MOBİL UYGULAMALARDA ERİŞİM İZİNLERİ

Hakan İlgar
112692043

İSTANBUL BİLGİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

Yrd. Doç. Dr. Tayfun ACARER

2016

MOBİL UYGULAMALARDA ERİŞİM İZİNLERİ

ACCESS PERMISSIONS IN MOBILE APPLICATIONS

Hakan İLGAR
112692043

Yrd. Doç. Dr. Tayfun ACARER : T. Acarer
(Danışman, İstanbul Bilgi Ü. Meslek Yüksek Okulu)

Doç. Dr. Leyla KESER BERBER :
(Jüri Üyesi, İstanbul Bilgi Ü. Hukuk F.)

Yrd. Doç. Dr. Mehmet Bedii KAYA :
(Jüri Üyesi, Yıldırım Beyazıt Ü. Hukuk F.)

Tezin Onaylandığı Tarih : 06 Mayıs 2017

Toplam Sayfa Sayısı : 63

Anahtar Kelimeler (Türkçe)

1) Mobil İşletim Sistemleri
2) Mobil Uygulamalar
3) Erişim İzinleri
4) Zararlı Yazılımlar
5) Güvenlik Zaafiyetleri

Anahtar Kelimeler (İngilizce)

1) Mobile Operating Systems
2) Mobile Applications
3) Access Permissions
4) Malicious Software
5) Security Vulnerabilities

ÖNSÖZ

Eğitimim boyunca emeği geçen, bilgilerini benden esirgemeyen değerli hocalarım Doç. Dr. Leyla Keser Berber, Yrd. Doç. Tayfun Acarer ve Yrd. Doç. Dr. Mehmet Bedii Kaya'ya ayrıca her konuda destek olan aileme sevgi ve teşekkürlerimi sunarım.

İÇİNDEKİLER

KISALTMALAR

API	:	Application Programming Interface
Apple Store	:	Store for Apple iOS apps
Bluetooth	:	Wireless Technology
Brute Force	:	Kaba Kuvvet Saldırı
DDoS	:	Distributed Denial-Of-Service
EULA	:	End User License Agreement
Google Play	:	Formerly Android Market
GPS	:	Global Positioning System
GSM	:	Global System for Mobile Communications
iCloud	:	Apple Inc Cloud storage
IMEI	:	International Mobile Equipment Identifier
IMSI	:	International Mobile Subscriber Identity
Jailbreak	:	iOS işletim sisteminde yazılım kısıtını kaldırma
MAC	:	Media Access Control
Malware	:	Malicious Software
MMS	:	Multimedia Messaging Service
OWASP	:	Open Web Application Security Project
PIN	:	Personal Identification Number
Rooting	:	Android işletim sisteminde tam yetkinin sağlanması
SD	:	Secure Digital Card
SMS	:	Short Message Service
SQL	:	Structured Query Language
SSL	:	Secure Sockets Layer
TED	:	Technology, Entertainment, Design
TLS	:	Transport Layer Security
UDID	:	Unique Device Identifier
URL	:	Uniform Resource Locator
UUID	:	Universally Unique Identifier
Wi-Fi	:	Wireless Local Area Networking
XML	:	Extensible Markup Language
XSS	:	Cross Site Scripting

ŞEKİLLER

TABLOLAR

ABSTRACT

Today, many users with intelligent devices are constantly interacting with or has to be. Accurate detection of security threats from many mobile applications has become an important and difficult issue for information security. These applications, which can offer various functions of users, require permissions in different types. It is difficult to understand that these permissions may overlap with application functionality and may be malicious. In this study, users attitudes to mobile applications and privacy levels of applications are examined; suggestions have been made to minimize the security risks. Within the scope of the research, access permissions that can be taken in mobile applications were examined with examples and effects were investigated. In addition, detection of malware and provision of user security on mobile devices has been reviewed and suggested within the scope of this research.

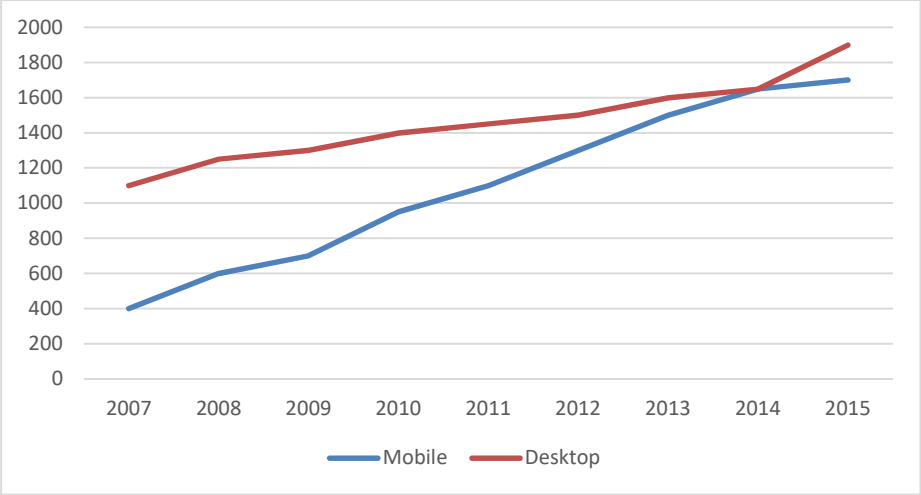
ÖZET

Bugün, akıllı cihaza sahip birçok kullanıcı, artan mobil uygulamalar ile sürekli etkileşim halindedir ya da olmak zorundadır. Birçok mobil uygulama arasından güvenlik tehditlerinin doğru tespit edilmesi, bilgi güvenliği açısından önemli ve zor bir konu haline gelmiştir. Kullanıcılar için çeşitli işlevler sunabilen bu uygulamalar, farklı türlerde izinler talep etmektedir. Alınabilecek bu izinlerin, uygulama işlevi ile örtüşüp örtüşmeyeceğini ve kötü niyetli olabileceği anlamak oldukça zordur. Bu çalışma içerisinde, kullanıcıların mobil uygulamalara karşı tutumu ve uygulamaların gizlilik seviyeleri incelenmiş; güvenlik risklerinin en aza indirilmesi için önerilerde bulunulmuştur. Araştırma kapsamında, mobil uygulamalarda alınabilecek erişim izinleri örneklerle incelenmiş ve etkileri araştırılmıştır. Ayrıca, mobil cihazlarda kötü amaçlı yazılımların tespit edilmesi ve kullanıcı güvenliğinin sağlanması, bu araştırma kapsamında incelenmiş ve önerilerde bulunulmuştur.

