların sorulara verdiği cevaplar dışında cihaz hakkında cihazın üreticisi, parmak izi, modeli, ürün adı, versiyonu, zaman dilimi, sim operatörü, sim ülke ISO değeri ve cihazın rootlanıp rootlanmadığı gibi bazı üst veri bilgileri arka planda toplanmaktadır.

Daha sonra, cihaz üzerindeki /system, /odm, /oem, /vendor ve /product dizinleri yinelemeli olarak taranarak ön yüklü uygulamaları da içeren aygıt yazılımı dosyaları tespit edilmektedir.

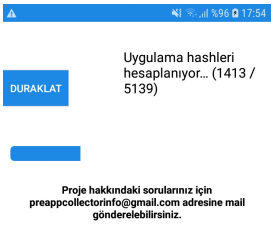
Bu dosyaların MD5 hash bilgileri hesaplanarak sunucuya gönderilmekte ve bunların daha önce sunucuya yüklenip yüklenmediği kontrol edilmektedir. Sunucuda olmayan dosyaların listesi cihaza gönderilerek, bunların cihaz tarafından sunucuya gönderilmesi sağlanmaktadır Şekil 2.1 (b).

Sunucuda olmayan dosyaların hash bilgisi tespit edildikten sonra, bu hash bilgilerine sahip dosyalara sunucuya yüklenmektedir Şekil 2.1 (c).

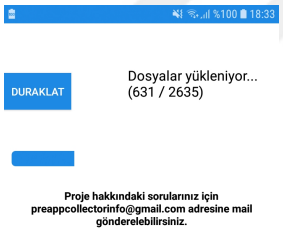
Son olarak, kullanıcılara cihazlarında bulunan ön yüklü uygulamaların bir listesi gösterilmekte ve cihazlarında bulunan aygıt yazılım dosyaları hakkında istatistiksel bilgiler gösterilmektedir Şekil 2.1 (d).



(a) Kullanıcı Onayının Alınması



(b) Dosya Hashlerinin Hesaplanması



(c) Dosyaların Sunucuya Yüklenmesi

(d) İşlemin Tamamlanması ve Kullanıcı Bilgilendirme

Şekil 2.1: Mobil Uygulama Ekran Görüntüleri.

2.2 Sunucu

İstemci olarak kullanılan mobil uygulama ile toplanan dosyaları göndermek için AWS üzerinden bir sunucu kiralanmıştır. Bu sunucunun temel olarak iki yapı bulunmaktadır: 1) Sunucu üzerinden çalışan ve Python FLASK ile yazılmış web servisi,

2) Bu servis tarafından gerekli bilgileri depolamak için kullanılan MySQL veri tabanı.

Sunucu şu şekilde çalışmaktadır:

Mobil uygulama üzerinde kullanıcıya ilk olarak çeşitli sorular sorulmaktadır. Kullanıcı bu sorulara cevaplayıp işleme devam ettikten sonra sorulara verdiği cevaplar sunucuya gönderilmekte ve sunucu üzerindeki MySQL veri tabanında depolanmaktadır.

Ayrıca bu aşamada mobil cihaza ait bazı üst veri bilgileri de sunucuya gönderilmektedir. Bu veriler şunlardır: cihaza uygulama tarafından atanan ve rastgele alfa-nümerik karakterlerden oluşan ID değeri, cihaz üreticisi, cihaz modeli, cihaz versiyonu, cihazın parmak izi (*fingerprint*) bilgisi, cihazın bulunduğu zaman dilimi, sim operatörü ISO bilgisi. Yine bu bilgiler de MySQL veri tabanında depolanmaktadır.

Ardından, Android uygulamadan sunucuya cihazda bulunan aygıt yazılımı dosyalarının bilgileri gönderilmektedir. Sunucuda bulunan MySQL veri tabanında dosyalara ait MD5 hash, dosya dizini, dosyanın sunucuya yüklenip yüklenmediği, dosya APK dosyası ise ilk yükleme ve son güncellenme zamanları, dosyanın bulunduğu cihaza atanan ID değeri gibi bilgiler tutulmaktadır. Sunucu üzerinden alınan dosyaların hash bilgileri ve sunucuya yüklenip yüklenmediği kontrol edilerek, yüklenmeyen dosyaların hash bilgileri tekrar Android uygulamaya gönderilmektedir.

Son olarak, Android uygulama tarafından gönderilen ve sunucuda bulunmayan dosyalara sunucuya yüklenmektedir. Yüklenme işlemi tamamlanan dosyaların veri tabanında yüklenme durumu bilgisi güncellenmektedir.

2.3 Veri Kümesi İstatistikleri

Kullanıcı cihazlarından toplanılan veri kümesi ile ilgili bazı ilginç istatistikler şu şekildedir:

- Tez çalışması kapsamında, toplam 22 farklı OEM'den ve 98 farklı cihazdan dosyalar toplanmıştır.
- Zaman dilimi bilgisine göre 14 farklı ülkede bulunan cihazlardaki dosyaların yüklendiği tespit edilmiştir.
- Toplamda, 14,178 APK dosyası, 418 sertifika, 58,721 paylaşımlı kütüphane ile birlikte 143,862 aygıt yazılımı dosyası toplanmıştır.
- Son olarak, varsayılan cevaplarla aynı cevaplara sahip olan ve aynı e-posta adresine sahip olan anket cevapları çıkarıldıktan sonra, çalışma kapsamında 77 farklı kullanıcıdan anket çalışmasına katılım sağlamıştır.

2.4 Ön Yüklü Uygulama Ekosistemi

Çalışma kapsamında Android cihazlardaki ön yüklü uygulamalara odaklanılmıştır. Buradaki ekosistemi keşfetmek için birkaç farklı analiz uygulanmıştır. İlk olarak, Python temelli bir tersine mühendislik aracı olan Androguard [46] aracı kullanılarak, uygulamaları imzalamak [47] için kullanılan sertifikalar çıkarılmıştır. Uygulama sertifikalarındaki "Issuer" alanı incelenerek uygulamanın hangi kişi veya firma tarafından geliştirildiğinin tespit edilmesi amaçlanmıştır. Aynı kişi veya firma tarafından geliştirilen uygulamaları imzalamak için tek bir sertifika kullanılmadığı için, firma veya kişiler tarafından ortak kullanılan sertifikalar gruplanmaya çalışılmıştır. Bu gruplar OEM'ler, OEM ile bağlantılı firmalar, 3. parti firmalar (Örn., Sosyal Ağlar, Tarayıcılar, Uygulama Marketleri, Arayan Tanımlama Firmaları, Haber Uygulamaları, Bulut Servisleri, Telekomünikasyon Firmaları, Pazarlama & Reklam Firmaları). Toplamda, 126 sertifika grubu altında uygulamalar toplanmıştır. Ek olarak, uygulama paket adına göre sorgulama yapılarak, uygulamaların kaç tanesinin Google Play Store'da [21] olup olmadığını kontrol edilmiştir. Bunun sonucunda uygulamaların sadece %9'unun Google Play Store üzerinden erişilebilir olduğu görülmüştür. Bunun yanında, uygulamalar toplanırken ilk yükleme zamanı, son güncelleme zamanı gibi üst veri bilgileri elde edilmiştir. Bu üst veri analizine göre, ön yüklü uygulamaların 14,178 tanesinden 7,829 tanesinin (%55) ilk yüklendikleri andan itibaren güncellenmediklerini tespit edilmiştir. (Not: Ön yüklü uygulamaların birçoğu 3. parti uygulamalar olmadıkları için sistem disk bölümünde yer alırlar. Bundan dolayı sadece üreticiler tarafından geliştirilen uzaktan güncelleme mekanizmaları kullanılarak güncellenebilirler ve bu güncelleme sonucu telefonun yeniden başlatılması gerekmektedir. Bundan dolayı, ön yüklü uygulamalar, uygulama marketlerindeki uygulamalar gibi kolay bir şekilde güncellenememektedir).

3. ANALİZ

Tez çalışması kapsamında, toplanan dosyalardan özellikle ön yüklü uygulamaların (APK dosyaları) analizine odaklanılmıştır. Böylece kullanıcıların mahremiyetini ve güvenliğini etkileyen çeşitli faktörler belirlenmiş ve uygulamaların bu faktörler baz alınarak analizi yapılmıştır.

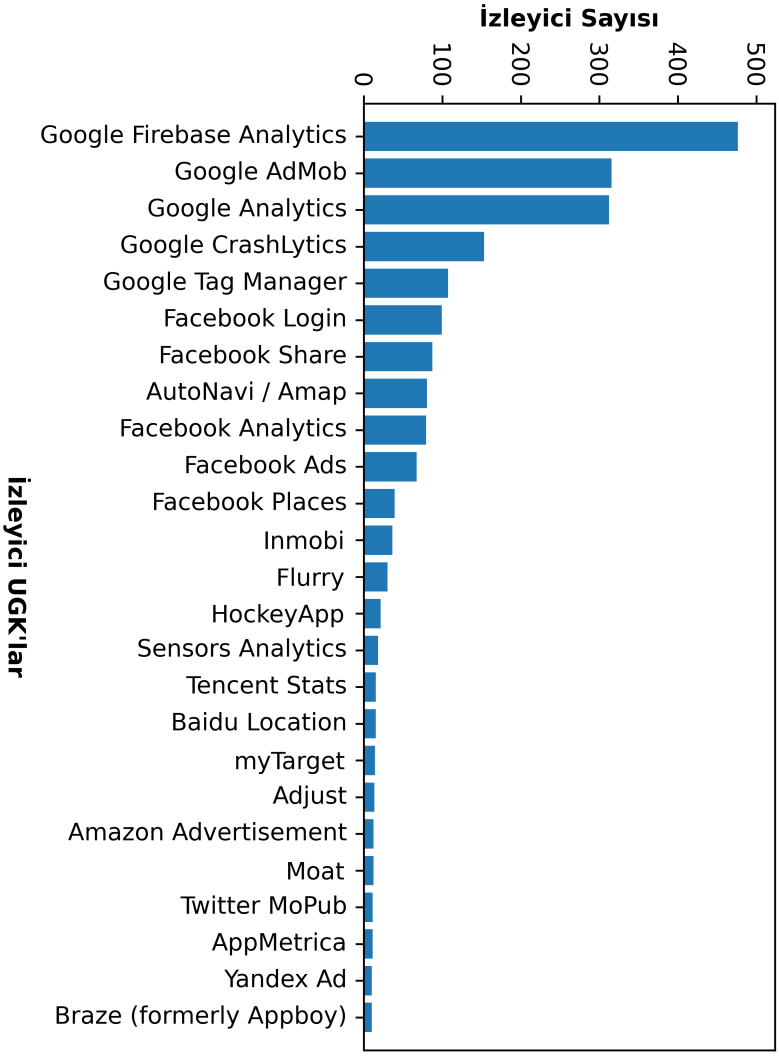
3.1 İzleyici Yazılım Geliştirme Kitleri Analizi

3.1.1 İzleyici Yazılım Geliştirme Kitleri

Android İzleyici SDK'lar, kullanıcılar ve onların uygulamalarını nasıl kullandığı hakkında bilgi toplamaktadırlar. Bunlar uygulama içlerine gömülmüş halde gelir ve hata raporlama, analitik, profilleme, kimlik tanımlama, reklam, konum takibi gibi çeşitli fonksiyonlara sahiptirler. Bu izleyicilerin analizi, Exodus Privacy [48] isimli, kar amacı gütmeyen ve Android izleyiciler ve bunların kullanıcı mahremiyetine etkisi üzerine çalışan bir organizasyonun çalışması üzerine temellendirilmiştir. Bu organizasyonun exodus-standalone [49] isimli aracı, ön yüklü uygulamalara gömülmüş izleyicileri tespit etmek için kullanılmıştır. Sonuç olarak, ön yüklü uygulamalardaki izleyici ekosistemi ve izleyicilerin kullanıcıların mahremiyetine etkisi keşfedilmiştir. Çalışma sonucu ana bulgularımız şu şekildedir:

- 836 farklı uygulamada toplam 85 farklı izleyici tespit ettik.
- Bu izleyicileri kullanan firmaları veya bağlantılı firmaları araştırdık. Ardından bu firmaların gizlilik politikalarını ve geçmişte kullanıcı mahremiyetini ihlal eden bir olaya karışıp karışmadıklarını inceledik. Bunun sonucunda bazı firmaların topladıkları bilgileri açıkça belirtmediklerini fark ettik (Bazı firmaların web sitelerinde ve gizlilik politikalarında çoklu dil desteği olmadığı için, bu tür siteleri ve gizlilik politikalarını incelemek için çevrimiçi çeviri servislerini kullandık).
- İzleyicilerin birçoğunun gizlilik politikasında, Kişi Tanımlayabilir Bilgi (PII), konumla ilgili veriler, kayıt bilgileri, kullanıcı davranışları, cihaz tanımlayıcılar, reklam tanımlayıcılar (Örn., Google Advertsing ID [50]) gibi bilgileri izledikleri belirtilmiştir. Bu durum kullanıcıların mahremiyetini farklı seviyelerde olumsuz olarak etkilemektedir.
- İzleyicilerin çoğunluğu gizlilik politikalarında GDRP [51] ve CCPA [52] gibi düzenlemelerle uyumlu olduklarının belirtmişlerdir. Ancak bazıları hala gizlilik politikalarında bu tür düzenlemelerden bahsetmemişlerdir. Ek olarak, gizlilik politikalarına göre, izleyiciler bu tür regülasyonlar altında olmadıkları durumlarda daha fazla bilgi toplama eğilimindedirler.

İstatistikler. Yukarıda bahsedildiği gibi, birçok farklı uygulamada birçok farklı izleyici tespit edilmiştir. Ön yüklü uygulamalarda bu izleyicilerden bazılarının diğerlerinden daha yaygın olduğu görülmüştür. Şekil 3.1, ön yüklü uygulamalarda bulunan en



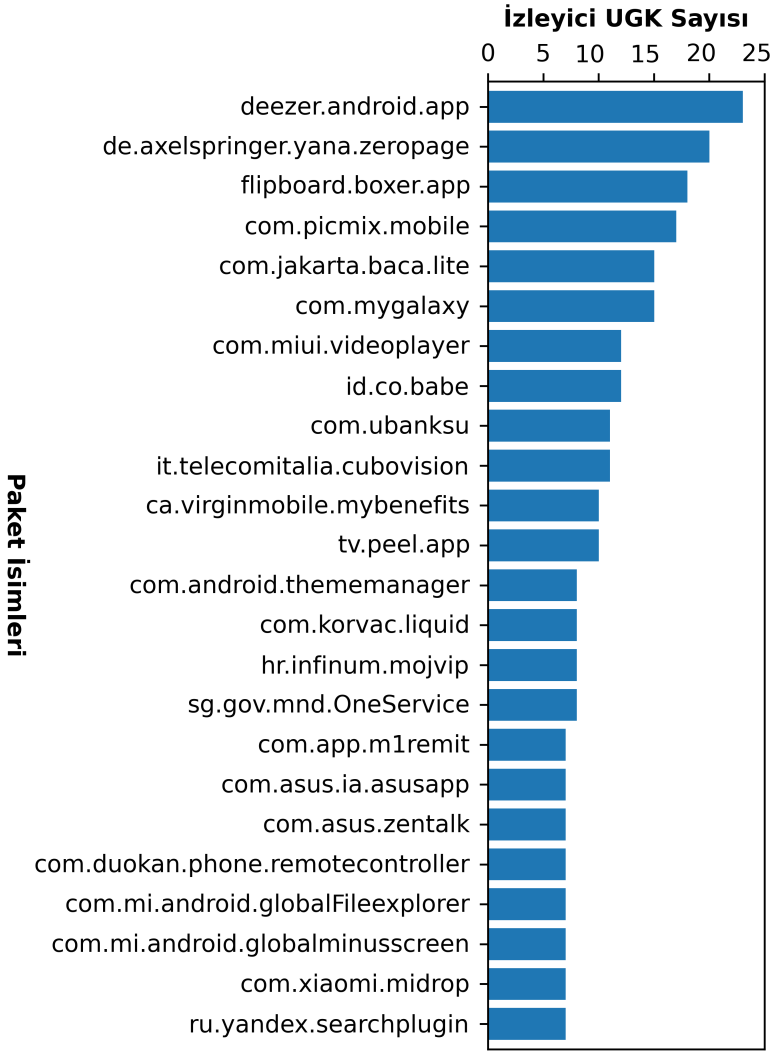
Şekil 3.1: Ön Yüklü Uygulamalardaki En Yaygın İzleyici SDK'ları.

yaygın İzleyici SDK'ları göstermektedir. Beklendiği şekilde Google, Facebook, Tencent ve Amazon gibi büyük teknoloji firmalarının bu alanda baskın bir şekilde yer aldığı görülmektedir.

Bunun yanında, bazı ön yüklü uygulamaların çok fazla miktarda izleyici barındırdığı gözlemlenmiştir. Bu durum kullanıcıların mahremiyetini ihlalini kaçılmaz bir hale getirmektedir. En fazla İzleyici SDK içeren ön yüklü uygulamalar Şekil 3.2'de görülebilir.

İlginç bir şekilde, yaptığımız sertifika analizine göre, bu uygulamaların çoğunluğunun 3. parti uygulamalar olduğu görülmektedir. Dolayısıyla, cihazlar temel fonksiyonlarını yerine getirmek için bu uygulamalara ihtiyaç duymamaktadırlar.

Ek olarak, izleyicileri firmalarına ve bu firmaların yönetim merkezlerinin hangi ülkede yer aldığına göre gruplanmıştır. Bu bilgi ülkelerin kullanıcı mahremiyetine saygısı ve ülkelerde uygulanan GDPR gibi regülasyonlardan dolayı önemlidir. Çizelge 3.1'de ülkeler ve bu ülkelerde merkezi bulunan izleyici firması sayısı gösterilmektedir.



Şekil 3.2: En Fazla Sayıda İzleyici SDK İçeren Ön Yüklü Uygulamalar.

Çizelge 3.1: Farklı Ülkelerdeki İzleyici Firmalarının Sayısı.

Ülke	**İzleyici Firmalarının Sayısı**
Amerika Birleşik Devletleri	56
Çin	11
Rusya	4
Almanya	4
Franse	3
Hindistan	2
Birleşik Krallık	1
İsrail	1
Açık Kaynak Kodlu	1

Çizelge 3.2: Firmalar ve Onlarla İlişkili İzleyici Servislerinin Sayısı.

Firma	İzleyici Servislerinin Sayısı
Alphabet (Google'ın Çatı Firması)	5
Facebook	5
Oath	3
Baidu	3
Microsoft	3

Çizelge 3.2'de görülebilecek analizimize göre, büyük teknoloji firmaları devamlı olarak izleyici servislerini satın almaktadır. Buna ek olarak, firmalar ve bu firmaların yöneticileri hakkında bilgi sağlayan Crunchbase [53] web sitesini kullanarak izleyici servislerinin firmalarının kontrol edilmiş ve bu firmaların başka firmalar tarafından sürekli olarak satın alındığını veya birbirlerini satın alarak büyüdüklerini ve bu alandaki pazar paylarını artırdıkları fark edilmiştir. Ancak, bazı izleyici servislerinin gizlilik politikalarında bahsedildiği gibi, bu firmalar başka firmalar tarafından satın alındığında kullanıcı verilerinin kontrolünden sorumlu olmadıkları ve satın alan firma ile bu verilerin paylaşıldığı belirtilmiştir. Bu durum kullanıcıların verilerini tehlikeye atmaktadır.