Mobil Uygulamalarda Erişim İzinleri

1. Giriş

Günümüzde, teknolojinin giderek geliştiğini, geliştikçe de boyutunun küçüldüğünü ama veri kapasitesinin de büyüdüğünü gün geçtikçe daha iyi anlıyoruz. Bu teknolojiler günlük yaşamımızın birçok ihtiyacını karşılayabilen, hesaplama yapabilen akıllı cihazlar haline gelmiş ve her alanda yüksek bir kullanım oranına sahip aygıtlar olmayı başarmıştır. İş toplantısında, bir e-posta gönderiminde, ulaşımda, iletişim sırasında ya da ödeme durumunda akıllı cihazlarında kullanımını sıklıkla görebiliriz. Bir akıllı telefon ile yaşamamızın her anını daha kolay ve hızlıca geçirebiliriz. Örneğin yapmanız gereken bir ödemeniz var ve süreniz de çok az. Vakit kaybetmeden ya da sıra beklemeden mobil cihazınıza kurulu uygulama üzerinden işleminizi yapabilir ve zamandan tasarruf edebilirsiniz. Bu durum teknolojinin sunmuş olduğu kolaylıklardan sadece biridir.



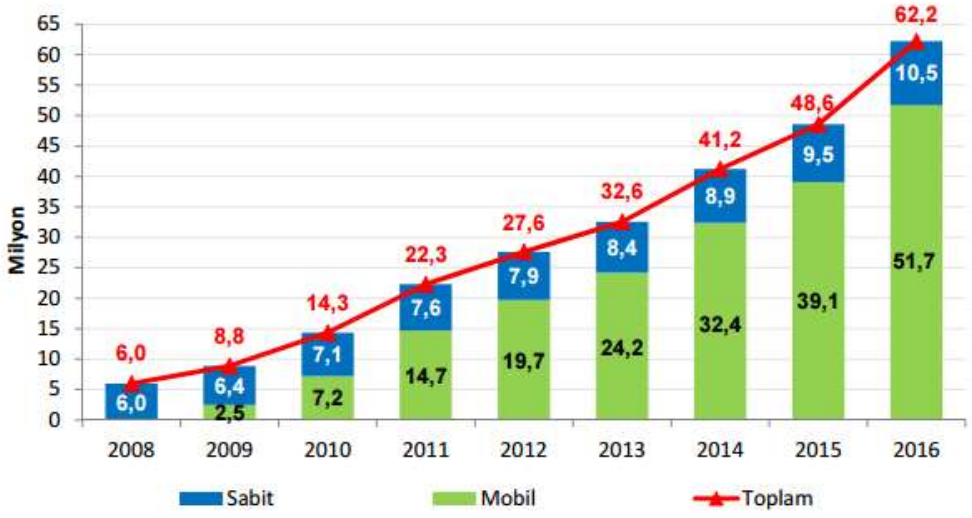
Şekil 1: Mobil Cihazlarda Artış Oranları [1]

Şu an mobil cihaz pazarında birçok cep telefonu, mobil iletişim standartlarının ve mobil iletişim teknolojisinin dördüncü nesli sayılan 4,5G şebekesini desteklemeye doğru gitmektedir. Aynı zamanda 3G teknolojisinin bir uzantısı da olan bu teknoloji, yüksek hız, daha fazla kapasite, çok güçlü performans ve evrensel

[1]Orjinal çizim için bknz. http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics

bir ağa sahiptir. Veri iletim hızının 3G'den çok daha hızlı olması ve teorik olarak da internet erişim hızının ötesine geçebilmesi onu son derece kusursuz kılmaktadır. 3G haberleşme sistemi, mobil telefonlar üzerinden sadece ses, sms hizmeti ve mobil internet hizmeti sunabiliyor iken bağlantı hızı en fazla 42 Mbps'a kadar ulaşabilmektedir. 4,5G'de ise bu durum biraz daha üst seviyeye taşındığı gibi, 1 Gbps bağlantı hızı ile de benzersiz bir üstünlük sağlamıştır. 4,5G altyapısı, 3G teknolojisinden farklı olarak "Çok daha hızlı veri ve internet bağlantısı, düşük gecikme süresi ile kesintisiz iletişim, yüksek görüntü kalitesi, daha iyi kapsama alanı, bulut bilişim teknolojisini kullanma, gerçek zamanlı veri paylaşımı, video konferans ve telekonferansta hızlı ve kaliteli iletişim, gelişmiş multimedya entegrasyonu, verilere uzaktan erişim, maliyet düşüşü, kaynakların verimli kullanılması, zaman tasarrufu" [2] sağlamıştır.

4,5G'nin ile birlikte sektörde yeni trendler oluşmaya ve güçlü yapılar kurulmaya başlandı. Bu büyüme trendi, hükümet, mobil cihaz üreticileri, teknoloji sağlayıcıları, telekom altyapı sağlayıcıları ve uygulama geliştiricileri de dahil olmak üzere 4,5G değer zincirindeki tüm paydaşlar için birçok fırsat yarattı. Devletin de katkısı ile yapılan 4,5G hizmetlerinin kullanımını teşvik etme ve daha fazla kullanıcı çekme, ulusal teknoloji ekosistemini şekillendirme açısından hayati bir rol oynadı.

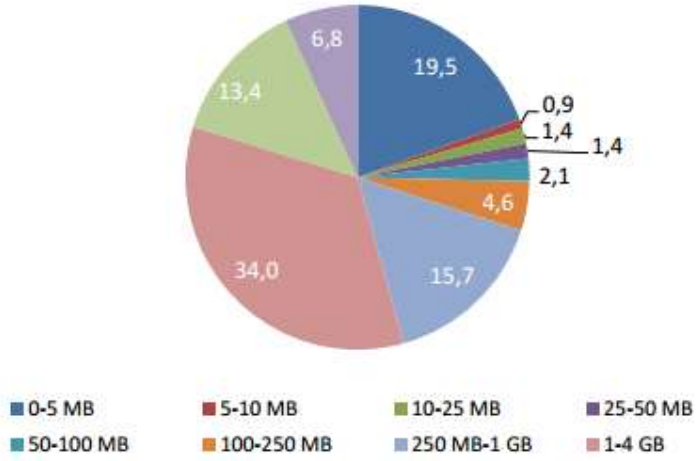


Şekil 2: Genişbant İnternet abone sayısı [3]

[2] 3G ile 4.5G Arasındaki Farklar Nelerdir? https://www.btk.gov.tr/tr-TR/Sayfalar/3G-ile-45G-Arasindaki-Farklar-Nelerdir

[3] Orijinal çizim için bknz. 2016-4 Üç Aylık Pazar Verileri Raporu

4,5G hizmet alt yapısındaki servislerinin büyümesi, video, müzik ve OTT (Over the Top) uygulamalarında kaliteli bir artışa neden oldu. OTT sayılabilecek (WhatsApp, Skype, Facebook ve Twitter) firmalar sektörde büyük kazançlar elde ederek, kullanıcılara ücretsiz, hızlı ve kaliteli bir hizmet sunmaya başladı.



Şekil 3: Mobil Cepten İnternet Abonelerinin Kullanıma Göre Dağılımı, % [4]

4,5G teknolojisi, mobil akıllı cihaz pazarını da hareketlendirdiği gibi OTT yazılım sektörünü de geliştirmiş oldu. Yüksek kalitede video izleme, mesajlaşma, gerçek zamanlı içerik paylaşımı ve görüntülü arama yapabilen gelişmiş yazılım ve uygulamalar, uygulama marketlerinde yerini aldı. Bu uygulamalar doğası gereği aktif, internete bağlı ve sürekli veri alıp verebilen bir yapıda olduğu için, operatörlerin sunmuş olduğu hız ve data paketleri de artmış oldu.

Bugün, akıllı telefona sahip birçok kullanıcı, artan mobil uygulamalar ile sürekli etkileşim halindedir ya da olmak zorundadır. Hesap makinesinden, gelişmiş dijital asistanlara kadar basit gibi görülebilen pek çok araç neredeyse sınırsız sayıda işlev sunabilir duruma gelmiş ve kullanıcıların kullanımına hazır hale getirilmiştir. Bu uygulamaların, mobil cihazlar üzerinde çalışabilmesi için, kurulum öncesinde cihazın özelliklerine ve bu cihazın kullanıcı bilgilerine erişebilmesi gerekmektedir. Kullanıcı farketmese de büyük bir güvenlik riski bu noktadan sonra başlar. Kullanıcının gizli bilgileri herhangi bir uygulama içinde açıldığı an, bu bilgilerin tamamı uygulamayı geliştirenlerin eline geçmiş olma olasılığı çok yüksektir. Elbette bunlar arasında güvenilir olmayan kişiler, kullanıcının bilgilerini istimar edebilir, doğrudan satışa sunabilir. Online sistemlerde, bankacılık ya da benzeri kurumlar

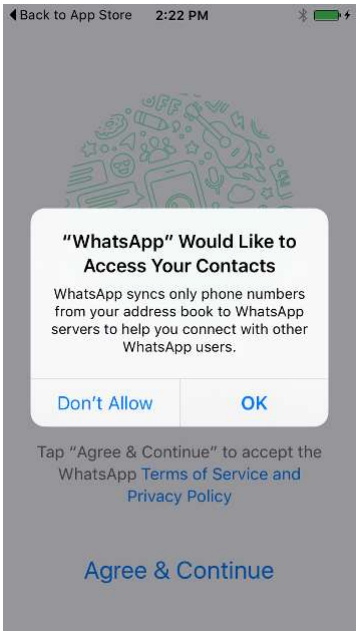
[4] Orijinal çizim için bknz. 2016-4 Üç Aylık Pazar Verileri Raporu

içerisinde bu bilgileri kullanarak sahtecilik (fraud) gerçekleştirebilir. Bu da demektir ki yöntem ne olursa olsun, hemen her kullanıcıyı tehdit edebilecek bu işlemler, kullanıcı açısından az da olsa tehlike arz edebilir. Örneğin kullanıcı uygulamayı cihazına yükler ve kullanmaya başlar. Uygulama kullanım sırasında sorun çıkarmamak ve aktif halde kalabilmek adına çalışmaya devam eder. Uygulamanın kurulum evresinde almış olduğu izinler, bu etkileşimin işlemesinde yani izinlerin vermiş olduğu yetkisel durumlarda önemli rol oynar. Eğer uygulama internet bağlantısı gerektiren ve çevrimiçi kalması gereken bir uygulama ise, kullanıcı uygulamayı kullanmaya başladığı anda sistem işlemeye başlar. Uygulama verileri ağ bağlantısı üzerinden servis sağlayıcısına belli senkronlarda verileri iletmeye başlar. İletilen bu veriler, kullanıcının kişisel verileri ya da uygulamanın kendi verileridir. Kullanıcı daha uygulamayı kullanmaya başlarken ki yapmış olduğu tüm aksiyonların bir kaydını karşı tarafa farkında olmasa da iletmiş olur. Uygulamanın, verileri ne şekilde okumaya başladığı, ne şekilde ilettiği, arada ki güvenliğin nasıl sağlandığı tamamıyla uygulamayı üreten geliştiren kişi ya da kurumun insiyatifine kalmıştır. En başında uygulama yüklenme aşamasında ona o izinleri veren kullanıcının kendisidir.

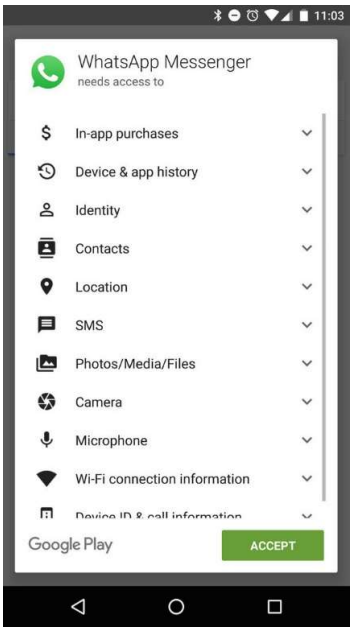
2. Mobil Cihazlarda Erişim İzinleri

Uygulama marketi (Google Play, Apple Store vs) üzerinden indirilen uygulamaların mobil cihazlar üzerine yüklenebilmesi için kullanıcıdan erişim izinlerinin alınması gerekmektedir.

Uygulamalara bu kurulum aşamasında verilen izinlerin ne anlama geldiğini, ne gibi tehlikeler oluşturabileceğini ya da bu izinlere ilişkin hukuki sözleşmelerin olup olmadığını birçoğumuz dikkat dahi etmeden geçiyor ve uygulamayı kullanmaya başlıyoruz.



Şekil 4: WhatsApp Erişim İzni - iPhone Örneği [5]



Şekil 5: WhatsApp Erişim İzni - Android Örneği [6]

Kullanıcılar mahremiyetlerini nasıl koruyabilecekleri konusunda henüz bilgi sahibi değiller. Bu durumu aydınlatıcı bulmak adına, geliştirici kişi ya da kurumlar, kullanıcı sözleşmesinde açıkça uygulamanın gizlilik ve politikalarını gerekçeleri ile belirtmişlerdir. Bu bilgiler arasında, verilerin ne şekilde

[5] Orijinal çizim için bknz. https://ssd.eff.org/en/module/how-use-whatsapp-ios
[6] Orijinal çizim için bknz. https://www.urbanairship.com/blog/app-permissions-cross-promotion-strategies

kullanılacağını, öncesinde ve sonra toplanan verilerin gizliliğini ve toplama gerekçelerini madde madde paylaşılmıştır. Örneğin popüler bir eposta istemci uygulaması Android işletim sistemi üzerine kurulduktan sonra, geliştirici firmanın uygulama ile beraber yayınlamış olduğu kullanıcı kullanım sözleşmesi içerisinde olabilecek tüm durumları belirtmiş olması gibi. Kişiden hangi bilgiler alınıyor, geliştirici firma ne kadar güvenli, kişisel veriler ne şekilde işlenecek veya üçüncü kişi ya da kişiler ile bu bilgiler paylaşılacak mı gibi sorular bu sözleşme metinleri içerisinde yer almaktadır.