Son olarak, Crunchbase üzerinden firmaların merkezlerinin bulunduğu ülkeleri kontrol edilmiştir. Çünkü Çin gibi bazı ülkelerde, firmalar istihbarat servisleri veya devletle istenen her türlü veriyi paylaşmaları gerekiyor. Ayrıca, kullanıcıların kişisel verileri, bu verileri koruyan regülasyonlar (Örn., GDPR, CCPA) altında olmayan ülkelere transfer edilebilir. Çizelge 3.1'de ülkeler ve bu ülkelerde bulunan izleyici firmalarının sayısı görülebilir.

İzleyicilerin Amacı. İzleyici SDK'lar çeşitli amaçlar için tasarlandıkları için, farklı özelliklere sahip olabilirler. Dolayısıyla, kullanıcı mahremiyetine etkileri değişebilir. İzleyiciler, Exodus Privacy [48] tarafından 6 farklı gruba ayrılmıştır:

- **Hata Raporlayıcı**: Bu izleyicilerin amacı, uygulama çöktüğünde geliştiricileri bilgilendirmek ve uyarmaktır. İzleyici servisleri arasında en meşru sebeplerle kullanılan tür bunlardır.

- **Analitik**: Bu tür izleyiciler veri kullanımı hakkında bilgi toplarlar ve geliştiricilerin hedef kullanıcıyı tanımalarına yardımcı olurlar. Örneğin, kullanıcının tarayıcı kullanım davranışı gözlemlenerek toplanabilir.

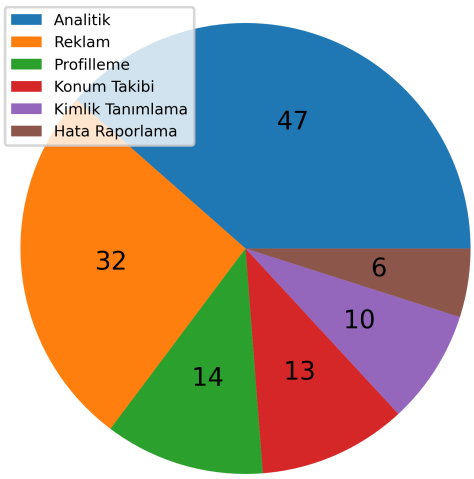
- **Profilleme**: Kullanıcılardan mümkün olduğunca fazla veri toplayarak, kullanıcıların sanal bir profilinin çıkarılması amaçlanır. Bu amaçla, tarayıcı geçmişi, yüklü uygulamaların listesi gibi veriler toplanır.

- **Kimlik Tanımlama**: Bu tür izleyicilerin amacı, kullanıcıların dijital kimliğini belirlemektir. Böylece, geliştiriciler kullanıcıların çevrim içi ve dışı aktiviteleri arasında bağlantı kurabilirler.

- **Reklam**: Bu izleyiciler, kullanıcıların dijital profillerini kullanarak, kullanıcılara hedefli reklamlar göstermeyi ve bu sayede geliştiricilerin uygulamalarından para kazanmalarını amaçlarlar.

- **Konum**: Bu tür izleyiciler Bluetooth, GPS anteni, IP adresi gibi donanımsal ve yazılımsal özellikleri kullanarak kullanıcıların konum bilgisini toplarlar.

Kullanıcı mahremiyetine etkisi farklılık gösterdiği için, tespit edilen izleyiciler bu gruplara göre kategorilere ayrılmıştır. Bazı izleyicilerin birden fazla fonksiyona sahip olduğu ve grupta yer aldığını görülmektedir. Şekil 3.3'te izleyici grupları ve bu gruplar altındaki izleyici sayısı görülebilir. Yukarıda da belirtildiği gibi her grupta bulunan izleyiciler farklı işlevlere sahiptir. Örneğin, farklı amaçlar için olsa bile, Analitik, Profilleme ve Kimlik Tanımlama gruplarındaki izleyici servisleri kullanıcı mahremiyetini diğer gruplardaki servislere göre daha fazla tehdit etmektedir. Bu gruplardaki izleyici servisleri işlevlerini yerine getirmek için, çoğunlukla kullanıcıların kişisel verilerini toplamaya ihtiyaç duymaktadır. Ayrıca, Konum grubu altındaki izleyici servisleri, reklam, ticari satış gibi amaçlarla kullanıcıların konum bilgilerini toplamaktadırlar. Son olarak, reklam grubundaki izleyici servisleri, daha iyi hedefli reklam için kullanıcıların kişisel verilerine erişmekte ve toplamaktadır. Ancak, tüm izleyiciler kötü olarak düşünülmemelidir. Hata Raporlayıcı grubundaki servisler çoğunlukla kullanıcı mahremiyetini tehdit etmemektedir. Yukarıda bahsedildiği gibi, bunlar genellikle uygulama hatalarını geliştiricilere göndermede kullanılırlar. Böylece geliştiricilerin uygulamalardaki problemleri keşfetmelerine ve çözmelerine yardımcı olurlar.



Şekil 3.3: İzleyici Grupları ve Bu Gruplardaki İzleyici Sayısı.

3.1.2 Gizlilik Politikaları ve Sorunlar

İzleyici servisi firmalarının gizlilik politikalarını ve bu firmalarla ilgili gizlilik sorunlarını araştırarak, hangi tür verilerin toplandığı, bu verilerin kimlerle paylaşıldığı ve firmaların GDPR ve CCPA gibi düzenlemelerle uyumlu olup olmadıkları anlaşılmaya çalışılmıştır.

Veri Toplama. Gizlilik politikalarında belirtildiğine göre, tüm izleyici servisleri çeşitli kullanıcı verilerini toplamaktadırlar. Bu servisler işlevlerini yerine getirmek için farklı türde veri toplarlar. Bu bölümün kalanında, izleyici firmaların gizlilik politikalarındaki, veri toplama rutinlerindeki ilginç noktalardan bahsedilmektedir.

İlk olarak, izleyici servislerinin çoğunluğu çeşitli şekillerde konum verisi toplamaktadırlar. Örneğin, neredeyse tüm servisler IP adresini toplamaktadır ve bu bilgi kullanılarak kullanıcıların yaklaşık konumu tespit edilebilir. Bunun yanında, erişilebilir olduğu zaman, bazı servisler cihazın GPS verisine erişerek kullanıcının konumunu tespit edebilirler. Ayrıca, bazı izleyiciler çevredeki Wi-Fi erişim noktaları, hücresel ağ ve Bluetooth verilerini kullanarak konum izleme yapabilir. Son olarak, birkaç izleyici bu metotlardan hepsini kullanarak kullanıcıların tam konumuna erişebilir.

İkinci olarak, neredeyse tüm izleyiciler cihazlardaki iOS Identifier for Advertising (IDFA) ve Google Advertising ID (GAID) gibi reklam ID'lerine reklamcılık amaçlarıyla erişmektedir.

Üçüncü olarak, birçok izleyici IP adresi, MAC adresi, bağlantı tipi (Örn., Wi-Fi, hücresel) vb. ağ tanımlayıcıları toplamaktadır. Bu değerler konum takibi ve cihaz kimlik tespiti için kullanılabilir.

Ek olarak, bazı izleyici servisleri IMEI ve IMSI numaraları gibi cihaz tanımlayıcı değerleri toplamaktadır. Bu değerler kullanıcılar tarafından değiştirilemez ve kullanıcı cihazlarını ayırt etmek için kullanılabilir. IMEI numarasının toplanmasının tehlikelerinden bahseden bir çalışma [54] mevcuttur.

Bunun yanında, bazı izleyiciler kullanıcıları profilleme ve onların cihaz veya uygulama kullanım davranışlarını anlamak için, tarayıcı geçmişi, uygulama kayıtları, uygulama kullanım istatistikleri, çerezler vb. değerleri toplarlar.

Son olarak, bazı izleyici firmalarının gizlilik politikalarında bahsedildiği gibi, bazı firmalar e-posta adresi, cinsiyet, irtibat bilgisi (Örn., telefon numarası) gibi kişi tanımlayabilir bilgileri toplayabilir. Bu tür bilgiler reklam ve izleme amaçlarıyla, kullanıcıları kesin olarak ayırt etmek için kullanılabilir.

Aşağı kısımda, yukarıda açıklanan durumlarla ilgili gerçek dünyadan bazı örnekler listelenmiştir:

- Baidu Inc.'nin büyük veri biriminin eski teknoloji yöneticisi Sang Wenfeng'in sahip olduğu Sensor Analytics firması Xiaomi ile kullanıcı davranışları daha için anlamak için bir ortaklık [55] içindedir.

- Citizen Lab'a göre, *Baidu Mobile Analytic SDK*, kendisini kullanan uygulamalarda hassas veri sızıntısına neden olmaktadır [56]. Bu verinin içinde IMEI numarası, GPS konumu ve yakındaki kablosuz ağların bilgisi yer almaktadır. Bunun yanında, Baidu Map Servisi, IMEI numarası, IMSI numarası, MAC adresi gibi hassas veriler toplayabilir [57].

- Gizmodo tarafından yapılan araştırmaya göre, Bugly isimli hata raporlama servisi kullanan uygulamalar, IMEI numarası ve IP adresi gibi bilgileri toplayarak Çin'de bulunan sunuculara göndermektedir [58].

- Gizlilik politikalarında belirtildiği gibi, Çinli izleme servisi Mintegral, IMEI numaralarını toplayabilir. Ek olarak, Google DoubleClick, Inmobi, MoPub, Tencent, Baiud vb. reklam değişim firmalarıyla iş birliği yapmaktadır [59].

- MoEngabe izleme kodu gömülü olan uygulamalardan, MoEngage'in gizlilik politikasında belirtildiğine göre [60], kullanıcıların e-posta adresi, ismi ve telefon numarası gibi PII'larını toplayabilir.
- Son olarak, AppCensus tarafından yapılan araştırmaya göre [61], JPush servisini kullanan uygulamalar, IMEI numarası, MAC adresi, seri numarası ve tam konum gibi bilgileri Aurora Mobil'in sunucularına gönderebilirler. [61].

Veri Paylaşımı. Gizlilik politikalarının analizine göre, izleyici servisleri kullanıcıların cihazlarından toplanan verileri paylaşabilir. Bu veriler şunlarla paylaşılabilir:

- İştirakler ve Bağlı Ortaklar,
- Servis Sağlayıcılar,
- Kanun Uygulayıcı Birimler,
- Ticari Devir,
- Reklamcılar,
- Araştırmacılar ve Akademisyenler,
- Yayımcılar,
- Veri Ortakları vb.

Bunun yanında, izleyici ekosistemi üzerine yapılan bir çalışmaya göre [32], izleyici servislerinin veri paylaşım uygulamaları kullanıcı mahremiyeti için büyük bir tehlike arz edebilir. Bu çalışma kapsamında en büyük 10 izleyici organizasyon üzerinde yapılan analize göre, bu organizasyonların tümü topladıkları veriyi 3. partilerle ve/veya iştirakleriyle paylaşma hakkına sahiptir. Bu paylaşım rutinlerinden dolayı, farklı firmalar farklı cayma prosedürleri uyguladığı için, kullanıcıların cayma hakları (*opt-out*) tehlikeye girmektedir. Ek olarak, bazı izleyici firmaları birbirleri ile veri paylaşımında bulunabilir. Buna örnek olarak, MoPub firmasının Ad Science, DoubleVerify ve Moat ile yaptığı iş birliği verilebilir [62].

Son olarak, bildiğimiz kadarıyla, tüm izleyici servisleri yasal amaçlardan dolayı veri paylaşımı eğilimi göstermektedir. Ancak, bu kanun uygulayıcı birimlere ve hukuki otoritelere yardımcı olmak için bir iyi niyetten kaynaklanmış olsa dahi, Çin gibi [63] bazı hükümetler tarafından suistimal edilerek kullanıcı mahremiyetini olumsuz yönde etkileyebilir.

Regülasyonlarla Uyumluluk. CCPA, GDPR ve COPPA gibi regülasyonlar sayesinde, kullanıcılar şu açılardan verileri hakkında bilgi ve kontrol sahibidir; ne tür veriler toplanıyor, toplanan veriler kimlerle paylaşılıyor veya kime satılıyor vb. Gizlilik politikaları üzerine yaptığımız analize göre, firmalar bu tür düzenlemeler altında olmadıklarında kullanıcı mahremiyetine daha az önemsemeye meyillilerdir. Yüksek cezalardan dolayı, firmalar bu tür düzenlemeler uyum sağlamak zorunda kalmakta ve kullanıcı verisi ve mahremiyetine daha fazla saygı göstermektedirler. Bu tür regülasyonların dünya geneline yayılması gerekmektedir, çünkü regülasyonlar olmadan firmalar, kullanıcı mahremiyetini Mintegral örneğinde [59] olduğu gibi tehdit etmeye devam ediyor.

3.2 Uygulama İzinleri ve Analizi

Android sistemlerde uygulama izinleri, yapılmak istenen aksiyonları ve sistem kaynaklarına erişimleri kısıtlayarak kullanıcı mahremiyetinin korunmasına katkı sağlar. Bilindiği üzere, Android tarafından uygulama geliştiricilere çeşitli API fonksiyonları sunulmuştur. Uygulama izinleri yardımı ile bu fonksiyonlara erişim kısıtlanır.

Sistemlerde kullanılan 3 farklı izin tipi bulunmaktadır. Bunlar; yükleme zamanı izinleri, çalışma zamanı izinleri ve özel izinler olarak listelenebilir. Her izin türü, uygulamaların erişim kısıtlarının kapsamını belirlemede farklı rol oynamaktadır.

3.2.1 Yükleme Zamanı İzinleri

Bu tür izinler, uygulamaların kullanıcı mahremiyetini ve sistem üzerindeki diğer uygulamaları en az seviyede etkileyeceği durumları kapsamaktadır. İsminde de belirtildiği üzere, bu izinler uygulama cihaza yüklenirken sistem tarafından otomatik olarak verilir, yani kullanıcının ek olarak izni alınmaz. Bu tür izinler iki alt başlıkta incelenebilir.

Normal İzinler. Bu tür izinler uygulama cihaza yüklenirken otomatik olarak verilir. Bunun ana sebebi, bu tür izinler sonucunda uygulamaların kullanıcı mahremiyetini en az seviyede etkileyecek kaynaklara erişim sağlamasına izin verilir. Bu kaynaklar genellikle uygulama kum havuzu dışında yer almaktadır. Bu izinlere örnek olarak, ağ durumunu erişim (ACCESS_NETWORK_STATE), internet erişimi (INTERNET), titreşime erişim (VIBRATE) verilebilir.

İmza İzinler. İmza izinleri, aynı sertifika ile imzalanmış uygulamalar tarafından birbirlerinin kaynaklarına erişmek amacıyla kullanılabilir. Eğer cihaz üzerinde yüklü olan bir uygulama, bir imza izin tanımladıysa ve bu uygulama ile aynı sertifika ile imzalanmış başka bir uygulama cihaza yüklenirse, yeni yüklenen uygulamanın tanımladığı imza izinler sistem tarafından otomatik olarak onaylanır.

Bu tür izinlerden bazıları 3. parti uygulamalar tarafından kullanılamaz. Sistem sertifikası ile aynı sertifikaya sahip uygulamalar (ön yüklü uygulamalar) da çeşitli imza izinleri tanımlayabilir.

3.2.2 Çalışma Zamanı İzinleri (Tehlikeli İzinler)

Çalışma zamanı izinleri aynı zamanda tehlikeli izinler olarak da bilinir. Bu izinler, kullanıcı mahremiyetini ve güvenliğini yüksek seviyede etkileyecek kaynaklara erişimi kontrol etmek için kullanılır. Bu izinler Android 6.0 ile birlikte, uygulama izinin gerektiği kaynağa erişeceği zaman kullanıcının onayı alınarak verilmektedir. Daha önceki versiyonlarda ise, yine kullanıcı onayı ile yükleme zamanında verilmektedir. Bu izinlere örnek olarak, konum erişimi (ACCESS_FINE_LOCATION), kamera erişimi (CAMERA), kişilere erişim (READ_CONTACTS), mesaj gönderme (SEND_SMS) gibi izinler verilebilir.

3.2.3 Özel İzinler(*Special Permissions*)

Özel izinler, bazı spesifik işlemleri gerçekleştirmek için kullanılır. Bu izinler sadece platformun kendisi ve OEM'ler tarafından tanımlanabilir. Bunun yanında, platform ve OEM'ler yüksek yetki gerektiren işlemleri korumak ve erişimlerini yönetmek için bu izinleri kullanırlar.

3.2.4 Özel Tanımlanmış İzinler (*Custom Permissions*)

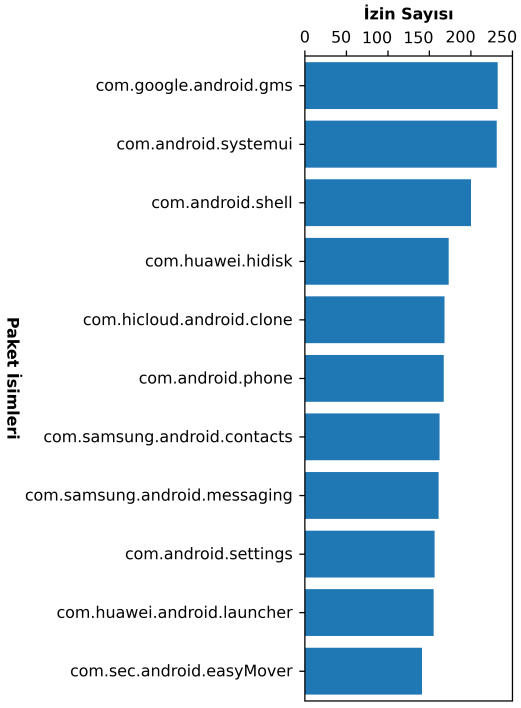
Android, uygulama geliştiricilerin kendi izinlerini tanımlamalarına izin vermektedir. Bilindiği üzere, Android sistemlerde Linux sistemlere benzer bir şekilde her uygulamanın kendi kullanıcı ID değeri vardır. Böylece uygulamalar birbirlerinden izole bir şekilde çalışırlar. Uygulama geliştiriciler kendi fonksiyonelliklerini başka uygulamalar paylaşmak amacıyla izin tanımlayabilirler. Ayrıca, yine izin tanımlayarak aynı sertifika ile imzalanmış başka uygulamaların, izni tanımlayan uygulamanın kaynaklarına otomatik olarak erişimi sağlanabilir. Bu yöntem, genellikle aynı uygulama geliştirici tarafından geliştirilmiş farklı uygulamaların iletişiminde kullanılmaktadır.

3.2.5 Uygulama İzinlerinin Analizi ve Etkileri

Yukarıda da belirtildiği gibi Android sistemlerde amaçlarına göre birçok türde izin bulunmaktadır. Bu izinlerden özellikle, Çalışma Zamanı İzinleri ve Özel Tanımlanmış İzinler kullanıcı mahremiyeti ve güvenliği açısından önemlidir. Bu kapsamda, ön yüklü uygulamalardaki izinler üzerinden çeşitli analizler yapılmıştır.