Basit anlatım ile uygulama marketine girdiniz, yüklemek istediğiniz uygulamayı seçip cihazınıza kurmak istediniz. Uygulamanın yükleme ön koşulu olarak sizden erişim izinleri talep edilebilir ya da edilmez. Bu adım sonrasında sizin vereceğiniz aksiyona göre uygulama cihazınıza yüklenir ve siz kullanmaya başlarsınız. İlerde sorun yaşamamak adına, mobil cihazlara yüklenebilecek bu uygulamların sağlıklı bir ortam üzerinden indirilip kullanılması beklenir. Ne kadar güvenli ya da bu uygulama cihaza zarar verebilir mi gibi sorularla boğuşmanızı en aza indirir. Ayrıca "belirli özelliklere erişmek için kullanıcının iznini almaya çalışmak, cihazlar arasında kötü amaçlı uygulamaların yayılmasını önlemek amaçlıdır".[7] Bu da demektir ki, kullanılanıcı en başında bu koşullara dikkat etmesi gerekir.

I. Erişim İzni Nedir?

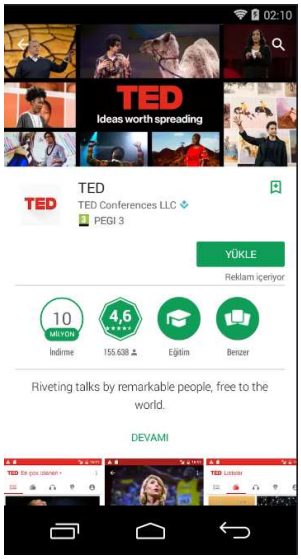
Uygulamanın cihaza yüklerken ki ön koşulu sayılır. Kullanıcı uygulamanın kurulabilmesi için izin vermez ise uygulama kurulamaz ya da belirtilen aksiyonu icraa edemez. Örneğin mesajlaşma uygulamasının telefon rehberine erişmek istemesi gibi. Eğer bu aksiyon için erişim izni vermezseniz, uygulama düzgün çalışmaz ya da erişim isteğini yinelemeye devam eder. Ta ki sizden o onayı alana kadar. Erişim izni verirseniz, uygulama kurulmaya başlar ve uygulamayı kullanan cihazın sahibi ile geliştirici arasındaki etkileşim başlamış olur. Kişinin verdiği onay sonrası, uygulamanın telefon rehberine erişmesi bu durumun bir örneğidir. Kullanıcı onay vermiş olduğu izinlerle aslında uygulamanın koşullarını kabul etmiş ve geliştiriciye olan güvenini bu şekilde kanıtlar.

---

[7] Trend Micro Inc. (2011) "When Android apps Want More Than They Need" http://www.trendmicro.co.uk/media/misc/when-android-apps-want-more-than-they-need-ebook-en.pdf

Uygulamalar sahip olduğu izinler ile cihazın mevcut kaynaklarına erişmek ister. Bu izinleri isteyen her uygulama da, zararlı yazılımlar sonucu üretilmiş uygulama değildir. Ve her uygulama tek bir izin ile sınırlandırılmamıştır. Cihazın özelliklerine erişebilmek için belli tiplere sahip izin ve yetkiler bulunmaktadır. Bu durum, kötü amaçlı yazılımların önüne geçebilmek ve kullanıcıyı ne gibi aksiyonların olabileceğine dair bilgi vermek için bir bildiridir.

Uygulama yüklemek için en güvenilir yer, cihazın sahip olduğu işletim sisteminin bağlı bulunduğu uygulama marketidir. Android platformu için Google Play, iOS platformu için AppleStore gibi. Uygulamalar bu marketlerden daha güvenli ve cihaza zarar vermeden yüklenebilir. Uygulamalar yüklenmeden hemen öncesinde, çalışmak için sizden izin ister. Amaçları sağlayacağı aksiyonlar hakkında fikir verebilmekdir. Örneğin TED Android uygulaması gibi. Bu uygulama Google Play marketi üzerinden indirilmek istendiğinde kullanıcıya vereceği ilk bilgiler, uygulamanın hangi amaçlara hizmet ettiği, kategorisi, indirilme oranı ve reklam içeriğinin olup olmamasıdır.



Şekil 6: Ted Android Uygulaması - Google Play Store [8]

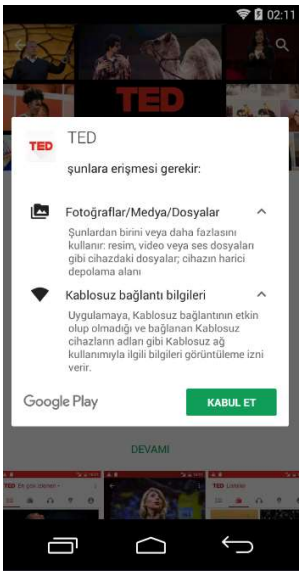
Bu durum, uygulama yükleme marketlerine göre değişebilir. Mesela Google Play üzerinde ödeme sisteminin uygulama içerisinde olabileceği ifade edilirken, AppleStore içerisinde bu durum belirtilmeyebilir.

Uygulamalar kurulmak üzere yüklenmek isteneceği zaman, kullanıcıdan izin ya da izinler taleb eder. Nedeni, cihazın mevcut kaynaklarına erişmek, uygulamanın

[8] Android Google Play marketi https://play.google.com/store/apps/details?id=com.ted.android

kendisini güncel tutabilmek ve kötü amaçlı yazılımların önüne geçebilmektir. Olası bir kötü eylemde kullanıcı farkında olmadan bazı erişim izinlerine onay vermiş de olabilir. Bu durum, kötü amaçlı eylemler tarafından istismar edilebilir. Yani, kendi rızan ile uygulayı indirmiş olur.

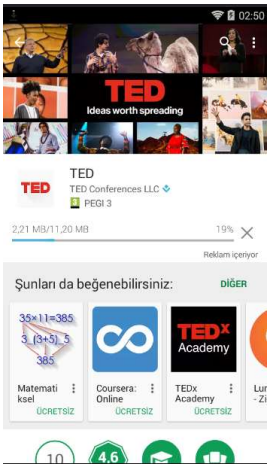
Aşağıda görüldüğü üzere, uygulama kurulum aşamasında alınabilecek eylemler kullanıcıya yansıltılmıştır. Kullanıcı isterse kabul eder ve uygulamayı kullanmaya başlar. İstemezse de kabul etmez ve uygulamada yüklenemez.



Şekil 7: Ted Android Uygulaması - Erişim İzin İsteği [9]

Kullanıcıdan onay alındıktan sonra yani uygulama kurulum bildirisini kabul ettikten sonra uygulama yüklenme işlemi başlar. Bu adım sonrası, uygulama cihaza yüklenir. Ve tüm sorumluluk kullanıcıya geçer. Diğer bir deyişle, tüm hükümleri kabul etmiş sayılırsınız. Sonrası olabilecek kontroller geliştiriciye aittir, onun insiyatifine bağlıdır. Kullanıcı isterse, son kullanıcı lisans anlaşmasını (EULA[10]) okuyabilir, gerekirse olabilecek sorunlara karşı tepkisini dile getirebilir. EULA metinleri, kullanıcı için yazılımın kullanılması sırasında oluşabilecek sorunlara cevap verebilecek bir kaynaktır. Geliştirici kişi ya da firmalar bu metinler üzerinden, uygulama kullanım haklarını belirtebilirler.