İzin Sayılarının Analizi. İlk olarak bazı uygulamaların çok fazla sayıda izin tanımladıkları tespit edilmiştir. Özellikle üreticilere ait bazı uygulamaların 140'ın üzerinde izin tanımladıkları görülmektedir. En çok izin tanımlayan uygulamalardan bazılarının listesi Şekil 3.4'te gösterilmiştir. Bu durum direkt olarak kullanıcı mahremiyetini ihlal etmese bile, yine de kullanıcı mahremiyeti açısından önemlidir.

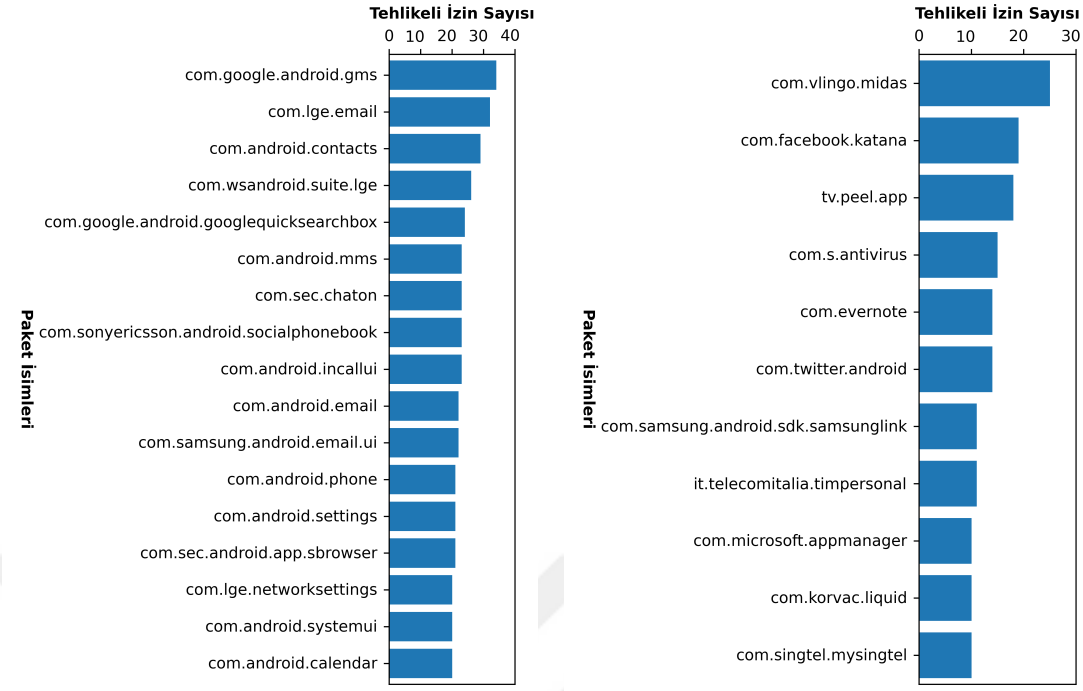
Ardından, uygulamalar tarafından tanımlanan tehlikeli izinler kontrol edilmiştir. Android sistemlerde tehlikeli izinler kullanıcı mahremiyeti açısından büyük önem arz ettiği için, uygulama marketlerindeki uygulamaların bu izinleri kullandığı durumlarda kullanıcılar bilgilendirilmekte ve kullanıcıların onayı alınmaktadır. Ancak ön yüklü uygulamalarda -özellikle üreticilere ait uygulamalarda- kullanıcılara bilgi verilmemekte ve onayları alınmamaktadır. Ön yüklü uygulamalardan üreticilere ve 3. partilere ait uygulamaların kullandığı tehlikeli izinler analiz edildiğinde, bazı uygulamaların yüksek sayılarda tehlikeli izin tanımladığı tespit edilmiştir. Üreticilere ve 3. partilere ait uygulamaların tanımladıkları tehlikeli izin sayıları Şekil 3.5'te gösterilmiştir. Bu durum daha önce de belirtildiği gibi kullanıcı mahremiyeti açısından büyük tehlike oluşturmaktadır. Bunun yanında, uygulamalar tarafından en çok kullanılan tehlikeli izinler çıkarılmıştır. Yine bu izinler Şekil 3.6'da görülebilir. Sonuçlar incelendiğinde 1,962 tane uygulamanın cihaz üzerinde kayıtlı kişilere erişebildiği (READ_CONTACTS) görülmektedir. Yine birçok uygulamanın, kullanıcıların yaklaşık ve tam konumlarına (ACCESS_COARSE_LOCATION ve ACCESS_FINE_LOCATION) erişim izni istediği görülmektedir. Son olarak, bazı uygulamaların telefon kamerası, cihazdaki mesajları



Şekil 3.4: En Fazla Sayıda İzin Kullanan Uygulamalar.

okuma ve mesaj gönderme gibi kullanıcı mahremiyeti ve güvenliğini etkileyebilecek izinler aldıkları görülmüştür.

Daha sonra, uygulamaların farklı cihazlarda ve üreticilerde tanımladıkları izin sayıları kontrol edilmiştir. Bu kapsamda uygulamaların farklı cihazlarda tanımladıkları izin sayılarının ortalaması alınmıştır. Ardından, en az ve en çok sayıda tanımlanan izin sayıları bu ortalamadan çıkarılmıştır. Elde edilen değerlerin farkının 9'dan büyük olduğu durumlar için daha detaylı bir inceleme gerçekleştirilmiştir. Bu inceleme sonucunda, aynı uygulamaların farklı cihazlarda farklı sayılarda izin tanımladıkları görülmüştür. Bu bazı uygulamaların aşırı yetkili (*over-privileged*) olarak çalıştığı konusunda gösterge olabilir. Örneğin, bazı durumlarda Samsung ve Huawei cihazların diğer üreticiler tarafından üretilen cihazlara göre çok daha fazla izin tanımladıkları görülmüştür. `com.android.settings` paket isimli uygulama bazı Samsung cihazlarda 156 ve Huawei cihazlarda 143 tane izin kullanırken, Sony cihazlarda 68 izin tanımladığı tespit edilmiştir. Ayrıca aynı uygulamaları farklı cihaz üreticileri tarafından farklı yetkilere sahip olduğu da tespit edilmiştir. `com.osp.app.signin` uygulaması, bazı Samsung cihazlarda 12 izin tanımlarken, bazılarında 82 izin tanımladığı görülmüştür. Bu analiz kapsamında tespit edilen uygulamaların paket ismi, uygulamanın en az tanımladığı izin sayısı ile cihaz üreticisi, en çok tanımladığı izin sayısı ile cihaz üreticisi ve farklı cihazlarda ortalama tanımladığı izin sayıları Çizelge 3.3'te gösterilmiştir.



(a) Üreticilere Ait En Çok Tehlikeli İzin Tanımlayan Uygulamalar.

(b) 3. Partilere Ait En Çok Tehlikeli İzin Tanımlayan Uygulamalar.

Şekil 3.5: En Çok Tehlikeli İzin Tanımlayan Uygulamalar.

Şekil 3.6: Uygulamalar Tarafından En Çok Kullanılan Tehlikeli Uygulamalar.

Çizelge 3.3: Uygulamalar ve Farklı Cihazlarda Tanımladıkları İzin Sayıları.

Paket Adı	**En Az Tanımladığı İzin Sayısı ve Cihaz Üreticisi**	**En Çok Tanımladığı İzin Sayısı ve Cihaz Üreticisi**	**Ortalama Tanımlanan İzin Sayısı**
com.google.android.dialer	45 (General Mobile)	74 (Xiaomi)	67
com.android.server.telecom	3 (LG)	54 (Samsung)	36
com.google.android.gms	107 (LG)	232 (Xiaomi)	193
com.samsung.knox.securefolder	62 (Samsung)	98 (Samsung)	88
com.samsung.android.app.smartcapture	46 (Samsung)	76 (Samsung)	70
com.osp.app.signin	12 (Samsung)	82 (Samsung)	62
com.samsung.android.scloud	43 (Samsung)	102 (Samsung)	86

Özel Tanımlanmış İzinlerin Analizi. Uygulamaların tanımladığı özel tanımlanmış izinler analiz edilmiştir. Bu izinler, uygulamalar tarafından manuel olarak tanımlandığı ve farklı uygulamaların birbirlerinin kaynaklarına erişim sağlamak için kullanıldıkları için önemlidir. Analiz sonucunda bazı üretici ve 3. parti firmaların uygulamalarında, aynı özel tanımlanmış izinler tespit edilmiştir. Örneğin, bazı cihazlarda DOWNLOAD_WITHOUT_NOTIFICATION izninin üretici (Samsung), platform (Google) ve 3. parti (Facebook (`com.facebook.katana`), IronSource (`com.ironsource.appcloud.oobe.hutchison`), Orange (`com.orange.aura.oobe`), Digital Turbine Ignite (`com.dti.globe`) vb.) firmalara ait uygulamalar tarafından ortak olarak kullanıldığı görülmüştür. Bu izne sahip uygulamalar kullanıcının haberi olmadan cihaz veri indirebilir. Ayrıca, yine Digital Turbine Ignite (`com.dti.samsung`) gibi bazı 3. partilere ait uygulamaların, `com.samsung.android.knox.permission.KNOX_SECURITY` iznine sahip oldukları tespit edilmiştir. Bu izni `com.android.systemui` uygulaması gibi üreticilere ait ön yüklü uygulamalar kullanmaktadır ve bu izne sahip olan uygulamalar Samsung cihazlarda, cihazın ön yüklü e-mail ve Google hesaplarının kontrolü, cihazdaki parola politikasının kontrolü, sertifikaların ve *keystore*'un yönetimi, cihaz kilit ekranın kontrolü gibi yüksek yetki gerektiren işlemleri gerçekleştirebilir.

Ek olarak, Facebook firmasına ait ön yüklü uygulamaların `com.facebook.system.stub.ENABLE_APPMANAGER` gibi bazı izinleri birbirleri ile ortak olarak tanımladıkları tespit edilmiştir. Birçok cihazda Facebook App Manager uygulamasının, Facebook firmasına ait Messenger, Instagram gibi uygulamaları güncellemek için kullanıldığı tespit edilmiştir [64, 65]. Bu kapsamda yapılan analizde, `com.instagram.android`, `com.facebook.katana` ve `com.facebook.orca` gibi paketlerin bu izni kullandığı görülmüştür. Yani bu izne sahip uygulamalar, Google Play Store gibi uygulama marketlerine ihtiyaç duymadan kendilerini güncelleyebilmektedir. Özellikle Facebook ile Samsung firmaları arasındaki iş birliği daha önce de araştırmacıların dikkatini çekmiş ve bu durumun kullanıcı mahremiyetine etkileri ile ilgili çeşitli araştırmalar yapılmıştır [15, 66]. Yine Samsung cihazlarda bulunan Vlingo uygulamasının, kritik sistem uygulamaları ile birlikte com.android.email.permission.ACCESS_PROVIDER iznine sahip olduğu tespit edilmiştir. Bu izin ile sistemdeki e-mail sağlayıcıya ait kullanıcı parolaları ve diğer gizli bilgilere erişilebilmektedir. Vlingo firmasının, daha önce cihazlardan kullanıcılara ait çeşitli bilgileri topladığı ve bu bilgileri kendisine ait sunuculara gönderdiği tespit edildiği için [67], bu durum kullanıcı mahremiyeti açısından bir tehdit oluşturmaktadır.

Son olarak, sistemlerde daha önce isimleri çeşitli kullanıcı mahremiyetini ihlallerinde geçen uygulamalar bulunmuştur. Bu uygulamaların, üreticilerle ortak izinler tanımladıkları tespit edilmiştir. Bu uygulamalardan Hiya [68] ve TrueCaller [69] arama koruma servisi olarak görev yapmaktadır. Bu firmaların gizlilik politikalarında, son kullanıcıya ait cihazdaki kayıtlı kişilerin bilgisi, UID değerleri ve kişisel bilgilerin toplandığı belirtilmiştir [70]. Bununla birlikte bir reklam firması olan Digital Turbine Ignite ve bu firmaya bağlı olan LogiaGroup firmalarına ait çeşitli uygulamalar (`com.LogiaGroup.LogiaDeck`, `com.dti.globe`,`com.dti.samsung`) tespit edilmiştir. Bu firmanın da gizlilik politikasında da UID değerleri, trafik kayıtları gibi bilgileri topladığı ve bu bilgileri iş ortakları ile paylaştığı belirtilmiştir [71]. Örneğin `com.dti.samsung` uygulaması firmanın Samsung ile iş birliği yaptığının bir göstergesidir. Benzer şekilde diğer bir reklam firması Iron Source ve bu firmanın *AURA Enterprise Solutions* isimli çözümüne [72] ait çeşitli ön yüklü uygulamalar da (`com.`

`ironsource.appcloud.oobe.hutchison`, `com.orange.aura.oobe`) tespit edilmiştir. Bu uygulamaların, kullanıcılara cihazlarını ilk çalıştırırken çeşitli özelleştirme seçenekler sunan ve bu sırada kullanıcı aktivitelerini de gözlemleyen uygulamalar (OOBE) oldukları görülebilir.

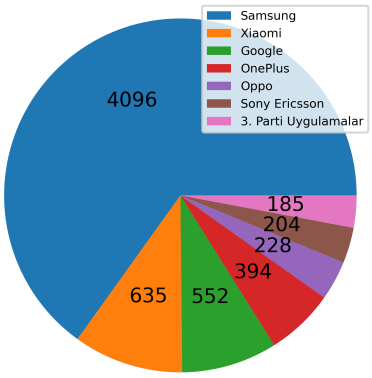
3.3 Manifest Özellikleri Analizi

Android uygulamalarda manifest dosyası [73], uygulamaya özel gereksinimleri barındıran ve XML formatında olan bir dosyadır. Bu gereksinimler uygulama paket adı, uygulama bileşenleri (*Activity, Service, Broadcast Receiver, Content Provider*), uygulama izinleri, uygulama özellikleri, manifest özellikleri vb. kapsar. Yaptığımız analiz kapsamında, kullanıcı güvenliği açısından manifest dosyasındaki en kritik alanlar arasında düşündüğümüz, sharedUserId, allowBackup, usesClearTextTraffic ve debuggable gibi özellikleri inceledik. Devam eden kısımda, neden bu alanların önemli olduğu ve bu alanlardaki hatalı konfigürasyonların kullanıcı mahremiyeti ve güvenliğine etkisinden bahsedilmektedir.

sharedUserId. Android sistemlerde, her uygulamaya eşsiz bir kullanıcı ID değeri atanır. Ancak, bazı durumlarda, bir cihazda aynı geliştiriciye veya firmaya ait birden fazla uygulama olabilir ve bu uygulamalar arası kaynak paylaşımı (Örn., izinler, kod) yapılmak istenebilir. Bu tür durumlarda, uygulamalar Linux sistemlere benzer bir şekilde aynı kullanıcı ID değerine sahip olmalıdır. Bu işlevselliği sağlamak için *sharedUserId* özelliği kullanılır. Fakat, bu özelliği hatalı kullanımı güvenlik zafiyetlerine yol açabilir. Ayrıca, saldırganlar bu özelliği kullanarak zararlı kod parçalarını kullanıcılar ve güvenlik analistlerinden gizleyebilirler. Ek olarak, sistem ile aynı sertifika ile imzalanan ön yüklü uygulamalar, Android sistemlerdeki en yetkili kullanıcılardan birisi olan sistem kullanıcısı hakları ile çalışabilirler. Analiz edilen 14,178 uygulamadan 3,303 tanesi uygulamaya sistem hakları veren "android.uid.system" sharedUserId değerine sahiptir. Saldırganlar bu uygulamalardaki potansiyel zafiyetleri sömürerek cihazlara sistem haklarıyla erişim sağlayabilirler [74]. Bunun yanında, Adups zararlı yazılımı [11] gibi içeriden tehditler, *Giriş* bölümünde belirtildiği gibi cihazlarda ön yüklü olarak gelebilirler. Ek olarak, ihtiyacı olmasa bile sistem hakları ile çalışan bazı uygulamalar (Örn., `com.cad.fmradio`) tespit edilmiştir. Bu durum açık bir şekilde en az yetki prensibini ihlal etmektedir. Bundan sonra, sistem yetkileri ile çalışan herhangi bir 3. parti uygulama olup olmadığını kontrol edilmiştir. Yapılan analiz sonucu bu tarz çalışan herhangi bir uygulama tespit edilmemiştir. Yine de, bu özelliğin neden olduğu kararsız davranışlardan dolayı, Android tarafından API 29'da kullanımı kaldırılmıştır.

allowBackup. Manifest dosyasında bu özellik açık olduğunda (allowBackup=true) ve cihazda USB hata ayıklaması modu aktif olduğunda, uygulama verileri cihaza fiziksel erişimi olan herhangi birisi tarafından yedeklenebilir. Böylece, /data/data/paket_adı dizininin altında bulunan verilen akıllı telefon dışına kopyalanabilir. Eğer bu dizin altında PII, parola, anahtar gibi bilgiler şifresiz olarak depolanırsa, saldırganlar tarafından kolay bir şekilde ele geçirilebilir. Bu çalışma kapsamında, hangi uygulamalarda allowBackup özelliğinin aktif olduğunu ve bu uygulamaların oluşturduğumuz sertifika gruplarına göre dağılımlarını inceledik. İlk olarak, adb kullanılarak veri yedeklenmesine izin veren toplamda 6,847 uygulama tespit ettik. Şekil 3.7'de yedeklemeye izin veren uygulamaların sayısı ve bu uygulamaların üreticilere göre dağılımı görülebilir.

Analize göre tüm üreticilerin allowBackup özelliğini kullandıkları görülmektedir. Bundan dolayı, bu konu üzerinde gelecekte daha detaylı bir araştırma yapılmalıdır, çünkü uygulamalar bu özelliği kullanıcılara yedekleme özelliği sunmak için kullanabilir. Ancak, böyle bir amaçla kullanılsa bile yedeklenen verilerin şifrelenerek korunmasına dikkat edilmelidir.