[9] TED Android Uygulaması https://play.google.com/store/apps/details?id=com.ted.android
[10] EULA, https://en.wikipedia.org/wiki/End-user_license_agreement



Şekil 8: Ted Android Uygulaması - Kurulum Aşaması [11]

Uygulama cihaza kurulduktan sonra, kullanıcı isterse uygulamayı sisteminden kaldırabilir ve ya kurulum sırasında vermiş olduğu izinleri görebilir. Bu durum tamamen kullanıcının kontrolün de olan bir durumdur.

Şekil 9: Ted Android Uygulaması - Kurulum sırasında almış olduğu izinler

II. Erişim İzinleri Nelerdir?

Uygulamalarda belli başlı izin tipleri vardır. Bu izinler uygulamayı amacına uygun halde çalışmasını sağlar. Misal lokasyon tabanlı uygulama kullanacaksanız, sistemin bu altyapıyı sağlayan erişim iznine onay vermeniz gerekmektedir. Bu özelliğin geliştirme aşamasında belirtilmesi ve ona uygun kodlama yapılması gerekir. Erişim izinlerinde olabilecek en belirgin izin tipleri şu şekildedir;

- Telefonun durumunu ve kimliğini okuma,
- Fotoğraf ve video çekimi,

[11] TED Android Uygulaması, https://play.google.com/store/apps/details?id=com.ted.android

- Ses kaydetme,
- Yaklaşık yer (ağ tabanlı) tahmini,
- Hassas yer (GPS ve ağ tabanlı) tahmini,
- SD kart içeriğinin okunması, değiştirilmesi veya silinmesi işlemi,
- Cihazdaki hesaplara erişim,
- Hizmet yapılandırılması ve ya Sistem yönetimi,
- Tam ağ erişimi,
- İnternetten veri aktarımı,
- Ağ bağlantılarını görüntülenmesi,
- Bluetooth ayarlarına erişim,
- Bluetooth cihazlarıyla eşleşim,
- Titreşim ayarları,
- Telefonun uyku durumu,
- Ses ayarları,
- Senkronizasyon ayarları ve açıp kapama durumu

Kullanıcılar uygulama kurulum aşamasında erişim izinlerine karşı, zaman zaman değişik tepkiler gösterebilir. Örneğin sıklıkla kullanılan bir uygulama geçmiş dönemlerde, sadece ağ erişim izni isterken, bugün telefon rehberine de erişmek isteyebilir. Bu durum tamamen ihtiyaca ve geliştiricinin kendi kurgusuna dayanmaktadır. Geliştirici gelen taleplere göre kodlamasını ileriye götürmek ister. Kullanıcı ise, uygulamanın daha iyi bir sürüm ile çıkmasını bekler. Tamamen arz talep durumu bu konuyu açıklayabilir. Diğer bir deyişle, uygulamalar teknolojinin de gelişmesiyle daha ileri seviye kodlanmakta ve daha gelişmiş cihazlar üzerine kurulmayı beklemektedir. Aynı şekilde kullanıcılarda daha iyi bir fonksiyona sahip uygulamayı cihazında görmek ister. Önceleri eski sürümlerde, daha az erişim izni istenirken, günümüz cihazlarında bu durum katlanarak artımıştır. Haliyle kullanıcılarda bu durumu görmezden gelir ve sadece o uygulamayı kullanmak ister. Örneğin Whatsapp uygulaması pek çok erişim izni talep eder, ama kimse buna dikkat etmez. Sadece kullanımı ile ilgilenir. Geliştirici ise, kullanıcının bu ilgisi karşısında sürekli değişim ve gelişime giderek yeni ek özellikler eklemeye devam eder.

Android temelde ayrıcalıklı bir işletim sistemi'dir. Her uygulama kendi sanal makinesinde farklı bir sistem kimliği ile çalışır. Bu mekanizma, uygulamaları birbirinden ve sistemden ayrı tutar. Varsayılan olarak, bir uygulama, diğer uygulamaları, işletim sistemini veya kullanıcıyı olumsuz olarak etkileyebilecek herhangi bir işlemi gerçekleştiremez. Ek izin, yetenek ya da özellik elde etmek için, bir uygulamanın ihtiyaç duyduğu izinlerin “AndroidManifest.xml” dosyası

içerisinde belirtilmiş olması gerekmektedir. Uygulama kurulumunda kullanıcının vereceği izinler, öncesince "AndroidManifest.xml" dosyası içerisinde tanımlı halde bulunurlar. Ve kullanıcıya uygulamanın çalışma zamanı süresince başka kontrolde yaptırılmaz. [12] Örneğin uygulamanın internet'e erişimesi gerekiyorsa, INTERNET erişim izin tanımının bu xml dosyası içerisinde belirtilmiş olması gerekir. Erişim izninin verildiği manifest dosyası aşağıda görüldüğü gibidir;