Şekil 3.7: allowBackup Özellikli Uygulama Sayısı ve Üreticilere Göre Dağılımları.

usesClearTextTraffic. Bu özellik aktif olduğunda (usesClearTextTraffic=true), uygulamalar ağ bağlantılarında şifresiz trafik kullanabilirler. Bu durumda ağ trafiği saldırganlar tarafından dinlenerek özel ve hassas verilerin eli geçirilmesine yol açabilir [75]. Günümüzde, uygulama geliştiricilerin çoğunluğu sunucularına bağlanırken ve veri yollarken şifreli bağlantı metotlarını kullanmayı tercih etmektedir. Android 6.0 ile birlikte, uygulama geliştiriciler *usesClearTextTraffic* özelliğini aktifleştirerek uygulamalarının açık metin bağlantı kurmalarını engelleyebilirler. Ancak, yapılan analiz sonucunda, bu bayrak değerini "true" olarak ayarlayan uygulamalar tespit edilmiştir. Analiz edilen uygulamalardan 1,270 tanesi, verilerini sunucuya şifresiz olarak yollayabilmektedir. Bu uygulamalardan çoğunluğunun OEM'lere ve sadece 37 tanesinin 3. parti firmalara ait olduğunu belirlenmiştir.

debuggable. Son olarak hangi uygulamaların *debuggable* özelliği aktif olarak geldiğini kontrol edilmiştir. Bu bayrağı aktif olan uygulamalar, cihaza fiziksel erişimi olan kişiler tarafından, jdb [76] gibi araçları kullanarak hata ayıklaması yapılabilir. Bu özellik kullanılarak uygulama sınıfları ve fonksiyonları görülebilir ve hatta saldırganlar tarafından manipüle edilebilir. Ek olarak, uygulamanın izinleri dahilinde sistem üzerinde herhangi bir kod çalıştırılabilir. Bundan dolayı, yayınlanan uygulamalarda bu bayrağın değerinin "false" yapılması şiddetle önerilmektedir. Çalışma sonucunda, bu bayrağın aktif olduğu sadece 5 uygulama bulunmuştur. Bunlarda 3 tanesi `com.sec.android.kiosk` paketinin farklı versiyonları, diğerleri ise `com.trendmicro.mars.mda.httpserver`, ve `com.huawei.camera2.mode.cosplay` paketleridir. Ayrıca, `com.huawei.camera2.mode.cosplay` paketinin Android Debug Sertifikası ile imzalandığı [47] tespit edilmiştir. Birçok uygulama marketi bu sertifika ile imzalanmış uygulamaları kabul etmemekte ve bu sertifikanın üretimdeki uygulamalarda kullanılmaması önerilmektedir.

Manifest dosyası analizine göre, *sharedUserId* ve *debuggable* özellikleri için geliştiricileri çoğunlukla en iyi uygulamaları takip ettikleri görülmüştür. Ancak, *allowBac-*

kup ve *usesClearTextTraffic* özellikleri için uygulama geliştiricileri en iyi uygulamaları daha dikkatli bir şekilde takip etmelidir.

3.4 Bulut Servisleri Analizi

Neredeyse tüm Android uygulamaları, işlevlerini yerine getirmek için arka planda çeşitli sunuculara bağlanmaktadır. Bu sunucular, veri depolama, uygulamanın ihtiyacı olan bilgiyi sorgulama, uygulama için çeşitli işlemleri gerçekleştirme gibi çeşitli amaçlar için kullanılabilir. Ancak, her geliştirici veya firmanın kendi sunucu alt yapısının oluşturacak zamanı ve kaynağı yoktur. Bu kaynaklara sahip olsa bile bazıları yine de listelenen amaçlar için kendi sunucu alt yapısını kurmamayı seçer. Kendi sunucularını kullanmak yerine, geliştiriciler ihtiyaçlarını karşılamak için bulut tabanlı çözümlerden faydalanırlar. Çünkü, bu çözümleri yönetimi çok daha kolay ve kendi sunucunu çalıştırmaya birçok avantajı vardır. Bulut tabanlı çözümler geliştiricilere veri depolama, bildirim yönetimi, analitik, API tabanlı servisler vb. birçok fonksiyonellik sunar. Mobil ekosistemdeki kritik rolünden dolayı, bulut tabanlı çözümler mahremiyet ve güvenlik açısından dikkatli bir şekilde yönetilmelidir. Bazı bulut çözümleri varsayılan olarak güvenlik olsa dahi, geliştiriciler kullanmadan önce bunların konfigürasyonları ve çalışma mantıkları hakkında bilgi sahibi olmalıdır. Maalesef, önemli sayıda geliştirici bu konfigürasyonları önemsememekte ve bu milyonlarca kişiyi etkileyebilmektedir. Bazı çok kullanılan bulut servisleri şunlardır: Google Firebase [77], Amazon Web Services (AWS) [78], Microsoft Azure [79], Google Maps API [80] vb. Bazı ön yüklü uygulamalar da bu servileri kullandıklarından dolayı, ön yüklü uygulamaların hangi bulut servislerini kullandıklarını ve bu servislerde ne tür hatalı konfigürasyonlar olabileceğini incelenmiştir.

İlk olarak, neredeyse tüm bulut servisleri kullanırken özel anahtarlar, sırlar ve URL formatlarına ihtiyaç vardır ve bu değerlerin ifşası, firma kaynaklarına yetkisi erişim, hassas ve gizli bilgi sızıntısı, servis dışı bırakma, şirket kaynaklarının gereksiz tüketimi ile sonuçlanabilir. Bu değerleri tespit edilmesi ve çıkarılmasında, çeşitli araçlar [81–84] ve özelleştirilmiş betikler kullanılmıştır. Ek olarak, bazı uygulamaları tersine mühendislik ile manuel olarak analiz edilmiştir. Bu çalışmanın sonucunda, Google Maps API, AWS, Firebase, Slack Webhooks ve OAuth [85] ile bağlantılı değerler tespit edilmiştir. Daha sonra, bu değerlerin güvenliğini otomatize olarak test etmek için, Python programlama dilinde özelleştirilmiş betikler yazılmıştır. Aşağıda kullanıcı mahremiyeti ve güvenliğini etkileyebilecek ilginç sonuçları listelenmektedir.

Google Maps API. Bu API servisi uygulama geliştiricilere, Google Maps Veri tabanı'nın özelliklerini uygulamalara yerleştirme ve bu veri tabanını kullanarak arama yapma imkanı sunar. 2018 yılına kadar, geliştiriciler bu servisi ücretsiz ve istedikleri şekilde kullanabiliyordu. Ancak 2018 yılından sonra, Google kullandıkça-öde modelini devreye soktu [86]. Bu modelde ücret, her Ürün Depo-Tutma Birimi (SKU)'ne yapılan istek sayısına göre belirlenmektedir. Her SKU, çağrılan servis veya işlevsellikle birlikte Ürün API değerinin kombinasyonundan [87] oluşur (Örn., Place API - Photo Details). Google Maps API değerlerini toplu olarak tespit etmek için apkleaks [81] aracının (URI, uç nokta ve sırları tespit etmek için çeşitli düzenli ifadeleri (REGEX) kullanan bir Python betiği) modifiye edilmiş bir versiyonu kullanılmıştır. API anahtarlarını tespit ettikten sonra, bunları kullanarak yapılabilecek yetkisiz erişimleri

bulmak için gmapapiscanner [84] isimli betiğin modifiye edilmiş versiyonu kullanılmıştır. Analiz sonuçları *Zafiyetli SKU*, SKU'yu kullanan *Zafiyetli Uygulama Sayısı* ve SKU'da bulunan zafiyelerin *Etki(ler)*'inden oluşan Çizelge 3.4'te listelenmiştir. Bu zafiyetler, geliştiricinin veya firmanın aylık kotasının tüketilmesine yol açabilir. Ek olarak, ay sonunda fazla faturalarla karşı karşıya gelebilirler. Son olarak, azami fatura limiti durumlarında, saldırganlar aylık kotayı tüketerek servis dışı bırakmalara yol açabilirler. Bu durumlar kullanıcı mahremiyetini ve güvenliğini direkt olarak etkilemese de uygulamaların işlevselliğini kısıtlayarak kullanıcıları dolaylı yoldan etkileyebilirler.

Çizelge 3.4: Zafiyetli Google Maps API SKU'ları ve Bulundukları Zafiyetli Uygulama Sayısı ile Etkileri.

Zafiyetli SKU	**Zafiyetli Uygulama Sayısı**	**Etki(ler)**
Places Photo API	199	1000 istek başına - $7
Nearby Search-Places API	198	1000 istek başına - $32
Text Search-Places API	198	1000 istek başına - $32
Find Place From Text API	196	1000 element başına - $17
Autocomplete API	196	1000 istek başına - $2.83, 1000 Oturum başına - $17
Place Details API	196	1000 istek başına - $17
Staticmap API	161	1000 istek başına - $2
Geocode API	81	1000 istek başına - $5
Geolocation API	51	1000 istek başına - $5
Timezone API	36	1000 istek başına - $5
Embed (Basic) API	26	Ücretsiz
Elevation API	16	1000 istek başına - $5
Streetview API	15	1000 istek başına - $7
Embed (Advanced) API	12	Ücretsiz
Directions API	7	1000 istek başına - $5
Distance Matrix API	5	1000 istek başına - $5
Nearest Roads API	4	1000 istek başına - $10
Route to Traveled API	4	1000 istek başına - $10

Amazon Web Servisleri. Amazon Web Servisleri (AWS), mobil uygulama geliştiricileri ve firmaları tarafından yaygın bir şekilde kullanılan bir bulut platformudur. Bulut platformları arasında en yaygın kullanılan platform olduğu için [88], diğer platformlara göre saldırganların daha fazla dikkatini çekmektedir. Mobil uygulama özellikle AWS'nin alt servislerinden birisi olan Amazon Basit Depolama Servisi (Amazon S3)'ni çeşitli objeleri depolamak için kullanırlar. Amazon S3'ü düzgün bir şekilde anlamak için "kova (bucket)", "obje (object)", "anahtar (key)" ve "bölge (region)" gibi konseptler bilinmelidir. Bir çeşit konteyner olan kova, objeleri organize etmek ve depolamak için kullanılır. Objeler, obje verisi ve üst veriden oluşan temel bileşenlerdir. Her objeyi ayırt etmek için anahtarlar kullanılır. Son olarak, bölgeler, kovaların hangi coğrafik konumda depolandığını gösterir. Örneğin, https://awsexamplebucket1.s3.us-west-2.amazonaws.com/photos/puppy.jpg şeklindeki bir URL'de "awsexamplebucket1" kullanılan kovanın adı, photos/puppy.jpg obje ve us-west-2 ise kovanın depolandığı coğrafik bölgedir.

Kovalara erişmek ve bu kovalarda objeleri depolamak için, geliştiriciler AWS erişim anahtar ID'si ve AWS gizli erişim anahtarı isimli API anahtarlarına ihtiyaç duyarlar. Bu anahtar çiftinin ifşası, saldırganların S3 kovalarına ve bu kovalarda depolanan objelere erişmesine neden olabilir. Amazon'un bu anahtarların yönetimi için en iyi uygulamaları içeren bir dokümanı [89] vardır. Bu en iyi uygulamalara göre, bu anahtarlar uygulama kodu içinde direkt olarak depolanmamalıdır. Bunun yerine Amazon tarafından dokümanda önerilen yerlerde depolanmalı veya "Token Vending Machine" [90] kullanılmalıdır. Ek olarak, güvenlik sebeplerinden dolayı bu anahtarlar periyodik olarak yenilenmelidir.

Tez çalışması kapsamında, apkleaks aracını kullanarak ve APK dosyalarını tersine mühendislik ile incelenerek, birçok S3 kovası, AWS erişim anahtar ID'leri ve AWS gizli erişim anahtarları tespit edilmiştir. Bu değerler arasından, Amazon S3 kovalarına bağlanmak için gerekli olan birkaç anahtar çifti bulunmuştur. Bu anahtar çiftlerinin hala aktif olup olmadıklarını ve bu firmaların S3 kovalarına erişim için kullanılabilirlik durumları test edilmiştir. Bu testler sonucunda, iki farklı firmaya ait hala aktif durumda S3 anahtar çiftleri tespit edilmiştir. Geçerli anahtar çifti sayısı çok az sayıda olsa bile, bu aktif anahtarların neden olduğu etkinin çok büyük olduğu görülmüştür. Bu anahtarları kullanarak firmaların S3 kovalarına erişim sağlanmış ve bu erişim sonucunda, kovalarda mevcut uygulamaya ait verilerin yanında, başka uygulama ve servislere ait kovaların ve objelerin de depolandığı tespit edilmiştir. Bu durum en az yetki prensibini açık bir şekilde ihlal etmektedir. Bunun yanında, bu kovalarda bulunan objeler incelenmiş ve PII, erişim bilgileri, uygulamaların ve servislerin kaynak kodları vb. bilgiler bulunmuştur. Sonuç olarak, geliştiriciler bu anahtarları güvenli bir şekilde kullanmalı ve bu değerlerin ifşasının etkilerinin farkında olmalıdır.

Google Firebase veri tabanı. Google geliştiricilere ve firmalara verilerin JSON formatında depolamak için bulut tabanlı bir veri tabanı [77] sunmaktadır. Firebase Gerçek Zamanlı veri tabanı isimli bu veri tabanı geliştiricilere SDK aracılığı ile, gerçek zamanlı senkronizasyon, çevrim dışı yanıt yönetimi, çoklu veri tabanı ölçeklenebilirliği ve istemci cihazlarından (Örn., mobil cihaz veya web tarayıcı) direkt erişim gibi anahtar kabiliyetler sunmaktadır. Bu veri tabanından faydalanmak için, geliştiriciler Firebase konsolundan bir veri tabanı oluşturmalıdır. Bu oluşturulan veri tabanının URL modeli <veriTabanıAdı>.firebase.io veya bölge sağlandıysa <veriTabanı-

Adı>.<bölge>.firebase.io şeklinde gözükmektedir. Varsayılan olarak, oluşturulan bu veri tabanında herkes erişebilir. Bundan dolayı Firebase veri tabanları, yetkisiz okuma ve yazmaları önlemek için düzgün bir şekilde konfigüre edilmelidir.

Tez çalışmasında, yukarıda bahsedilen URL modelini kullanarak apkleaks aracı ile Firebase URL'lerini tespit edilmiştir. Firebase veri tabanından faydalanan toplamda 665 uygulama bulunmuş ve bu uygulamalar yazılan özel Python betikleri ile test edilmiştir. Bu test kapsamında Firebase veri tabanının herkes tarafından okunulabilir olup olmadığını kontrol etmek için, URL'nin sonuna ".json" ifadesi eklenerek HTTP GET isteği yapılmalıdır. Eğer bu isteğe dönen durum kodu 200 ise veri tabanı herkes tarafından okunulabilir olduğu anlaşılabilir. Ek olarak, yazılabilir veri tabanlarını tespit etmek için, JSON formatında bir veri ile PUT isteği yapılır ve yine dönen durum kodu 200 ise veri tabanı yazılabilir olduğu anlaşılabilir. Sonuç olarak, herkese okuma-yazma izni veren 2 farklı uygulamaya ait 2 farklı Firebase veri tabanı tespit edilmiştir. Ancak 2 veri tabanında da kullanıcılara veya firmalara ait, hassas veya gizli bir verinin bulunmadığı görülmüştür. Bu veri tabanlarından birisi Xiaomi firmasına, diğeri ise 3. parti bir haber uygulamasına aittir. Ayrıca başka bir güvenlik araştırmacısının, tespit edilen bir veri tabanına kendi verilerini yazdığı tespit edilmiştir. Bu URL'lerin ifşasının ve hatalı konfigürasyonun etkisi az olsa da geliştiriciler ve üreticiler bu veri tabanlarının kullanımı ve konfigürasyonu konusunda dikkatli olmalıdır. Çünkü potansiyel bir hatalı konfigürasyon durumunda kullanıcılara ve firmalara ait hassas ve gizli bilgilerin sızıntısı yaşanabilir.

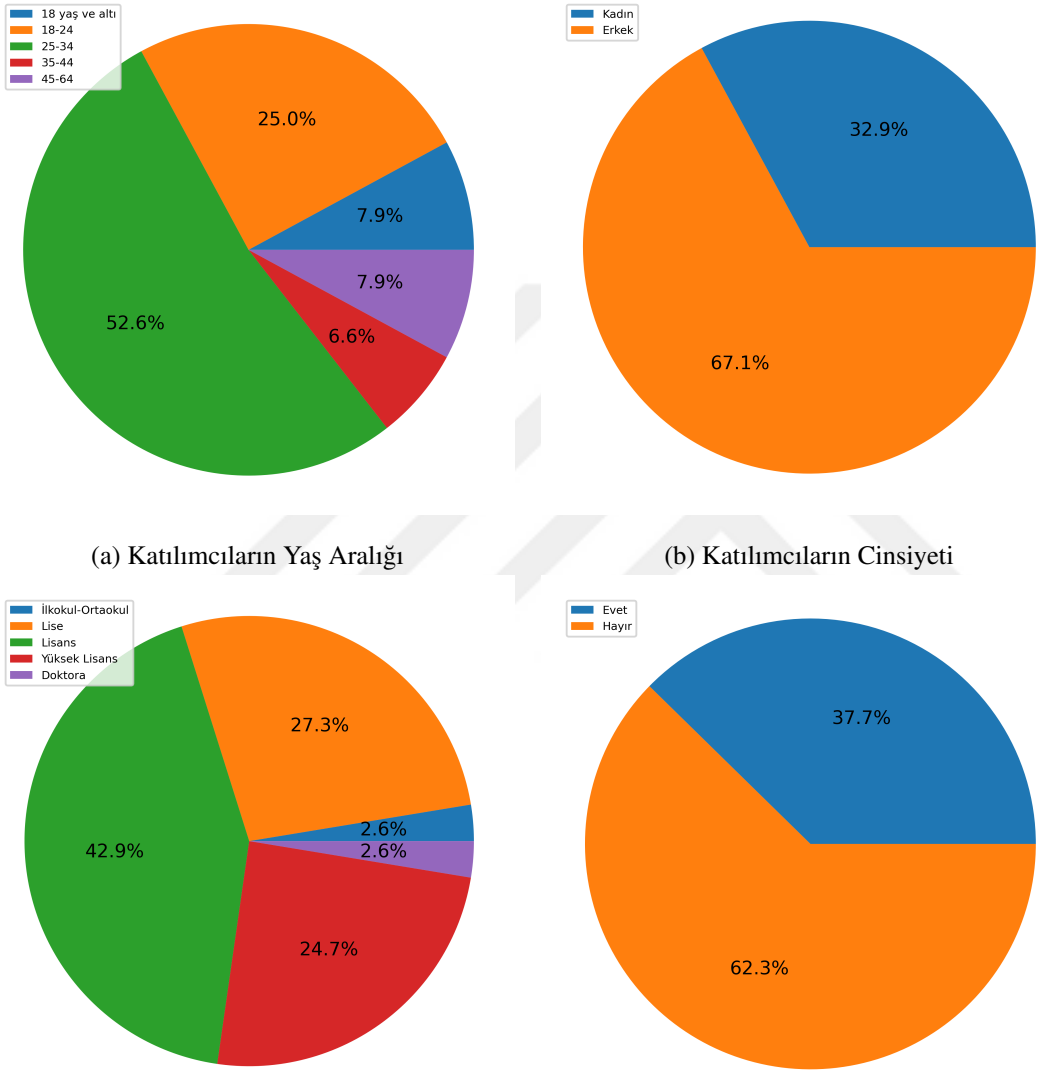
OAuth. Çeşitli API'lere veya servislere erişmek için, Android uygulamalar OAuth 2.0 kullanırlar. Servislerde ve API'lerde kimlik doğrulamak için, uygulama geliştiriciler client_id ve client_secret değerlerini kullanırlar. Bundan dolayı, bu değerler özellikle client_secret değeri korunmalıdır. Bu değerleri korumak için, geliştiriciler The Proof Key for Code Exchange (PKCE) yöntemi ile bir gizli değer oluşturur ve bu değeri erişim jetonu (*token*) elde etmede kullanılan yetkilendirme kodunu değiştirirken kullanır [91]. Tez çalışması kapsamında, bazı uygulamaların Google, Outlook, Office 365, Yahoo, Microsoft ve mail.ru gibi servislere ait OAuth değerlerini açık metin olarak depoladıkları tespit edilmiştir. Saldırganlar bu değerleri çalabilir ve bunları kullanarak listelenen API ve servislere erişim sağlayabilir. Bu durum veri sızıntısına ve servislere yetkisiz erişime neden olabilir.

4. KULLANICI ANKETİ

Android uygulamayı [19] kullanarak veri seti oluştururken, kullanıcıların ön yüklü uygulamalar hakkındaki endişelerini ve bilgi seviyelerini ölçmek amacıyla bazı sorular sorulmuştur. Anket soruları *EKLER* kısmında görülebilir.

Başlangıç olarak, tüm cevapları varsayılan cevaplarla aynı olan ve aynı e-posta adresine sahip olan cevapları elimine edildikten sonra, kullanıcı anketine toplam 77 kişi katılım sağlamıştır. Anketin başında kullanıcı profillerini çıkarmak için katılımcılara bazı sorular sorulmuştur. Sonuç olarak, katılımcıların 40 tanesinin 25-34 yaş aralığında, 19 tanesinin ise 18-24 yaş aralığında oldukları görülmüştür. Soruları cevaplayan 76 kişiden 26'sının cinsiyeti kadındır ve bir kişi ise cinsiyet bilgisini sağlamak istememiştir. Bunun yanında, katılımcıların eğitim seviyesi çoğunlukla lisans seviyesindedir. Sürpriz bir şekilde, katılımcılardan sadece 29 tanesi siber/mobil güvenlik ile ilgilenmektedir. Şekil 4.1'de kullanıcıların profili yaş, cinsiyet, eğitim seviyesi ve siber/mobil güvenlik ilgisi açılarından gösterilmiştir.

İkinci olarak, cihaz alırken kullanıcı davranışları ve düşünce yapısının anlaşılması amaçlanmıştır. Bunun amaçla sorulan soruya, 17 kişi herhangi bir cevap vermezken, kalan 60 kişiden 51'ini akıllı telefonlarını çevrim içi marketler, teknoloji mağazaları veya mobil şebeke operatörlerinden aldıklarını belirtmiştir. Bu kullanıcıların telefon alırken genellikle büyük satıcılara güvendiklerini göstermektedir. Bu durumun kullanıcı mahremiyeti ve güvenliği açısında iyi sonuçları olabilir. Örneğin, The Verge'de bahsedildiği şekilde [92], Amazon ön yüklü bir zararlı yazılımla gelen Blu telefonların kendi platformu üzerinden satışını kısıtlamıştır. Ayrıca, katılımcıların sadece %10'u 700 TL ve altında telefonlar kullanmaktadır. Ek olarak, 44 kişi 1001-2500 TL arasında telefonlar kullanırken, 27 tanesi 2501-5000 TL arası telefonlar kullanmaktadır. Bu durum ucuz telefonların pahalı telefonlara göre kullanıcı mahremiyetini ve güvenliğini daha fazla tehdit ettiği için [93] önemlidir. Ardından, kullanıcıların telefonlarını ne kadar süredir kullandıklarını ve ne sıklıkla değiştirdikleri tespit edilmeye çalışılmıştır. Buna göre kullanıcıları yaklaşık olarak yarısı (%40) cihazlarını 2 ile 5 yıl arası bir süreçte kullanmaktadır. Daha da kötüsü bazı kullanıcılar 5 yıldır aynı telefonları kullanmaktadır. Birçok üretici ortalama olarak 2 yıl süresince güvenlik güncellemelerini desteklediklerini için [94], bu durum kullanıcıları potansiyel güvenlik açıklıklarına karşı tehlikede bırakmaktadır. Bunun yanında kullanıcılara cihazlarında kaç yılda bir değiştirdikleri sorulmuştur, çünkü bazı kullanıcılar cihazlarını yeni almış olabilecekleri için, bir önceki soruda çıkarılan değişim periyodu hatalı olabilir. Sonuç olarak, neredeyse tüm kullanıcıların (77 kişiden 68'i) cihazlarının 2 yıldan fazla sürede değiştirdiği sonucuna ulaşılmıştır. Yukarıda da bahsedildiği gibi, üreticiler sadece 2 yıl süresince güvenlik güncellemelerini desteklediklerini için, bu durum Android ekosisteminde büyük bir sorun olarak yer almaktadır. Kullanıcı akıllı telefonlarının güncelliği ile ilgili tam anket sonuçları Şekil 4.3'te görülebilir. Daha sonra, telefon alırken kullanıcıların dikkat ettiği kriterleri öğrenmek için, ankete çoklu seçimli bir soru eklenmiştir. Beklendiği gibi, çoğu insan için akıllı telefonun fiyatı ve modeli önemli kriterler arasındadır. Ancak, sadece 14 kişi üreticilerin gizlilik ve güvenlik politikalarını önemsemektedir. Bunun yanında 13 kişi üreticinin ülkesine dikkat etmektedir. Buna göre kullanıcılar politikalar hakkında daha fazla bilgilendirilmeli ve üreticinin ülkesinin kullanıcı mahremiyetine etkisinin farkında olmalıdır.



(a) Katılımcıların Yaş Aralığı

(b) Katılımcıların Cinsiyeti

(c) Katılımcıların Eğitim Seviyesi

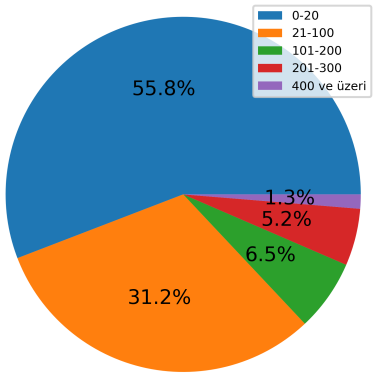
(d) Katılımcıların Siber/Mobil Güvenlik İlgisi

Şekil 4.1: Anket Katılımcılarının Profili.

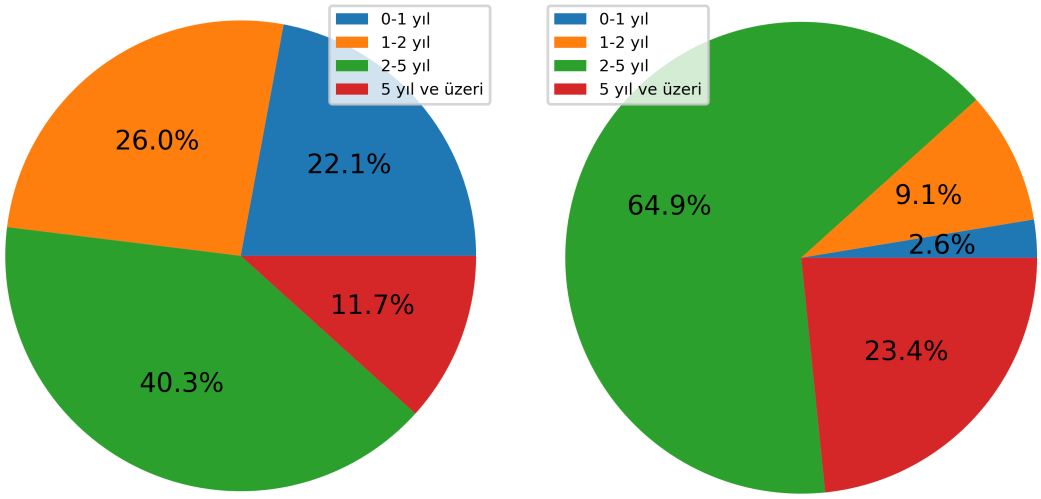
Üçüncü olarak, kullanıcıların ön yüklü uygulamalar ve onların davranışları hakkındaki bilgi seviyelerinin ölçülmesi amaçlanmıştır. Başlangıç olarak, kullanıcıların cihazlarda bulunan ön yüklü uygulama sayısındaki bilgisinin gerçekten çok uzak olduğu görülmüştür. Şekil 4.2'de kullanıcıların ön yüklü uygulamaların sayısı hakkındaki tahminleri görülebilir. Bu şekilde birçok kullanıcının ön yüklü uygulama sayısını, gerçek rakamlardan daha az olduğunu düşünmektedir. Örneğin, katılımcıların yarıdan fazlası (%55.8) cihazlarında sadece 0-20 arasında ön yüklü uygulama olduğunu düşünmektedir. Ancak, cihazlarda bulunan ortalama ön yüklü uygulama sayısı 294 olup, kullanıcıların tahminlerine göre çok daha fazladır. Bunun yanında, kullanıcıların ön yüklü uygulamaların davranışları hakkında bilgilendirilip bilgilendirilmedikleri anlaşılmaya çalışılmıştır. Katılımcıların 31 tanesinin cihazlarını ilk defa çalıştırırken bu konuya dikkat etmedikleri görülmektedir. Ek olarak, katılımcıların 27 tanesi, ön yüklü uygulamaların aksiyonları hakkında bilgilendirilmediklerini düşünmektedir. Ayrıca, katılımcıların %40'ı bu konuya dikkat etmemekte ve 30 tanesi de ön yüklü uygulamaların davranışları hakkında izinlerinin alınmadığını düşünmektedir. Bundan dolayı, geliştiriciler ve üreticiler kullanıcı izinleri konusunda daha dikkatli ve kullanıcıların onayının alırken daha bilgilendirici olmalıdır.

Ardından, kullanıcıların Android izinlerini yönetirken davranışlarını öğrenmek için, onlara 2 farklı soru sorulmuştur. Bunun sonucunda, katılımcıların yarısı (77'de 38) uygulamaları yüklemeden önce uygulama izinlerini kontrol etmektedir. Ayrıca, katılımcıların %71'i hangi uygulamanın hangi izinleri kullandığını düzenli olarak kontrol etmemektedir. Bu yüzden, önemli miktarda insanın uygulamaları yüklerken önemli miktarda insan izinleri kontrol etmektedir. Ancak, ön yüklü uygulamalar cihazın kutudan çıktığı haliyle ön yüklü geldikleri için, yukarıdaki bahsedildiği şekilde uygulama izinlerini düzenli olarak kontrol etmeyen kişiler, ön yüklü uygulamaların kullandığı izinler hakkında fikir sahibi değildir.

Daha sonra, kullanıcıların güncelleme mevcut olduğunda uygulayıp uygulamadıklarının anlaşılması amaçlanmıştır. Buna göre, katılımcıların çoğunluğu (%81) cihazlarındaki uygulamaların güncel olmasına dikkat etmektedir. Fakat, *Ekosistem* bölümünde bahsedilen ve tez çalışması kapsamında yapılan üst veri analizine göre, ön yüklü uygulamaların yarısından fazlası cihazla ilk yüklü geldiklerinden beri güncellenmemiştir.



Şekil 4.2: Telefonunuzu ilk aldığınızda kaç tane ön yüklü (cihaz kutudan çıktığında yüklü olarak cihazda bulunan) uygulama olduğunu düşünüyorsunuz?



(a) Ne kadar süredir bu akıllı telefonu kullanıyorsunuz?

(b) Ne sıklıkla akıllı telefonunuzu değiştiriyorsunuz?

Şekil 4.3: Telefonların Güncelliği Hakkındaki Anket Sonuçları.

Dahası, Android akıllı telefonlar sadece 2 yıl boyunca güvenlik güncellemeleri almaktadır. Bu iki durum kullanıcıları potansiyel güvenlik açıklıklarına karşı açıkta bırakmaktadır.

Son olarak, katılımcıların GDPR [51] veya KVKK [95] gibi düzenlemeleri duyup duymadıklarını ölçülmeye çalışılmıştır. Maalesef, katılımcıların yarısından fazlasının, bu düzenlemeleri duymadığı görülmüştür. İzleyiciler kısmında belirtildiği gibi, bu regülasyonlar kullanıcı mahremiyeti açısından önemli bir role sahiptir. Bundan dolayı, insanlar bu düzenlemeler, bunların önemi ve kullanıcı mahremiyetine etkisi hakkında bilgilendirilmelidir.

Anket çalışmasının sonunda, analiz sonuçlarını göndermek amacıyla kullanıcıların e-posta adreslerini toplanmıştır. Çünkü yapılan çalışmaya göre, kullanıcıların ön yüklü uygulamaların kullanıcı mahremiyetine ve güvenliğine etkisi hakkında bilgilendirilmesi gerekmektedir.

5. WEB SİTESİ VE SKORLAMA

Kullanıcı anketi sonucunda, kullanıcıların Android cihazlardaki ön yüklü uygulamalar ve bu uygulamaların kullanıcı mahremiyeti ve güvenliğine etkileri konusunda yeterli seviyede bilgi sahibi olmadıkları görülmüştür. Bu sebepten dolayı hem kullanıcıları bilgilendirmek ve bilinçlendirmek, hem de daha fazla araştırmacının dikkatini çekmek amacıyla bir web sitesi oluşturulmuştur. Bu sitede yapılan analiz sonuçları kullanıcıların ve araştırmacıların anlayabileceği şekilde düzenlenmiştir. Bunun yanında, yapılan analiz sonuçları kullanılarak her cihaza bir skor verilmiştir. Bu skor ile kullanıcıların, cihazların mahremiyete ve güvenliğe etkileri konusunda daha kolay bir şekilde fikir edinmeleri amaçlanmıştır. Aşağıdaki oluşturulan web sitesi ve skorlama sistemi hakkında detaylar açıklanmıştır.

5.1 Web Sitesi

Yukarıda da belirtildiği üzere, web sitesinde yapılan analiz sonuçları düzenlenerek kullanıcıların ve araştırmacıların erişimine sunulmuştur. Yapılan analiz sonuçlarına [96] üzerinden erişim sağlanabilir. Bu sayfada, cihazlar üreticilerine göre gruplanmıştır. Kullanıcı istediği üreticiye ait cihazları görüntüleyerek, bu gruptaki herhangi bir cihaz için yapılan analiz sonuçlarını listeleyebilir. Cihaz seçildikten sonra sonuçlar kullanıcıya 4 ana bölümde gösterilmektedir. Bu bölümler; Cihaz Detayları (*Device Details*), Ön Yüklü Uygulamalar (*Pre-installed Applications*), Uygulama Detayları (*Application Details*) ve İlginç Sonuçlar (*Interesting Results*) şeklindedir.

5.1.1 Cihaz Detayları

Bu kısımda cihaz hakkında cihaz üreticisi, cihaz modeli, cihaz ürün kodu, cihaz versiyonu bilgileri listelenmiştir.

5.1.2 Ön Yüklü Uygulamalar

Bu kısımda cihazda bulunan ön yüklü uygulamaların paket isimleri ve ön yüklü uygulama sayısı görüntülenebilir.

5.1.3 Uygulama Detayları

Bu bölümde cihazda bulunan uygulamalar üzerinden yapılan analiz sonuçları listelenmiştir. Bu bölümde sonuçlar 7 gruba bölünmüştür: Uygulama Üst Verisi, Manifest Özellikleri, Uygulama İzinleri, Dışarıya Açık (*exported*) Uygulama Bileşenleri, 3. Parti Kütüphaneler, İzleyici SDK'lar ve Bulut Servisleri.

Uygulama Üst Verisi. Bu bölümde uygulama hakkında çeşitli uygulama üst veri bilgileri listelenmiştir. Bu bilgiler uygulamaların statik analizi ve cihaz üzerinden toplanarak elde edilmiştir. Bu kapsamda, uygulamayanın ilk yüklenme zamanı, son güncel-

lenme zamanı, APK dosyasının MD5 hash bilgisi, paket adı, versiyon kodu, versiyon adı, hedef SDK versiyonu, minimum SDK versiyonu, sertifika bilgileri ve sertifika üzerinden yapılan analiz sonucu elde edilen sertifika tanımlayıcı bilgileri görülebilir.

Manifest Özellikleri. Bu kısımda uygulamanın manifest dosyalarındaki bazı hassas özelliklerin analizi sonucunda elde edilen veriler yer almaktadır. Bu kapsamda, eğer varsa uygulamanın *sharedUserId* değeri ile *allowBackup*, *debuggable* ve *usesClearTextTraffic* özelliklerinin aktif olup olmadıkları listelenmiştir.

Uygulama İzinleri. Bu kısımda uygulama izinleri, tüm uygulama izinleri, 3. parti uygulama izinleri ve sonradan tanımlanan uygulama izinleri olarak 3 grupta listelenmiştir. Tüm uygulama izinleri bölümünde, ilgili izne ait eğer mevcut ise, iznin ne işe yaradığına dair açıklama, iznin amacına dair etiket bilgisi, izin grubu ve izin koruma seviyesi bilgileri yer almaktadır. 3. parti uygulama izinleri bölümünde, uygulama marketlerindeki uygulamalar tarafından kullanılamayan ancak üreticiler tarafından kullanılan izinler yer almaktadır. Sonradan tanımlanan uygulama izinleri bölümünde ise, uygulama tarafından sonradan tanımlanan izinler listelenmiştir. Bu izinler "Özel Tanımlanmış İzinleri" ile aynı kapsamdadır. Bundan dolayı, bu izinlerin ortak kullanımı önceki bölümlerde de bahsedildiği gibi, üreticiler ile 3. partiler arasındaki iş birliklerinin ortaya çıkarılması açısından önemlidir.

Dışarıya Açık Uygulama Bileşenleri. Bu bölümde uygulamanın dışarıya açık olan bileşenleri listelenmiştir. Bu bileşenler *Activities, Services, Content Providers, Broadcast Receivers* olarak ayrı ayrı gösterilmiştir. Ayrıca eğer ilgili bileşene erişmek için gerekli izinler de bu bölümden görülebilir. Uygulama bileşenleri özellikle diğer uygulamalar tarafından erişilebilir oldukları için, uygulamalar üzerindeki atak yüzeyini artırmaktadır. Bununla birlikte, bu bileşenler bazı kritik fonksiyonellik sağladıkları ve hassas verilere eriştiklerinden dolayı, kullanıcı mahremiyeti ve güvenliği açısından da büyük öneme sahiptir.

3. Parti Kütüphaneler. Bu kısımda uygulamalar tarafından kullanılan 3. parti kütüphaneler, bu alandaki en gelişmiş araçlardan biri (*state of art*) olan LibRadar [97] aracı kullanılarak çıkarılmış ve listelenmiştir. Bilindiği üzere, 3. parti kütüphanelerin kullanımı uygulama geliştiricilere büyük kolaylıklar sağlamaktadır. Bundan dolayı da yaygın olarak kullanılmaktadır. Ancak bazı 3. parti kütüphaneler haberli veya habersiz olarak, kullanılan uygulamanın sahip olduğu izinler çerçevesinde kullanıcı bilgilerine erişmekte ve bu bilgileri toplamaktadır. Ayrıca, uygulama tarafından kullanılan 3. parti kütüphanede bulunan bir zafiyet uygulamanın ve uygulama üzerinden kullanıcı verilerinin güvenliğini de tehlikeye atmaktadır. Bu sebeplerden dolayı, uygulamalar tarafından kullanılan 3. parti kütüphanelerin bilinmesi ve kontrol edilmesi kullanıcı mahremiyeti ve güvenliği açısından önemlidir.

İzleyici SDK'lar. Bu bölümde uygulama tarafından kullanılan izleyici SDK'lar yer almaktadır. Bu kapsamda her izleyiciye ait izleyici adı, izleyicinin çalışma amacına göre bulunduğu gruplar ve izleyicinin sahip olduğu izinler listelenmiştir. İzleyici SDK'ların kullanıcı mahremiyeti açısından önemi önceki bölümlerde açıklanmıştır.