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
 package="com.example.testapps.mytest">
…
<uses-permission android:name="android.permission.INTERNET" />
…
</manifest>
```

Android işletim sistemi içerisinde, erişim izin tipleri *4 farklı seviyede* incelenmektedir. Bu erişim izinleri seviyelerine göre farklı yetki ve sorumluluklar barındırır.

i) Normal: Bu izin tipi varsayılan ve düşük değerde bir izin tipidir. Uygulamanın diğer uygulamalara, sisteme veya kullanıcıya yönelik özelliklere çok az riskle erişmesini sağlar. Kullanıcının, uygulama kurulum aşamasında açık onayını istemeden sistem tarafından otomatik olarak da izin verilebilir. En yaygın izinlerin bazıları aşağıda verilmiştir.
* Veri bağlantısı kontrolü ve değiştirilmesi: Şebeke durumu, Wi-Fi durumu, Bluetooth ve İnternet bağlantı durumu ve kontrol yetkisi bu seviye bir izin tipidir.

android.permission.INTERNET
android.permission.CHANGE_WIFI_STATE
android.permission.BLUETHOOTH
android.permission.CHANGE_NETWORK_STATE
android.permission.ACCESS_WIFI_STATE

[12] Chan, P. P., Hui, L. C., & Yiu, S. M. (2012, April). Droidchecker: analyzing android applications for capability leak. In Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks (pp. 125-136). ACM.

ii) Tehliheli: Bu izin tipi, uygulamanın kullanıcı verilerine erişmesine izin veren veya sistem / diğer uygulamaları etkileyen izinlerdir. Bu izin tipine sahip uygulamalar, potansiyel olarak hassas bazı bilgilere erişme veya aygıtta işlem yapma yetkisine sahiptir.

* Kişisel verilere erişim, sms gönderimi, şebeke araması, lokasyon durumu veya kullanıcı hesaplarına erişim bu izin tipi ile yapılacak işlemlerden biridir.

Bu seviyede kullanılabilecek en yaygın izin tipleri,

android.permission.CAMERA
android.permission.CELL_PHONE
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.SEND_SMS
android.permission.RECEIVE_SMS
android.permission.GET_ACCOUNTS
android.permission.READ_PHONE_STATE
android.permission.ACCESS_FINE_LOCATION
android.permission.ACCESS_COARSE_LOCATION

iii) İmza Korumalı: Her uygulama farklı bir imza ile üretilir ve yüklenmek üzere uygulama marketine bırakılır. Kullanıcılar uygulamaları cihazlarına yüklemeye başladıkları anda, sistem cihaz içerisinde aynı imzaya sahip başka bir uygulama var mı, bu nu kontrol eder. Aynı şekilde, cihazlarda üretim aşamasında varsayılan sistem uygulamaları ile piyasaya çıkar ve önceden yüklenmiş uygulamaları kullanıcıların hazır olarak kullanmasını kolaylaştırır. Bu bağlamda, aynı geliştirici ekibinden ve şirket tarafından üretilen uygulamalar, cihazlarda önceden yüklenmiş olarak gelebilir. Yani, sonradan kurulacak olan uygulama, sistemde hazır halde gelen aynı sahip başka bir uygulama ile eşleşirse erişim izni alınmadan bu atlanabilir.

* Görev yöneticisi, hesap yöneticisi, cihaz giriş araç ve denetleyicileri veya servis yöneticileri bu izin tipi ile alınabilecek aksiyonlardan biridir.

Bu seviyede kullanılabilecek en yaygın izin tipleri,
android.permission.ACCOUNT_MANAGER
android.permission.DEVICE_POWER

android.permission.DIAGNOSTIC
android.permission.REMOVE_TASKS
android.permission.SET_INPUT_CALIBRATION
android.permission.SET_KEYBOARD_LAYOUT

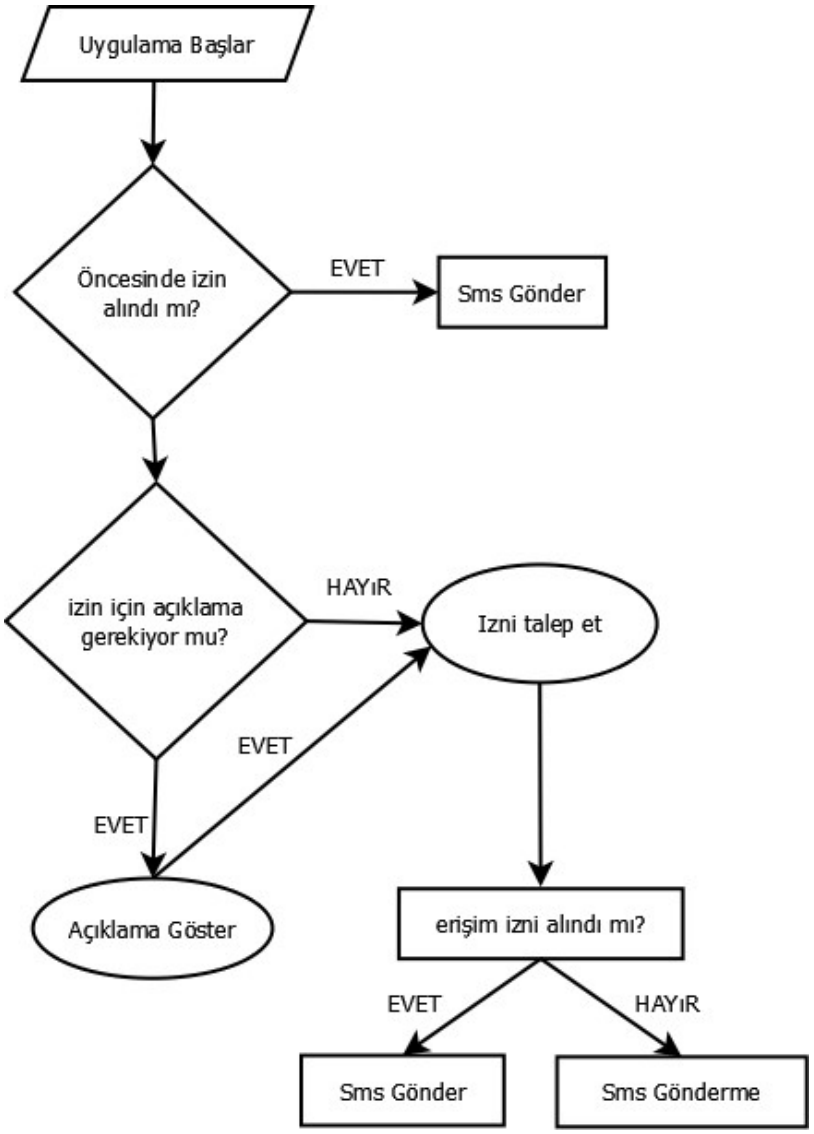
iv) İmza/Sistem Korumalı: Bu izin tipi, imza korumalı izin tipi ile aynıdır. Ancak, sistem kurulumda otomatik olarak izinleri alır. Dikkat edilmesi gereken bir izin tipidir. Yalnızca aygıt üreticileri tarafından kullanılmak üzere tasarlanmıştır.
* Kullanıcı yönetimi, uygulama paket doğrulama, seri bağlantı (USB, Media cihazları) kontrolü, cihazı açma, cihazı kapama ve yeniden başlatabilme kontrolleri bu izin tipi ile yapılabilecek aksiyonlardır.
Bu seviyede kullanılabilecek en yaygın izin tipleri şunlardır,

android.permission.REBOOT
android.permission.PACKAGE_VERIFICATION_AGENT
android.permission.MANAGE_USB
android.permission.MANAGE_USERS
android.permission.ACCESS_MTP
android.permission.ACCESS_NETWORK_CONDITIONS

Bu izinlerden yola çıkarak basit bir sms gönderim uygulamasını ele alalım. Uygulamanın kurulum aşamasında izleyeceği yol şu şekilde olacaktır:

- Uygulama başlar. Uygulama için öncesinde erişim izin tanımlamaları manifest dosyasında geliştirici tarafından yapılmıştır.
- Eğer daha önceden kullanıcıdan, sms gönderimi için izin alındı ise, izin talep ekranı atlanacak ve sadece sms gönderim kısmına geçilecektir.
- Eğer izin alınmadıysa, izin alınması gereken erişim tipine ilişkin bilgilendirme mesaj ekranı gelecektir. Kullanıcıdan erişim izni almadan önce, gelecek olan bu ekranda, verilecek olan bu iznin tüm koşulları kabul ediyorum ya da reddediyorum mantığına dayanan bir ara ekran gelecektir. Kullanıcı kabul ederse, bir sonraki aşamada erişim izni onay ekranı gelecektir.

- Kullanıcı eğer uygulamanın talep etmiş olduğu bu erişim iznine onay verirse, sms gönderim işlemi başlayacaktır. Eğer vermez ise, sms gönderilemeyecek ve işlem yarıda kalacaktır.



Şekil 10: Android izin akış modeli [13]

Her mobil uygulama kurulumu sırasında, bu işlem sıklıkla tekrarlanır. Erişim izinleri bu akışa göre uygulamanın kullanım seyirini değiştirir. Bu izinler arasında en çok kullanılan hiç kuşkusuz ağ iletişimidir. Çoğu uygulama internet üzerinden veri alış verişi yapmak ve uygulamayı aktif tutmak ister. Yine Android

[13] Orjinal çizim için bknz. http://www.androidrey.com/run-time-permission-request-in-marshmallow

işletim sistemi üzerinden örnek vericek olursak, Google Play markette yer alan uygulamaların erişim izinlerini ve yüzdelik dilimlerini aşağıdaki tabloda görülebilir.

Kullanım Oranı(%)	İstenen izin tipi
83	Tam ağ erişimi
69	Ağ bağlantılarını görüntüle
54	Korunan belleğe erişim sınama
54	USB depolama biriminin içeriğini değiştirme veya silme
35	Telefon durumunu ve kimliğini okuma
27	Cihazın uyku halini önleme
24	Konum bilgisi (GPS ve Ağ tabanlı)
23	Kablosuz ağ bağlantılarını görüntüle
21	Titreşim kontrolü
21	Konum yer tahmini (Ağ tabanlı)

Tablo 1: En çok kullanılan Android uygulama izinleri [14]

Aşağıdaki tabloda ise popüler sayılabilecek uygulamalar yer almaktadır. En belirgin özelliğini ve hangi izin türü üzerinden hangi işlemi gerçekletirdiği görülebilir.

Uygulamalar	Erişim İzinleri	Amacı
Gmail	Telefon Rehberi	Uygulama içerisinde e-posta gönderim öncesinde, kişinin adres defterine erişmek istemesi
Foursquare	Lokasyon	Kişinin bağlı bulunduğu konumu bilmek istemesi.

Tablo 2: Popüler uygulamaların istedikleri izinler ve görevleri [15]

a) Ağ iletişimi

Bu izin tipi uygulamayı ağ bağlantısı üzerinden veri alış-verişinde bulunmasını sağlar. Aynı zamanda en çok kullanılan Android izin tipidir. Uygulamanın ağ bağlantısı üzerinden internet'e çıkabilmesi için bu erişimin izninin kabul edilmesi

[14] Lenhart, A. (2009). Teens and mobile phones over the past five years: Pew Internet looks back.
[15] Orijinal çizim için bknz. Tan, J., Nguyen, K., Theodorides, M., Negrón-Arroyo, H., Thompson, C., Egelman, S., & Wagner, D. (2014, April). The effect of developer-specified explanations for permission requests on smartphone user behavior. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 91-100). ACM.

gerekir. Uygulama kendi güncelliğini korumak, iletişimin sürekliliğini sağlamak ve veri aktarımını icra edebilemek için bu erişim iznine ihtiyaç duyar. Ve bu erişim izninin kabulu sonrasında bağlı bulunduğu servis sağlayıcı ile iletişim halinde bulunmaya başlar. Kullanıcı farkında olmasa dahi veriler bu noktaya belli zaman aralıklarında gidip gelmeye devam eder.

Erişim izni verildikten sonra, geliştiricinin oluşturabileceği backdoor denen zararlı olabilecek geçitlere imkân tanımışta olabilir. Yani, masum gibi görülen bir izin tipi mobil casusların ve veri hırsızlarının uzaktan sizi yönetmesine imkân tanıyabilir. Sizi kontrol edebilecekleri gibi, bilgilerinizi belli zaman aralıklarında karşı tarafa iletmesini de sağlayabilirler. En çok suistimal edilen izin tipidir.

b) Depolama İzinleri

Bu izne sahip uygulamalar, mobil cihazın tüm bellek tiplerini veya veri (SD) kartını yönetebilir, içeriğini silebilir, okuma, yazma veya silmesine olanak tanır. Uygulama bu izin tipi ile çalıştığı anda, geliştiriciye cihazın belleğine erişim için yetki vermiş olur. Uygulama sistem loglarını, kullanıcı kayıtlarını ya da veri okuma-yazma-silme işlemlerini kullanıcının vermiş olduğu izin sonrasında bellek üzerinde rahatça yürütebilir. Yalnız kullanıcının atladığı bir durum vardır; geliştirici isterse bilgileri işler ve bir kopyasına kendisine de gönderebilir. Veri çalma yazılımları ile SD kart üzerindeki veriler, internet üzerinden istem dışı olarak diğer platformlara aktarılabilir. Öyleki, kullanıcı vermiş olduğu bu izin ile bir bakıma cihazının belleğini paylaşıma açmış da oluyor. Yakın zamanda yaşanan iPhone iCloud sızıntısı bu durumun en çarpıcı örneğidir[16]. Kullanıcıların özel fotoğrafları, bu iznin dikkatsizce kullanılması ile ortaya çıkmıştır.

Kullanıcıların iCloud hesaplarının ele geçirilmesi ile birçok ünlü ismin müstehcen fotoğrafları internette yayınlaşmıştı. Hacker olarak tanımlanan kişi ya da kişilerin, iPhone mobil cihaz üzerinde kurulu halde bulunan “Find my iPhone” uygulamasındaki bir açıktan faydalanarak, kullanıcıların özel bilgilerini internete sızdırıldığı ve bu açığı Brute-Force denen kaba kuvvet saldırısı olarak da adlandırılan saldırı tipi ile gerçekleştirdiği öğrenilmiştir.[17] Kullanılan yöntem, doğru şifreyi bulana kadar farklı birleşim üzerinden denemeye devam eden

[16] Peterson, E. Y. A., & Warrick, J. (2014). Leaks of nude celebrity photos raise concerns about security of the cloud.
[17] Park, Y. (2016). Up in the Cloud.

tahmine dayalı bir yöntemdir. Bu yol ile birçok ünlü kişinin kişisel verilerine erişilmiş ve sanal ortamda paylaşılmıştır. Sorun gündeme geldikten sonra saldırıyı gerçekleştiren kişi birkaç yıl sonra yakalanmış ve suçunu itiraf etmiştir.[18]

c) Konum Bilgisi

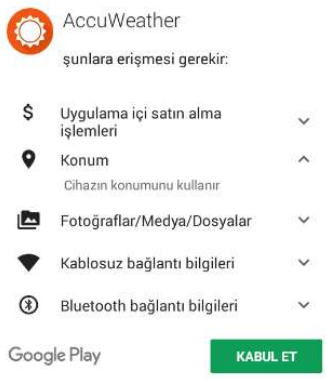
Eğer konum tabanlı bir uygulama kullanıyorsanız, bu erişim tipini onaylamış olabilirsiniz. Şebeke yani genel konumlandırma ve hassas (GPS) konum sistemi olarak iki kısımda incelenebilir.

Şebeke tabanlı konumlamalarda, cihazın lokasyonunun belirlenebilmesi için, bağlı bulunduğu yerde hücresel ağ veritabanın konum kaynaklarına erişmesi gerekir. Zararlı olabilecek uygulamalar, bu işlevi cihazın bulunduğu yeri yaklaşık olarak olarak belirlemek için kullanılır.

Hassas (GPS) tabanlı konumlandırma sisteminde ise, cihazın bulunduğu nokta üzerinden küresel konumlandırma sistemi gibi hassas konum sayılabilecek kaynaklara erişim sağlayama çalışılır. Bu erişim iznine sahip uygulamalar, cihazın bulunduğu noktayı belirleyerek spam mesajlar gönderebilir ya da cihazın pil tuketimini hızlandırabilir.