Bulut Servisleri. Bu bölümde uygulama tarafından kullanılan bulut servilerindeki zafiyetler listelenmiştir. Daha önce açıklandığı üzere, günümüzde bulut servisleri uygulamalar tarafından yaygın bir şekilde kullanılmaktadır. Bu kapsamda, zafiyetli bulut

servisinin adı ve zafiyet hakkında bilgileri yer almaktadır.

5.1.4 İlginç Sonuçlar

Bu bölümde analiz sonuçlarının birleştirilmesiyle elde edilen bazı ilginç sonuçları listelenmektedir.

Uygulama Sertifika Tanımlayıcıları. Bu kısımda cihazda bulunan uygulamalar sertifika tanımlayıcılara göre gruplanmıştır. Böylece cihazda bulunan üreticilere ait uygulamaların yanında, 3. parti firmalara ait uygulamaların listesi de görüntülenebilir.

Aynı sharedUserId Değerine Sahip Uygulamalar. Bu kısımda uygulamalar sharedUserId değerlerine göre gruplanmıştır. Bu şekilde, hangi uygulamaların aynı UID değerine sahip olduğu ve birbirlerinin verilerine erişebildikleri tespit görülebilir. Bunun yanında, Android sistemlerdeki en yetkili kullanıcılarda birisi olan sistem kullanıcısı hakları ile çalışan uygulamalar listelenebilir.

Aynı 3. Parti İzni Kullanan Uygulamalar. Bu kısımda uygulamalar, ortak olarak tanımladıkları sonradan tanımlanmış izinlere (*custom permissions*) gruplanmıştır. Bu veri yardımı ile özellikle üretici firmalar ile 3. parti firmalar olmak üzere aynı izni kullanan farklı firmalar tespit edilebilir. Bu şekilde uygulamalar dolayısıyla firmalar arasındaki iş birlikleri bulunabilir.

Ön Yüklü Uygulamalar. Bu kısımda daha önce listelenen ön yüklü uygulama sonuçlarından sadece yüksek öneme sahip olanlar seçilerek listelenmiştir. Örneğin, manifest özellikleri kısmı için, önceki bölümde tüm sonuçlar listelenirken bu bölümde sadece aktif olan özellikler listelenmiştir.

5.2 Skorlama

Uygulamalar üzerinden yapılan analizler sonucu, kullanıcı mahremiyeti ve güvenliği açısından birçok önemli çıktı elde edilmiştir. Ancak bu sonuçların özellikle normal kullanıcılar tarafından anlaşılması çok mümkün değildir. Bu sebepten dolayı elde edilen sonuçlar çeşitli kriterlere göre değerlendirilerek ilkel bir skorlama sistemi oluşturulmuştur. Bu sistem oluşturulurken, bulgunun uygulanabilirliği, kullanıcı güvenliği ve mahremiyetine etki düzeyi ve kullanıcının bulgu hakkındaki farkındalığı göz önünde bulundurulmuştur. Ayrıca skor hesaplanırken 50 ve üzeri sayıda ön yüklü uygulama barındıran cihazlar dikkate alınmıştır. Bunun ana sebepleri, uygulama toplama aşamasında bazı cihazlardan tüm uygulamaların toplanamaması ve bundan dolayı az uygulama toplanan cihazlar için hesaplanan skorların kapsayıcılıktan uzak olmasıdır. Bulgular 3 farklı kritere göre değerlendirilmiştir. Bunlar yukarıda da bahsedildiği gibi, bulgunun istismar edilme zorluğu, kullanıcı mahremiyeti ve güvenliği üzerindeki etkisi ve kullanıcının bulgu hakkındaki farkındalığıdır. Bu kriterlerin tamamı bulgulara göre düşük, orta yüksek ve kritik olarak değerlendirilmiştir. Buna göre bulgular sırasıyla 0.1, 0.15, 0.25 ve 1.0 katsayıları ile çarpılmıştır.

Bulgunun uygulanabilirliği. Skorlama kapsamında kullanılan bulguların her birinin uygulanması eşit zorlukta değildir. Bundan dolayı skorlama yapılırken bulguların uy-

gulanabilirliği ve ne kadar kolay istismar edilebileceği de dikkate alınmalıdır. Bu kapsamda, bulgular bu açıdan değerlendirilmiş ve uygulanabilirlik yönünden düşük, orta, yüksek ve kritik olarak sınıflandırılmıştır. Buna göre uygulanması çok zor olan bulgular 0.1, zor olan bulgular 0.15, orta seviyede olan bulgular 0.25 ve kolay olan bulgular 1.0 katsayıları ile çarpılmıştır.

Bulgunun etkisi. Her bulgunun kullanıcı mahremiyeti ve güvenliğine etkisi farklılık göstermektedir. Bundan dolayı, bulgular analiz edilerek etki seviyelerine göre çok yüksek, yüksek, orta ve düşük etkili olarak değerlendirilmiştir. Böylece bulgular etki seviyelerine sırasıyla 1.0, 0.25, 0.15 ve 0.1 katsayıları ile çarpılmıştır.

Kullanıcının farkındalığı. Kullanıcıların bulguların etkileri ve istismar edilmeleri gibi konuların farkında olmaları, bulguların engellenmesi ve kullanıcıların bilinçlenmesi açısından önemlidir. Bundan dolayı, skorlama aşamasında bulgular kullanıcıların ne seviyede farkında olabileceğine göre değerlendirilmiştir. Bu kapsamda, kullanıcı farkındalığı ihtimalinin düşük olduğu bulgular 1.0, orta seviye olduğu bulgular 0.25, yüksek olduğu bulgular 0.15 ve çok yüksek olduğu bulgular 0.1 katsayıları ile çarpılmıştır.

Bulgular yukarıdaki kriterlere göre değerlendirilerek, elde edilen tekil skorlar katsayılarla çarpılmıştır. Bunun yanında elde edilen sonuçlar çok küçük değerler oldukları için, bunları daha anlaşılabilir hale getirmek amacıyla değerler 100 ile çarpılmıştır. Bu işlemin skorlara bir etkisi bulunmamaktadır. Bunun sonucunda elde edilen skorlar toplanarak nihai bir cihaz skoru elde edilmiştir.

5.2.1 Düşük Dereceli Bulgular

Cihaz üzerinden bulunan sistem uygulaması sayısı. Android sistemlerde sistem kullanıcısı en yetkili kullanıcılardan birisidir ve üreticiler tarafından gerekli olduğu durumlarda uygulamalar bu kullanıcı ile çalışmaktadır. Yapılan analiz sonunda sharedUserId değeri "*android.uid.system*" olan uygulama sayısının, tüm ön yüklü uygulama sayısına oranı çıkarılmıştır. Bu değer mahremiyet ve güvenlik açısından direkt bir gösterge olmasa bile bu uygulamaların çok sayıda olmasından dolayı, bunlarda bulunan olası bir zafiyet sonucunda cihazın ve cihazda bulunan verilerin güvenliği tehlikeye girebilir. Sistem uygulamalarında zafiyet bulmanın ve bu zafiyeti sömürmenin zorluklarından dolayı, bulgunun uygulanabilirliği açısından çok zor olarak değerlendirilmiştir. Ek olarak, bulgunun etkisi orta seviye ve kullanıcı farkındalığı konularında çok yüksek seviye şeklinde değerlendirme yapılmıştır.

Bu işlem denklem 5.1'de görülebilir.

a=Cihaz üzerinde bulunan sistem uygulaması sayısı,

b=Cihaz üzerinde bulunan uygulama sayısı

$$skor = (a/b) * 0.1 * 0.15 * 0.1 * 100 \tag{5.1}$$

5.2.2 Orta Dereceli Bulgular

İzne gerek olmadan dışarıya açık bileşenler. Android uygulamalarda herhangi bir izne tabi olmadan dışarıdan erişilebilen uygulama bileşenleri uygulamaların atak yüzeyini artırmaktadır. Bu bileşenler kullanılarak zararlı uygulamalar yetkisiz işlemler gerçekleştirebilir veya cihaz üzerindeki kullanıcı verilerine yetkisiz olarak erişebilir. Ayrıca bazı üretici ve 3. parti firmaların sahip olduğu ön yüklü uygulamalar yetki gerektiren işlemleri dışarı açarak, 3. parti uygulamaların yetkili işlemleri gerçekleştirmesi için olanak sağlayabilir. Bu sebeplerden dolayı, bu kısımdaki bulgular orta dereceli olarak değerlendirilmiştir. Skorlama hesaplanırken, dışa açık ve izin gerektirmeyen bileşenlerin cihaz üzerindeki uygulamalara oranı çıkarılmıştır. Bu kapsamdaki bulgular uygulanabilirlik açısından çok zor, kullanıcı mahremiyeti ve gizliliğine etkileri bakımından orta seviye ve kullanıcı farkındalığı bakımından orta seviye olarak değerlendirilmiştir. Bu işlem denklem 5.2'de görülebilir.

a=İzne gerek olmadan dışarıya açık bileşenlerin sayısı,

b=Cihaz üzerinde bulunan uygulama sayısı

$$skor = (a/b) * 0.1 * 0.15 * 0.25 * 100 \tag{5.2}$$

allowBackup özelliği aktif olan uygulamalar. Bu özelliğin aktif olduğu uygulamaların verileri cihaza fiziksel erişimi olan bir kişi tarafından yedeklenerek erişilebilir. Bu bilgilerin erişimi durumunda, uygulama kum havuzunda bulunan kullanıcı mahremiyetini yüksek oranda etkileyebilecek verilere erişim sağlanabilir. Güncel işletim sistemlerinde (Android 6.0 ve sonrası) adb hata ayıklama modu, varsayılan olarak kapalı olduğu ve bu saldırının gerçekleşmesi için cihaza fiziksel erişim ihtiyacı olduğu için, bu kategorideki bulgular orta dereceli olarak puanlanmıştır. Skorlama hesaplanırken cihaz üzerinde allowBackup özelliği açık olan uygulamaların tüm uygulamalara oranı alınmıştır. Bu kapsamdaki bulgular uygulanabilirlik açısından çok zor, kullanıcı mahremiyeti ve gizliliğine etkileri bakımından yüksek seviye ve kullanıcı farkındalığı bakımından yüksek seviye olarak değerlendirilmiştir. Bu işlem Denklem 5.3'te görülebilir.

a=allowBackup özelliği aktif uygulama sayısı,

b=Cihaz üzerinde bulunan uygulama sayısı

$$skor = (a/b) * 0.1 * 0.25 * 0.15 * 100 \tag{5.3}$$

Üretici tarafından imzalanmayan uygulama sayısı. Daha önceki kısımlarda bahsedildiği gibi, uygulamaları imzalamada kullanılan sertifikalar incelenerek uygulama geliştiricileri tespit edilmeye çalışılmıştır. Bu analiz sonucunda, cihazlarda hem üreticiler hem de 3. partiler tarafından geliştirilen uygulamalar tespit edilmiştir. Üreticiler tarafından geliştirilen uygulamalar çoğunlukla cihazın çalışması için gereklidir. Ancak 3. partiler tarafından geliştirilen uygulamalar olmasa bile cihazın çalışması etkilenmeyecektir. Ayrıca birçok 3. parti uygulama çeşitli izleyici servislerine sahiptir. Yine 3. parti uygulamaların ön yüklü olarak gelmesi, uygulama marketlerinden yüklenmesine göre çeşitli fazla yetkilere ve izinlere sahip olmasına neden olabilir. Bu gibi nedenlerden dolayı, bu kapsamda yapılan analiz sonuçları orta dereceli olarak ele alınmıştır.

Skorlama yapılırken, üreticilere ait olmayan uygulamaların tüm uygulamalara oranı alınmıştır. Bu kapsamdaki bulgular uygulanabilirlik açısından orta seviye, kullanıcı mahremiyeti ve gizliliğine etkileri bakımından orta seviye ve kullanıcı farkındalığı bakımından orta seviye olarak değerlendirilmiştir. Bu işlem Denklem 5.4'te görülebilir.

a=Üretici tarafından imzalanmayan uygulama sayısı,

b=Cihaz üzerinde bulunan uygulama sayısı

$$skor = (a/b) * 0.25 * 0.15 * 0.25 * 100 \tag{5.4}$$

2 yıldan uzun süredir güncellenmeyen uygulama sayısı. Üreticiler Android cihazlara ortalama olarak 2 yıl boyunca güvenlik güncellemesi desteği vermektedir. Bu durum güncellenmeyen cihazları potansiyel zafiyetlere karşı tehdit altında bırakmaktadır. Bundan dolayı, bu kapsamdaki bulgular orta dereceli olarak değerlendirilmiştir. Bu analiz için kullanılan veriler, uygulama toplama aşamasında cihazdan toplanmıştır. Analiz kapsamında ise, cihazda bulunan ve 2 ve daha uzun yıldır güncellenmeyen uygulamaların sayısının cihazda bulunan tüm uygulamalara oranı alınmıştır. Bu kapsamdaki bulgular uygulanabilirlik açısından zor seviyede, kullanıcı mahremiyeti ve gizliliğine etkileri bakımından orta seviye ve kullanıcı farkındalığı bakımından orta seviye olarak değerlendirilmiştir. Burada kullanılan işlem denklem 5.5'te görülebilir.

a=2 yıldan uzun süredir güncellenmeyen uygulama sayısı,

b=Cihaz üzerinde bulunan uygulama sayısı

$$skor = (a/b) * 0.15 * 0.15 * 0.25 * 100 \tag{5.5}$$

5.2.3 Yüksek Dereceli Bulgular

Tehlikeli izin sayısı. Android sistemlerde tehlikeli izinler, kullanıcı mahremiyetini ve güvenliğini etkileyebilecek aktiviteleri yönetmek ve kısıtlamak için kullanılmaktadır. Bundan dolayı bu izinlerin kullanımı çalışma zamanında kullanıcının onayına bırakılmıştır (Android 6.0 ve sonrasında). Ancak ön yüklü uygulamalar çeşitli istisnalar yardımı ile bazı durumlarda bu izinleri kullanıcıların haberi olmadan ve onayını almadan kullanmaktadır. Bu durum hassas verilerin güvenliğini ve kullanıcı mahremiyetini tehlikeye atmaktadır. Bu kapsamdaki bulgular uygulanabilirlik açısından orta seviyede, kullanıcı mahremiyeti ve gizliliğine etkileri bakımından orta seviye ve kullanıcı farkındalığı bakımından orta seviye olarak değerlendirilmiştir. Burada kullanılan işlem denklem 5.6'da görülebilir.

a=Tehlikeli izin sayısı,

b=Cihaz üzerinde bulunan uygulama sayısı

$$skor = (a/b) * 0.25 * 0.15 * 0.25 * 100 \tag{5.6}$$

usesClearTextTraffic özelliği aktif olan uygulamalar. Günümüzde SSL/TLS protokolleri bir standart haline gelerek şifreli iletişimde yaygın bir şekilde kullanılmaktadır.

Android uygulamalarda API 27 ve sonrasında usesClearTextTraffic özelliği varsayılan olarak "true" olarak gelmektedir. Daha önceki versiyonlarda ise bu özellik "false" olarak gelmektedir. Bu özelliğin *true* olması durumunda, uygulamanın şifresiz olarak ağ bağlantısı yapmasına izin vermektedir. Bu durum ortadaki adam saldırısı gibi saldırılara karşı uygulama trafiğini tehlikeye atmaktadır. Bu kapsamdaki bulgular uygulanabilirlik açısından orta seviyede, kullanıcı mahremiyeti ve gizliliğine etkileri bakımından yüksek seviye ve kullanıcı farkındalığı bakımından orta seviye olarak değerlendirilmiştir. Analiz için kullanılan işlem denklem 5.7'de görülebilir.

a=usesClearTextTraffic özelliği aktif olan uygulama sayısı,

b=Cihaz üzerinde bulunan uygulama sayısı

$$skor = (a/b) * 0.25 * 0.25 * 1.0 * 100 \tag{5.7}$$

debuggable özelliği aktif olan uygulamalar. Bu özellik uygulama geliştiriciler tarafından geliştirme aşamasında genellikle hataları tespit etmek amacıyla kullanılmaktadır. Ancak bu özelliğin üretim ortamındaki uygulamalarda kullanılması en iyi uygulamalar kapsamında tavsiye edilmemekte ve resmi Android uygulama marketlerine yüklenmesi engellenmektedir. Ayrıca bu özellik ile uygulama sınıflarına ve metotlarına erişilebilmekte ve uygulamanın davranışı değiştirilebilmektedir. Bu kapsamdaki bulgular uygulanabilirlik açısından zor seviyede, kullanıcı mahremiyeti ve gizliliğine etkileri bakımından çok yüksek seviye ve kullanıcı farkındalığı bakımından yüksek seviye olarak değerlendirilmiştir. Bu işlem için kullanılan denklem 5.8'de görülebilir.

a=debuggable özelliği aktif olan uygulama sayısı,

b=Cihaz üzerinde bulunan uygulama sayısı

$$skor = (a/b) * 0.15 * 1.0 * 0.15 * 100 \tag{5.8}$$

5.2.4 Kritik Dereceli Bulgular

İzleyici SDK ve hata raporlama grubunda olmayan izleyici sayısı. Önceki bölümlerde detaylı bir şekilde açıklandığı üzere, izleyici SDK'ların ve bulundukları grupların kullanıcı mahremiyeti üzerindeki etkileri büyüktür. Ayrıca bu SDK'ların uygulamalarda gömülü olarak gelmeleri, kullanıcıların bu servislerden ve servislerin aktivitelerinden haberinin olmaması gibi konular, derecelendirme yapılırken göz önünde bulundurulmuştur. İzleyici gruplarının tespitinde hata raporlama grubundaki izleyici servisleri, kullanım amaçlarından dolayı sayıya dahil edilmemiştir. Bu kapsamdaki bulgular uygulanabilirlik açısından kolay seviyede, kullanıcı mahremiyeti ve gizliliğine etkileri bakımından çok yüksek seviye ve kullanıcı farkındalığı bakımından düşük seviye olarak değerlendirilmiştir. Bu kapsamdaki skorlama işlemi denklem 5.9'da görülebilir.

a=İzleyici SDK ve hata raporlama grubunda olmayan izleyici sayısı,

b=Cihaz üzerinde bulunan uygulama sayısı

$$skor = (a/b) * 1.0 * 1.0 * 1.0 * 100 \tag{5.9}$$

Bulut servislerindeki zafiyet sayısı. Bulut servisleri ve bu servislerin Android uygulamalar açısından öneminden, önceki bölümlerde bahsedilmiştir. Bu kapsamda çeşitli bulut servislerinde bulunan zafiyetler kullanıcı mahremiyetini ve güvenliğini farklı yönlerden etkilemektedir. Bu kapsamdaki bulgular uygulanabilirlik açısından kolay seviyede, kullanıcı mahremiyeti ve gizliliğine etkileri bakımından çok yüksek seviye ve kullanıcı farkındalığı bakımından düşük seviye olarak değerlendirilmiştir. Skorlama için kullanılan işlem denklem 5.10'da görülebilir.

a=Bulut servislerindeki zafiyet sayısı,

b=Cihaz üzerinde bulunan uygulama sayısı

$$skor = (a/b) * 1.0 * 1.0 * 1.0 * 100 \tag{5.10}$$

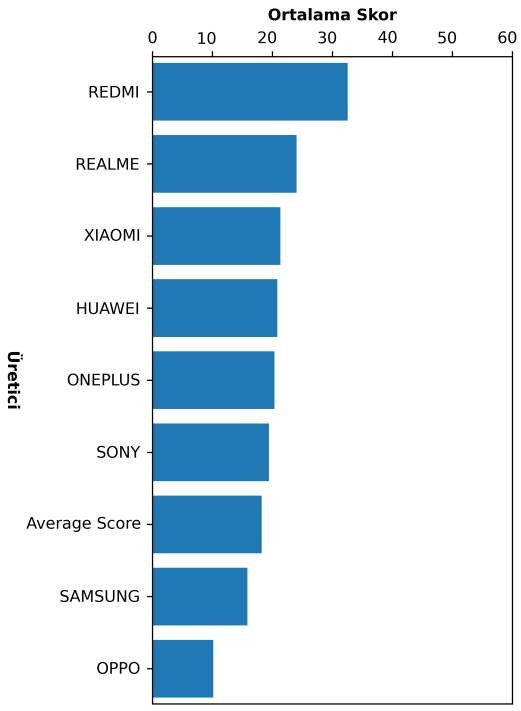
5.2.5 Kısıtlar ve Sonuçlar

Kısıtlar. Skorlama aşamasındaki kriterlerin ve değerlendirilen cihazların sayısının yetersizliğinden dolayı elde edilen sonuçlar cihazların kullanıcı mahremiyeti ve güvenliğini ne kadar tehdit ettiğini yeterli miktarda yansıtamamaktadır. Bundan dolayı veri kümesinin genişletilerek, daha gelişmiş bir skorlama sisteminin tasarlanması gerekmektedir. Bu işlem için kriterlerin nihai skora etkilerini belirlemede kullanılan katsayı değerleri ve tekil skorlar dinamik hale getirilebilir. Bu katsayılar gelecekte yapılacak analizler sonucunda belirlenecek çeşitli eşik değerlere göre tespit edilebilir. Ayrıca belirtmek gerekir ki, bulguların kritikliği bulgunun bulunduğu uygulamanın kritikliğine göre de çeşitlilik gösterebilir. Ancak bu konu üzerinde gelecekte daha detaylı bir çalışma yapılması gereklidir.

Ayrıca tekil skorlar hesaplanırken, bulguların sayısının cihazda bulunan uygulamaların sayısına oranı alınmıştır. Ancak bu durum sonucunda ön yüklü uygulama sayısı diğer cihazlara göre daha fazla olan cihazlarda hatalı sonuçlara yol açabilir. Örneğin aynı sayıda ve etkide zafiyetlere sahip iki farklı cihazdan fazla sayıda ön yüklü uygulamaya sahip olan cihazın skoru daha az çıkacaktır. Bundan dolayı yanlış algılara neden olmamak için hesaplanan skorların normalize edilmesi gereklidir. Bu işlem gelecekte yapılacak çalışmalara bırakılmıştır.

Sonuçlar. Yukarıda elde edilen tekil sonuçların toplanması sonucunda cihazlar için nihai skor değerleri elde edilmiştir. Uygulama toplama aşamasında, çeşitli sebeplerden dolayı bazı cihazlarda tüm uygulamalar toplanamadığı için, skor hesaplama aşamasında sadece 50 ve üzeri uygulamaya sahip cihazlar skorlamaya dahil edilmiştir. Yüksek skora sahip cihazlar, mahremiyet ve güvenlik açısından en tehlikeli cihazlardır.

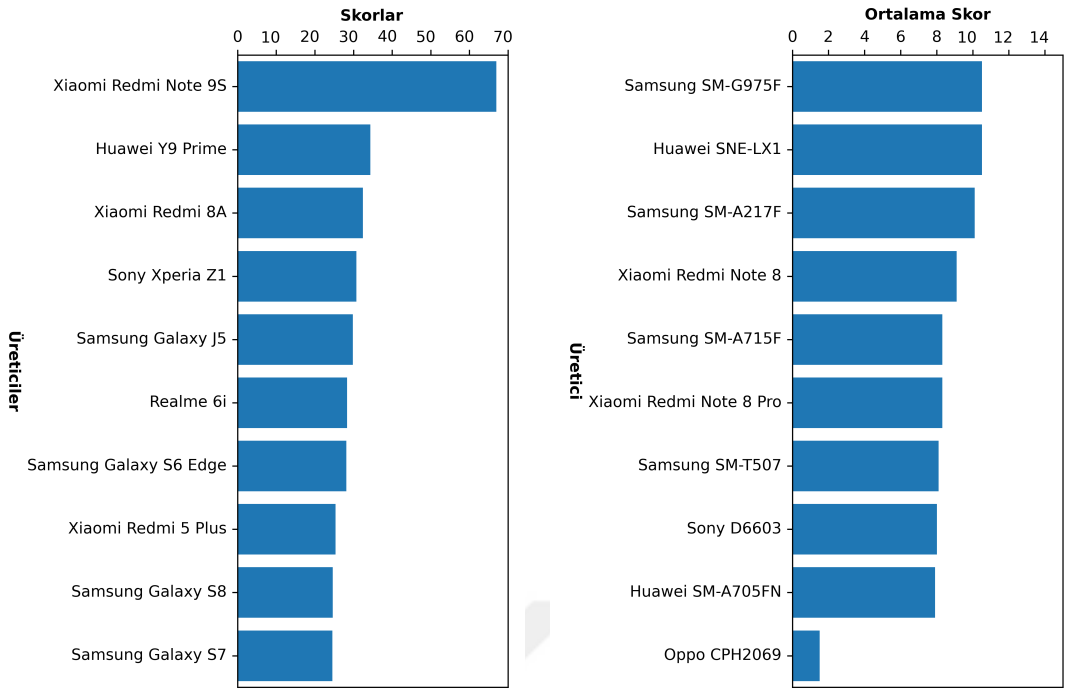
Cihaz skorları hesaplandıktan sonra ilk olarak, cihazlara göre üreticilerin ortalama skorları belirlenmiştir. Bu kapsamda hesaplama yapılırken, 50 ve üzeri uygulama şartının yanı sıra her üreticiye ait en az 2 cihazın bulunması şartı da uygulanmıştır. Şekil 5.1'de de gösterildiği üzere, Xiaomi Redmi marka cihazlar hesaplanan skorlara göre, kullanıcı mahremiyet ve güvenliği açısından en tehlikeli cihazlardır. Bunun haricinde hesaplanan ortalama cihaz skorunun olan 18'in üzerinde, Realme, Xiaomi, Huawei, OnePlus ve Sony üreticilerine ait cihazlar bulunmaktadır. Kullanıcı mahremiyeti açısından en güvenli cihazlar ise sırasıyla, Samsung ve Oppo marka cihazlardır.



Şekil 5.1: Üreticilere Göre Ortalama Cihaz Skorları.

Ardından, en yüksek ve en düşük skorlu 10 cihaz çıkarılmıştır. Ortalama skorların aksine, en yüksek skorlu 10 cihazdan 4 tanesinin üreticisi Samsung'dur. Bunun yanında, Xiaomi Redmi'ye ait 3 cihazda yüksek skorlu cihazlar arasındadır. Yine en yüksek skorlu cihazlar arasında Huawei, Sony ve Realme'ye ait cihazlar da bulunmaktadır. En düşük skorlu cihazlar 10 cihazdan 4 tanesinin üreticisi Samsung'dur. Bu durum cihaz üreticisi ile, skor arasından bir bağlantı olmadığını göstermektedir. Bunun haricinde en düşük skorlu cihazlar arasında Huawei, Xiaomi Redmi, Sony ve Oppo'ya ait cihazlar bulunmaktadır. En düşük ve en yüksek skorlu 10 cihazın listesi Şekil 5.2'de görülebilir. Şekilde de görüleceği üzere en yüksek skorlu 10 cihazın tamamı ortalama skorun üzerinde ve en düşük skorlu 10 cihaz ise, ortalama skorun altındadır.

Geliştirilen skorlama sistemi ile cihazların kullanıcı mahremiyeti ve güvenliğine etkisi genel hatlarıyla anlaşılsa bile, kullanılan kriterlerin detaylandırılması ve daha çok cihaz incelemeye dahil edilmesiyle birlikte, bu konu derinlemesine bir şekilde ele alınarak sistem daha güvenilir hale getirilebilir.



(a) En Yüksek Skorlu Cihazlar.

(b) En Düşük Skorlu Cihazlar.

Şekil 5.2: En Yüksek ve En Düşük Skorlu 10 Cihaz.

6. KISITLAR

Kapsam. Tez çalışması kitle kaynaklı metotlar kullanılarak oluşturduğumuz ve 14178 APK dosyası barındıran veri setini kapsamaktadır. Bu sayı ön yüklü uygulama ekosistemini kapsamaktan uzaktadır. Gözlemlerimize göre, veri setini oluşturmak için kullandığımız uygulama resmi bir komite tarafından onaylansa bile, birçok insanın bilinmeyen bir uygulamayı cihazlarına yükleme konusunda çekinceleri olduğunu fark ettik. Ek olarak, insanlar bildikleri ve güvendikleri kaynaklar tarafından yapılan araştırmalara daha fazla destek olma eğilimindedirler. Bundan dolayı, gelecekte kullandığımız Android uygulamanın ve sunucunun kodlarını herkese açık hale getirmeyi planlıyoruz. Böylece bu kodlar kullanılarak benzer çalışmalar yaygınlaşabilir ve daha fazla veri seti oluşturulabilir. Bu veri setleri birleştirilerek daha kapsayıcı bir veri seti oluşturulabilir ve daha kapsayıcı çalışmalar yapılabilir.

Araştırmacıların Sayısı. Açık bir şekilde görülmektedir ki, Android cihazlardaki ön yüklü uygulamalar üzerine daha fazla araştırmacı odaklanmalıdır. Bunun ana sebeplerinden birisi, çeşitli sebeplerden dolayı bu uygulamaların çoğunluğunun dinamik analiz edilememesi ve sadece statik analiz yöntemleri ile analiz edilebilmesidir. Ancak, statik analiz yöntemleri doğası gereği daha fazla zaman ve kaynağa ihtiyaç duymaktadır. Bundan dolayı, araştırmacılar bu alan hakkında daha fazla bilgilendirilmeli ve bu alanda çalışmak için teşvik edilmelidir.

Tam Analiz.Yukarıda bahsedildiği gibi, çalışmamız kapsamında sadece statik analiz metotlarını kullandık. Ancak, uygulamaların tam fonksiyonelliğinin sadece bu analiz metotları ile anlaşılması mümkün değildir. Çünkü uygulamalar yansıma (reflection), dinamik kod yükleme, yerel kütüphaneler (Örn., .so files), kod karmaşıklaştırma ve çeşitli şifreleme yöntemleri kullanabilir. Bundan dolayı, araştırmacılar dinamik analiz metotlarının ve platformlarının ön yüklü uygulamalara uygulanabilecek hale getirmek amacıyla çalışmalar yapmalıdır.

7. SONUÇ

Bu tez çalışmasında, hala olgunlaşmakta olan Android cihazlardaki ön yüklü uygulamaların mahremiyet ve güvenlik açısından analizine katkıda bulunulması amaçlanmıştır. Bu kapsamda, ilk olarak ön yüklü uygulamalarda oluşan bir veri seti oluşturulmuştur. Bu veri seti araştırmacıların ve kullanıcıların erişimine açılmıştır [18].

Bu veri seti üzerinde yapılan analizler sonucunda, ön yüklü uygulamalarda bulunan izleyici ekosistemi keşfedilmiş ve bu izleyicilerin kullanıcı mahremiyetine etkisi analiz edilmiştir. Çalışma sonucunda, bu izleyicilerin çoğunlukla 3. parti uygulamalarda bulunduğu gözlemlenmiştir. Cihazlarda bulunan ve ön yüklü olarak gelen 3. parti uygulamalar kaldırılamadığı ve sadece devre dışı bırakılabildiği için, bu durum kullanıcı mahremiyetini tehdit etmektedir. Bu sorun üreticiler ve Google tarafından cihazın çalışması için gerekli olmayan uygulamaların kaldırılmasına izin verilmesi ile çözülebilir. Ayrıca bazı üreticilere ait ön yüklü uygulamalarda da 3. parti izleyici SDK'lar tespit edilmiştir. Yine bu durum önceki çalışmada belirtildiği gibi [17], üreticiler ile reklam ve izleyici servisleri arasındaki iş birliğini doğrulamaktadır.

Daha sonra, uygulamalar tarafından kullanılan ve tanımlanan izinlerin analizi gerçekleştirilmiştir. Analiz sonucunda, özellikle bazı 3. parti firmalara ait ön yüklü uygulamalar olmak üzere, bazı uygulamaların ihtiyaçları üzerinde izin tanımladıkları tespit edilmiştir. Yine bazı 3. parti firmaların normalde kullanamayacakları yetkilere izin veren izinleri kullandıkları görülmüştür. Ayrıca üreticilere ait bazı ön yüklü uygulamalar ile 3. parti firmalara ait uygulamaların ortak izinler tanımladıkları belirlenmiştir. Bu durum üreticilerle 3. parti firmalar arasındaki iş birliğini ortaya sermektedir. Bu kapsamda, ön yüklü uygulamaların kullandığı tehlikeli izinlerin analizi de gerçekleştirilmiştir. Bu izinler, normal kullanımda kullanıcı onayı ile izne ihtiyaç duyulan durumlarda verildiği, ancak ön yüklü uygulamalarda kullanıcıdan habersiz bir şekilde kullanıldığı için önemlidir.

Bunun yanında, ön yüklü uygulamalardaki manifest dosyaları ve bulut servisleri analiz edilmiştir. Analiz sonucunda bazı uygulamaların sharedUserId, allowBackup, usesClearTextTraffic ve debuggable gibi manifest özellikleri için, en iyi uygulamaları uygulamadıkları tespit edilmiştir. Bu özelliklerin hatalı yönetimi kullanıcı mahremiyeti ve güvenliğini tehlikeye atan durumlara yol açabilir. Bundan dolayı, bu özellikler konusunda geliştiricilerin en iyi uygulamaları takip etmeleri büyük önem arz etmektedir. Ek olarak, ön yüklü uygulamalar tarafından kullanılan bulut servisleri analiz edilmiştir. Bu çalışma sonucunda bazı bulut servislerine ait çeşitli hatalı konfigürasyonlar tespit edilmiştir. Bu hataların bazıları tespit edildiği uygulamanın yanı sıra, firmalara ait başka uygulama ve servisleri de etkilemektedir. Bu yüzden, uygulama geliştiriciler bulut servislerinin güvenli kullanımı konusunda azami dikkat göstermelidir.

Bununla birlikte, yaptığımız anket çalışması sonucunda kullanıcıların Android cihazlarda bulunan ön yüklü uygulamalar hakkında yeterli bilgi sahibi olmadığını tespit edilmiştir. Bu durumu iyileştirmek adına, üreticiler kullanıcılara yaptıkları işlemler hakkında daha bilgilendirici ve şeffaf olmalıdır. Ayrıca kullanıcıları bu konuda bilgilendirmek için, ön yüklü uygulamalar üzerine yapılan çalışmalar artırılmalı ve sonuçları normal kullanıcıların anlayacağı şekilde yaygınlaştırılmalıdır.

Kullanıcıları bilinçlendirmek ve daha fazla araştırmacının dikkatini çekmek amacıyla bir web sitesi oluşturulmuş ve yapılan çalışma sonucunda elde edilen verilen burada yayınlanmıştır. Ayrıca yapılan analizler sonucunda elde edilen sonuçlar kullanılarak ilkel bir skorlama sistemi geliştirilmiş ve cihazlar bu sisteme göre değerlendirilmiştir. Gelecekte yapılacak çalışmalar ile daha detaylı analizler yapılarak ve daha kapsayıcı bir veri seti kullanılarak bu sistem geliştirilebilir.

Sonuç olarak, yapılan çalışma ile Android ekosistemindeki ön yüklü uygulamaların kullanıcı mahremiyetine etkisini ve kullanıcıların bu konudaki algılarını aydınlatmaya katkı sunulmuştur. Bu çalışma ile duyurulan ve tanıtılan herkese açık ön yüklü uygulama veri kümesi [18] kullanılarak ön yüklü uygulamalara detaylı manuel statik analiz yapılması, ön yüklü uygulamaların dinamik olarak incelenmesine yönelik sistem geliştirilmesi, ön yüklü uygulamaların *IPC (Inter Process Communication)* için kullandığı mekanizmaların güvenlik analizinin yapılması gibi konularda daha fazla araştırmacının çalışma yapmasına yardımcı olacağı ümit edilmektedir. Yine bu çalışmada sunulan skorlama sistemi geliştirilerek, kullanıcıların cihazlarının satın alırken dikkat ettikleri bir etmen haline gelmesi hedeflenmektedir.

KAYNAKLAR

[1] "Mobile operating system market share worldwide - statcounter global stats," https://gs.statcounter.com/os-market-share/mobile/worldwide, (Son Erişim Tarihi 06/27/2021).

[2] "Android open source project," https://source.android.com/, (Son Erişim Tarihi 06/27/2021).

[3] "Android compatibility program overview - android open source project," https://source.android.com/compatibility/overview?hl=en, (Son Erişim Tarihi 06/27/2021).

[4] "Android compatibility definition document," https://source.android.com/compatibility/cdd, (Son Erişim Tarihi 06/27/2021).

[5] "Compatibility test suite - android open source project," https://source.android.com/compatibility/cts, (Son Erişim Tarihi 06/27/2021).

[6] "Android – certified," https://www.android.com/certified/, (Son Erişim Tarihi 06/27/2021).

[7] "Android certified partners," https://www.android.com/certified/partners/, (Son Erişim Tarihi 06/27/2021).

[8] "Securing the system: A deep dive into reversing android preinstalled apps," https://i.blackhat.com/USA-19/Thursday/us-19-Stone-Securing-The-System-A-Deep-Dive-Into-Reversing-Android-Preinstalled-Apps.pdf, (Son Erişim Tarihi 06/27/2021).

[9] "Google approval, certification for android devices - venturus," https://www.venturus.org.br/en/google-approval-certification-for-android-devices/, (Son Erişim Tarihi 06/27/2021).

[10] "Vendor test suite (vts) & infrastructure," https://source.android.com/compatibility/vts?hl=en, (Son Erişim Tarihi 11/09/2021).

[11] "Android firmware sending private information without consent - kryptowire," https://www.kryptowire.com/kryptowire-discovers-mobile-phone-firmware-transmitted-personally-identifiable-information-pii-without-user-consent-disclosure/, (Son Erişim Tarihi 06/27/2021).

[12] "Google android security 2018 report final.pdf," https://source.android.com/security/reports/Google_Android_Security_2018_Report_Final.pdf, (Son Erişim Tarihi 06/27/2021).

[13] “Two weeks of securing samsung devices: Part 1 - oversecured blog,” https://blog.oversecured.com/Two-weeks-of-securing-Samsung-devices-Part-1/, (Son Erişim Tarihi 06/27/2021).

[14] “Two weeks of securing samsung devices: Part 2 - oversecured blog,” https://blog.oversecured.com/Two-weeks-of-securing-Samsung-devices-Part-2/, (Son Erişim Tarihi 11/09/2021).

[15] “Facebook app can’t be deleted from certain samsung phones - bloomberg,” https://www.bloomberg.com/news/articles/2019-01-08/samsung-phone-users-get-a-shock-they-can-t-delete-facebook, (Son Erişim Tarihi 06/27/2021).

[16] “Facebook gave device makers deep access to data on users and friends - the new york times,” https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html?mtrref=undefined&gwh=DFAE7B3996870E0D2452CDBF4B2F1154&gwt=pay&assetType=PAYWALL, (Son Erişim Tarihi 06/27/2021).

[17] J. Gamba, M. Rashed, A. Razaghpanah, J. Tapiador, and N. Vallina-Rodriguez, “An analysis of pre-installed android software,” in *2020 IEEE Symposium on Security and Privacy (SP)*, 2020, pp. 1039–1055.

[18] “Android pre-installed applications | kaggle,” https://www.kaggle.com/abdullahzbay/android-preinstalled-applications, (Son Erişim Tarihi 11/09/2021).

[19] “Pre-app collector - google play,” https://play.google.com/store/apps/details?id=com.preappcollector, (Son Erişim Tarihi 06/27/2021).

[20] “Devices,” https://preappcollector.com/analysis_results, (Son Erişim Tarihi 11/09/2021).

[21] “Google play store,” https://play.google.com/store, (Son Erişim Tarihi 06/27/2021).

[22] “Galaxy store apps - the official samsung galaxy site,” https://www.samsung.com/global/galaxy/apps/galaxy-store/, (Son Erişim Tarihi 06/27/2021).

[23] “The amazon app,” https://www.amazon.com/gp/mas/get/amazonapp, (Son Erişim Tarihi 06/27/2021).

[24] “F-droid - free and open source android app repository,” https://f-droid.org/en/, (Son Erişim Tarihi 06/27/2021).

[25] “Apkpure.com,” https://apkpure.com/, (Son Erişim Tarihi 06/27/2021).

[26] K. W. Y. Au, Y. F. Zhou, Z. Huang, and D. Lie, “Pscout: Analyzing the android permission specification,” in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, ser. CCS ’12. New York, NY, USA: Association for Computing Machinery, 2012, p. 217–228. [Online]. Available: https://doi.org/10.1145/2382196.2382222

[27] “Github - dlgroupuoft/pscout: This hosts the original version of the pscout android permission mapping tool,” https://github.com/dlgroupuoft/PScout, (Son Erişim Tarihi 11/10/2021).

[28] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, "Android permissions demystified," in *Proceedings of the 18th ACM Conference on Computer and Communications Security*, ser. CCS '11. New York, NY, USA: Association for Computing Machinery, 2011, p. 627–638. [Online]. Available: https://doi.org/10.1145/2046707.2046779

[29] C. Gibler, J. Crussell, J. Erickson, and H. Chen, "Androidleaks: Automatically detecting potential privacy leaks in android applications on a large scale," in *Trust and Trustworthy Computing*, S. Katzenbeisser, E. Weippl, L. J. Camp, M. Volkamer, M. Reiter, and X. Zhang, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 291–307.

[30] G. Tuncay, S. Demetriou, K. Ganju, and C. Gunter, "Resolving the predicament of android custom permissions," 01 2018.

[31] B. Liu, J. Lin, and N. Sadeh, "Reconciling mobile app privacy and usability on smartphones: Could user privacy profiles help?" in *Proceedings of the 23rd International Conference on World Wide Web*, ser. WWW '14. New York, NY, USA: Association for Computing Machinery, 2014, p. 201–212. [Online]. Available: https://doi.org/10.1145/2566486.2568035

[32] A. Razaghpanah, R. Nithyanand, N. Vallina-Rodriguez, S. Sundaresan, M. Allman, C. Kreibich, and P. Gill, "Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem," in *NDSS*, 2018.

[33] R. Binns, U. Lyngs, M. Van Kleek, J. Zhao, T. Libert, and N. Shadbolt, "Third party tracking in the mobile ecosystem," in *Proceedings of the 10th ACM Conference on Web Science*, ser. WebSci '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 23–31. [Online]. Available: https://doi.org/10.1145/3201064.3201089

[34] B. Hu, Q. Lin, Y. Zheng, Q. Yan, M. Troglia, and Q. Wang, "Characterizing location-based mobile tracking in mobile ad networks," in *2019 IEEE Conference on Communications and Network Security (CNS)*, 2019, pp. 223–231.

[35] "Unsecured cloud configurations exposing information in thousands of mobile apps," https://blog.zimperium.com/unsecured-cloud-configurations-exposing-information-in-thousands-of-mobile-apps/, (Son Erişim Tarihi 06/27/2021).

[36] "Mobile app developers' misconfiguration of third party services leave personal data of over 100 million exposed - check point research," https://research.checkpoint.com/2021/mobile-app-developers-misconfiguration-of-third-party-services-leave-personal-data-of-over-100-million-exposed/, (Son Erişim Tarihi 06/27/2021).

[37] "Mobile security testing guide," https://mobile-security.gitbook.io/mobile-security-testing-guide/, (Son Erişim Tarihi 06/27/2021).

[38] D. Barrera, J. Clark, D. McCarney, and P. C. van Oorschot, "Understanding and improving app installation security mechanisms through empirical analysis of android," in *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, ser. SPSM '12. New York, NY, USA:

Association for Computing Machinery, 2012, p. 81–92. [Online]. Available: https://doi.org/10.1145/2381934.2381949

[39] E. Ratazzi, Y. Aafer, A. Ahlawat, H. Hao, Y. Wang, and W. Du, "A systematic security evaluation of android's multi-user framework," *ArXiv*, vol. abs/1410.7752, 2014.

[40] H. Elahi, G. Wang, and J. Chen, "Pleasure or pain? an evaluation of the costs and utilities of bloatware applications in android smartphones," *J. Netw. Comput. Appl.*, vol. 157, no. C, May 2020. [Online]. Available: https://doi.org/10.1016/j.jnca.2020.102578

[41] M. Elsabagh, R. Johnson, A. Stavrou, C. Zuo, Q. Zhao, and Z. Lin, "FIRMSCOPE: Automatic uncovering of privilege-escalation vulnerabilities in pre-installed apps in android firmware," in *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Aug. 2020, pp. 2379–2396. [Online]. Available: https://www.usenix.org/conference/usenixsecurity20/presentation/elsabagh

[42] E. Blázquez, S. Pastrana, Á. Feal, J. Gamba, P. Kotzias, and J. E. Tapiador, "Trouble over-the-air: An analysis of fota apps in the android ecosystem," 2021.

[43] A. Possemato, S. Aonzo, D. Balzarotti, and Y. Fratantonio, "Trust, but verify: A longitudinal analysis of android oem compliance and customization," in *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, pp. 87–102.

[44] "Pre-app collector," https://preappcollector.com/, (Son Erişim Tarihi 11/13/2021).

[45] "ethical_approval.pdf," https://preappcollector.com/static/ethical_approval.pdf, (Son Erişim Tarihi 08/11/2021).

[46] "Androguard," https://github.com/androguard/androguard, (Son Erişim Tarihi 06/27/2021).

[47] "Application signing," https://developer.android.com/studio/publish/app-signing, (Son Erişim Tarihi 06/27/2021).

[48] "exodus," https://reports.exodus-privacy.eu.org/en/, (Son Erişim Tarihi 06/27/2021).

[49] "exodus-standalone," https://github.com/Exodus-Privacy/exodus-standalone, (Son Erişim Tarihi 06/27/2021).

[50] "Google advertising id - play console help," https://support.google.com/googleplay/android-developer/answer/6048248, (Son Erişim Tarihi 06/27/2021).

[51] "General data protection regulation (gdpr)," https://gdpr-info.eu/, (Son Erişim Tarihi 06/27/2021).

[52] "California consumer privacy act (ccpa)," https://oag.ca.gov/privacy/ccpa, (Son Erişim Tarihi 06/27/2021).

[53] “Crunchbase: Discover innovative companies and the people behind them,” https://www.crunchbase.com/, (Son Erişim Tarihi 06/27/2021).

[54] “Why do you even need the imei?” https://blog.appcensus.io/2019/04/26/why-do-you-even-need-the-imei/, (Son Erişim Tarihi 06/27/2021).

[55] “Exclusive: Warning over chinese mobile giant xiaomi recording millions of people’s ’private’ web and phone use,” https://www.forbes.com/sites/thomasbrewster/2020/04/30/exclusive-warning-over-chinese-mobile-giant-xiaomi-recording-millions-of-peoples-private-web-and-phone-use/?sh=7579d95c1b2a, (Son Erişim Tarihi 06/27/2021).

[56] “Baidu’s and don’ts: Privacy and security issues in baidu browser,” https://citizenlab.ca/2016/02/privacy-security-issues-baidu-browser/, (Son Erişim Tarihi 06/27/2021).

[57] “Data leakage found from android apps on google play with millions of downloads,” https://unit42.paloaltonetworks.com/android-apps-data-leakage/, (Son Erişim Tarihi 06/27/2021).

[58] “Dji releases security findings it hopes will quash ’chinese spying’ fears,” https://gizmodo.com/dji-releases-security-findings-it-hopes-will-quash-chin-1825469976, (Son Erişim Tarihi 06/27/2021).

[59] “Privacy policy - mintegral,” https://mintegral.com/en/privacy/, (Son Erişim Tarihi 06/20/2021).

[60] “Privacy policy - moengage,” https://www.moengage.com/privacy-policy/, (Son Erişim Tarihi 06/27/2021).

[61] “Report: Aurora mobile’s jpush sdk – the appcensus blog,” https://blog.appcensus.io/2020/09/15/report-aurora-mobiles-jpush-sdk/, (Son Erişim Tarihi 06/27/2021).

[62] “Industry collaborations - mopub,” https://www.mopub.com/en/resources/partnerships, (Son Erişim Tarihi 06/27/2021).

[63] Z. Wang, “Systematic government access to private-sector data in China,” *International Data Privacy Law*, vol. 2, no. 4, pp. 220–229, 07 2012. [Online]. Available: https://doi.org/10.1093/idpl/ips017

[64] “What is"com,facebook,app manager" and why is it trying to download instagram, facebook, and messenge - android forums at androidcentral.com,” https://forums.androidcentral.com/android-apps/547447-what-com-facebook-app-manager-why-trying-download-instagram-facebook-messenge.html, (Son Erişim Tarihi 11/21/2021).

[65] “com.facebook.appmanager | xda forums,” https://forum.xda-developers.com/t/com-facebook-appmanager.2919151/, (Son Erişim Tarihi 11/21/2021).

[66] “Facebook is the new crapware | techcrunch,” https://techcrunch.com/2019/01/09/facebook-is-the-new-crapware/, (Son Erişim Tarihi 11/20/2021).

[67] “Vlingo privacy breach: Data sent to remote servers without consent | nextpit,” https://www.nextpit.com/Vlingo-security-flaw, (Son Erişim Tarihi 11/19/2021).

[68] “Hiya: Caller id, call blocker & protection for a better voice experience,” https://www.hiya.com/, (Son Erişim Tarihi 11/21/2021).

[69] “Truecaller is the leading global platform for verifying contacts and blocking unwanted communication. | truecaller,” https://www.truecaller.com/, (Son Erişim Tarihi 11/21/2021).

[70] “Hiya data policy,” https://www.hiya.com/hiya-data-policy, (Son Erişim Tarihi 11/21/2021).

[71] “Privacy policy - digital turbine,” https://www.digitalturbine.com/privacy-policy/, (Son Erişim Tarihi 11/21/2021).

[72] “Aura for advertisers,” https://www.slideshare.net/ironSource/aura-for-advertisers, (Son Erişim Tarihi 11/22/2021).

[73] “App manifest overview | android developers,” https://developer.android.com/guide/topics/manifest/manifest-intro, (Son Erişim Tarihi 06/27/2021).

[74] “Nvd - cve-2018-14825,” https://nvd.nist.gov/vuln/detail/CVE-2018-14825, (Son Erişim Tarihi 06/27/2021).

[75] “Android developers blog: Protecting against unintentional regressions to cleartext traffic in your android apps,” https://android-developers.googleblog.com/2016/04/protecting-against-unintentional.html, (Son Erişim Tarihi 06/27/2021).

[76] “jdb - the java debugger,” https://docs.oracle.com/javase/7/docs/technotes/tools/windows/jdb.html, (Son Erişim Tarihi 06/27/2021).

[77] “Firebase,” https://firebase.google.com/, (Son Erişim Tarihi 06/28/2021).

[78] “Amazon web services (aws) - cloud computing services,” https://aws.amazon.com/, (Son Erişim Tarihi 06/28/2021).

[79] “Cloud computing services | microsoft azure,” https://azure.microsoft.com/en-us/, (Son Erişim Tarihi 06/28/2021).

[80] “Google maps platform | google developers,” https://developers.google.com/maps, (Son Erişim Tarihi 06/28/2021).

[81] “dwisiswant0/apkleaks: Scanning apk file for uris, endpoints & secrets.” https://github.com/dwisiswant0/apkleaks, (Son Erişim Tarihi 06/28/2021).

[82] “skylot/jadx: Dex to java decompiler,” https://github.com/skylot/jadx, (Son Erişim Tarihi 06/28/2021).

[83] “Apktool - a tool for reverse engineering 3rd party, closed, binary android apps.” https://ibotpeaches.github.io/Apktool/, (Son Erişim Tarihi 06/28/2021).

[84] “gmapsapiscanner,” https://github.com/ozguralp/gmapsapiscanner/, (Son Erişim Tarihi 06/28/2021).

[85] “Oauth 2.0 — oauth,” https://oauth.net/2/, (Son Erişim Tarihi 06/28/2021).

[86] “Billing: Mapping previous skus to new skus | google maps platform,” https://developers.google.com/maps/billing/sku-mapping-old-to-new, (Son Erişim Tarihi 06/28/2021).

[87] “Google maps platform billing | google developers,” https://developers.google.com/maps/billing/gmp-billing, (Son Erişim Tarihi 06/29/2021).

[88] “Global cloud infrastructure market share 2021 | statista,” https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/, (Son Erişim Tarihi 06/29/2021).

[89] “Aws general reference - reference guide,” https://docs.aws.amazon.com/general/latest/gr/aws-general.pdf, (Son Erişim Tarihi 06/29/2021).

[90] “Authenticating users of aws mobile applications with a token vending machine - aws articles,” https://aws.amazon.com/tr/articles/authenticating-users-of-aws-mobile-applications-with-a-token-vending-machine/, (Son Erişim Tarihi 08/15/2021).

[91] “Protecting mobile apps with pkce - oauth 2.0 simplified,” https://www.oauth.com/oauth2-servers/pkce/, (Son Erişim Tarihi 07/05/2021).

[92] “Amazon suspends sales of blu phones for including preloaded spyware, again - the verge,” https://www.theverge.com/2017/7/31/16072786/amazon-blu-suspended-android-spyware-user-data-theft, (Son Erişim Tarihi 06/27/2021).

[93] “Buying a smart phone on the cheap? privacy might be the price you have to pay - privacy international,” https://privacyinternational.org/long-read/3226/buying-smart-phone-cheap-privacy-might-be-price-you-have-pay, (Son Erişim Tarihi 06/26/2021).

[94] “Mobile security updates: Understanding the issues,” https://www.ftc.gov/system/files/documents/reports/mobile-security-updates-understanding-issues/mobile_security_updates_understanding_the_issues_publication_final.pdf, (Son Erişim Tarihi 06/26/2021).

[95] “Kişisel verileri koruma kurumu | kvkk | personal data protection authority,” https://www.kvkk.gov.tr/en/, (Son Erişim Tarihi 06/26/2021).

[96] “Devices,” https://preappcollector.com/analysis_results, (Son Erişim Tarihi 11/23/2021).

[97] “Github - pkumza/libradar: Libradar - a detecting tool for 3rd-party libraries in android apps.” https://github.com/pkumza/LibRadar, (Son Erişim Tarihi 11/24/2021).

EKLER

EK 1 : Kullanıcı Anketi Soruları.

EK 1

1) Lütfen yaş aralığınızı seçiniz.
a. 18 yaş ve altı
b. 18-24
c. 25-34
d. 35-44
e. 45-64

2) Lütfen cinsiyetinizi seçiniz.
a. Kadın
b. Erkek
c. Cevaplamak istemiyorum

3) Eğitim durumunuz nedir?
a. İlkokul-Ortaokul
b. Lise
c. Lisans
d. Yüksek Lisans
e. Doktora

4) Siber güvenlik/mobil güvenlik ile profesyonel olarak ilgileniyor musunuz?
a. Evet
b. Hayır

5) Akıllı telefonunuzu nereden satın aldınız?
a. Teknoloji Mağazası, Telefon Operatörü, Yerel Mağaza, 2. El Satıcı, Online Market vb. Teknoloji Mağazası, Telefon Operatörü, Yerel Mağaza, 2. El Satıcı, Online Market vb. (Metin Kutusu)

6) Akıllı telefonunuzu ne kadar paraya satın aldınız?
a. 0-130 $
b. 131-350 $
c. 351-700 $
d. 701–1400 $
e. 1400 $ and above

7) Ne kadar süredir bu akıllı telefonu kullanıyorsunuz?
a. 0-1 Yıl
b. 1-2 Yıl
c. 2-5 Yıl
d. 5 Yıl ve üzeri

8) Ne sıklıkla akıllı telefonunuzu değiştiriyorsunuz?
a. 0-1 Yıl
b. 1-2 Yıl
c. 2-5 Yıl
d. 5 Yıl ve üzeri

9) Telefonunuzu ilk aldığınızda kaç tane ön yüklü (cihaz kutudan çıktığında yüklü olarak cihazda bulunan) uygulama olduğunu düşünüyorsunuz?
a. 0-20
b. 21-100
c. 101-200
d. 201-300
e. 301-400
f. 400 ve üzeri

10) Akıllı telefon satın alırken, satın alma kararınızı etkileyen faktörleri seçiniz. (Kullanıcılar birden fazla seçenek seçebilirler.)
a. Fiyat
b. Model
c. Popülerlik
d. Üretici şirketin bulunduğu ülke (Samsung – Güney Kore, Huawei – Çin vb.)
e. Üreticinin/Satıcının Güvenlik ve Gizlilik Politikası
f. Büyük ve bilinen firmalar tarafından satılması/üretilmesi

11) Akıllı telefonunuzun kurulumunu yaparken ön yüklü uygulamalar ve bu uygulamaların gerçekleştirdiği işlemler ve topladığı veriler hakkında bilgilendirildiniz mi?
a. Evet bilgilendirildim.
b. Hayır bilgilendirilmedim.
c. Dikkat etmedim / Okumadım.

12) Bu konularda sizden izin alındı mı? a. Hayır alınmadı.
b. Evet alındı.
c. Dikkat etmedim / Okumadım.

13) Telefonunuza yüklediğiniz uygulamaların hangi izinleri kullandığına dikkat ediyor musunuz?
a. Hayır etmiyorum.
b. Evet ediyorum.

14) Düzenli olarak bu izinleri kontrol ediyor musunuz?
a. Hayır etmiyorum.
b. Evet ediyorum.

15) Cihazınızda bulunan uygulamaların güncel olmasına dikkat ediyor musunuz?
a. Evet
b. Hayır

16) Kişisel Verileri Koruma Kanunu (KVKK) hakkında bilgi sahibi misiniz?
a. Evet
b. Hayır