Lokasyon olarak kesin koordinat bilgisinin herkes tarafından bilinmesi riskli bir durumdur. Kişinin bilgi ve hareketlerini takip etmeyi sağlayan bu erişim tipi, kullanıcı açısından büyük bir güvenlik riski arz edebilir. Ayrıca gündelik hayatta da kullanılan bu erişim tipi ile uzaktaki bir yakınınıza olan mesafeyi, acil bir durumda size en yakın olan noktayı (eczane gibi) ya da bulunduğu konuma ait hava sıcaklığının belirlenmesini sağlayabilir. Örneğin AccuWeather uygulaması hava tahminleri yapan bir sistem üzerine kurulmuştur. Uygulama mobil cihaza kurulmadan önce, kullanıcıdan konum bilgisine erişmek istediğini belirtir. Uygulamaya erişim izni verildikten sonra, bir bakıma konum bilgisi de geliştirici ile paylaşılmış sayılır.

[18] Pennsylvania Man Charged with Hacking Apple and Google E-Mail Accounts Belonging to More Than 100 People, Mostly Celebrities (https://www.justice.gov/usao-cdca/pr/pennsylvania-man-charged-hacking-apple-and-google-e-mail-accounts-belonging-more-100)



Şekil 11: AccuWeather Android Uygulaması [19]

d) Telefonun Kimliği ve Kişilere Erişim

En önemli erişim izinlerinden biridir. Bu izne sahip uygulamalar, cihaz üzerinden kullanıcının kişisel iletişim bilgilerini okuyabilir ya da yazabilir, yeni bir hesap oluşturabilir, mevcut hesapları görüntüleyebilir ve bu bilgileri internet üzerinden başka bir veritabana aktarabilir.

Her kullanıcı sahip olduğu akıllı cihazlar üzerinde bir kimlik taşır. Bu kimlik kişinin çağrı bilgilerini, görüşlerini ve iletişim kurduğu kişi ya da kişileri barındaran özel bir veridir. Kullanıcı bu izni uygulamaya sağladıktan sonra, geliştirici kişi ya da kişiler uygulamanın içerisinde bu özel verileri kullanarak değişik yapma hakkına sahip olur. Örneğin iletişim uygulamalarında bu izin sıkça kullanılır. Skype bu örneğe uygundur. Kullanıcı karşı kullanıcı ile uygulama üzerinden görüşmeye başlamadan önce, uygulamanın bu kişiye dair bazı bilgilere erişiyor olması gerekiyor, telefon numarası gibi.

Uygulama açıldığı anda tam yetki ile donatıldığı için, kullanıcıya sormadan adres defterini inceler, analiz eder ve kullanıcının iletişim kurabilmesi için onayına sunar. Ve uygulama kişiden aldığı yönlendirmeler ile çalışmasına devam eder.

3. Mobil Platformlarda Kullanıcı Deneyimleri

Mobil uygulamalar, ihtiyaca göre farklı platformlarda farklı modellerle geliştirilip kullanıcıya sunulabilir. Özellikle Android platformu üzerinden geliştirilebilen uygulamalar; geliştiriciyi, reklam ağını ve hatta yazılım firmalarını etkilemeyi başarmıştır. Kullanıcılar ise üretilen uygulamaları farkında olmadan

[19] Android AccuWeather Uygulaması, https://play.google.com/store/apps/details?id=com.accuweather.android

kullanmaya devam ederler. Fakat arka planda ise bilinmeyen bir karışıklık vardır. Belirsiz sektör kuralları, hiç bir birimi denetlemeyen yazılım pazarı, uygulama izinlerini kötüye kullanma, gizli bilgilere erişme, gereksiz mesajların çoğalması ve ya kötü amaçlı eklentilerle yapılan kesintiler gibi problemlerde beraberinde oluşmaktadır.

Örneğin telefona bir kaç uygulama indirip kurabilen kullanıcı, mobil ekranında belli belirsiz reklam pencereleri oluştuğunu ve spam mesajları verdiğini görür. Bu açılır pencerelerin her gün birden fazla olmak üzere, diğer mesajlaşma uygulamalarının daha ilk açılışında da belirdiğini söyler. En kötüsü de, bu reklam pencereleri üzerine tıklandığı zaman, herhangi bir pencere görüntülenmeden ortadan kalktığını belirtir. Çaresiz kaldığı için bütün uygulama listesini temizlediğini ifade eder. Kurulum sırasına göre tek tek uygulamaları kaldırır ve nihayetinde bir korsan kuş vurma oyununu kaldırdığında telefonun bu virüsten kurtulduğunu fark eder.

Bir başka kullanıcı ise, farklı olarak uygulama kurulumu ve kullanımı sürecinde izin isteklerine Evet ya da Hayır gibi seçimlerle cevap veriyor. Ona göre, kullanım aşamasında internet verileri, mesajlar, telefon rehberi gibi izin yetkisi talep eden özellikleri bu şekilde kısıtlayarak, cihazını kontrol altına almak istemiştir.

Kimi zaman bu da yeterli olmuyor. Bazı uygulamalar vardır ki daha da öteye giderek arkaplanda siz erişim izni vermesiniz dahi çalışmaya devam eder ve kullanıcı bundan haberdar değildir.

I. Netiquette Nedir?

Netiquette sözcüğü İnternet ve görgü kurallarının yani "etiquette" kelimesinin bir birleşimidir. Bir bakıma İnternet etiketi'de denebilir. Netiquette, günlük yaşantımızda doğru şekilde davranmak için izlediğimiz kurallar dizisidir. [20] İletişim etiği olarak da söylenebilir. Sohbet, mesaj gönderme, blog yazma ve haber ya da web sitesinde yorum yazma, sosyal ortamlarda durum güncelleme gibi internette iletişiminde sıklıkla kullanılan "nezaket" durumları olarak yorumlanabilir. İnternetteki iletişim etiği esasen dürüst olmak, iyi sözcükler kullanmak, samimi olmak ve açıkça anlaşılır bir şekilde konuşmak gibi günlük hayatta "gerçek dünyada" iletişim kurma etiği ile aynıdır. Interaktif ortamda

[20] Shea, V. ,What is Netiquette, http://www.albion.com/netiquette/introduction.html

etkileşim kurarken 10 kural sunulur. Asıl nokta, gerçek dünyadaki iletişim etiği ile aynıdır; zarar vermeyin, rahatsız etmeyin, etkili konuşun, yanlış yaparsanız özür dilemekten çekinmeyin vs gibi. Çünkü mesajın ucunda her zaman gerçek bir insan vardır.

a) *İnsanı hatırlamak*

İnternet kullanıcıları arasında daha hoşgörülü ve saygılı davranışları teşvik etmek amacıyla konulan bu kuraldır.[21] Unutulmaması gereken bir durum; e-postayı veya yayınları okuyan kişi duygusu olan bir insandır; rahatsız edilebilir veya zarar görebilir. Bu yüzden başkalarına zarar vermek kötü bir davranış olabilir. Utanç verici e-postalar veya mesaj gönderilmemesi en uygun davranış biçimidir. Bu durumu mobil yazılım için düşünürsek, kişinin her zaman kendisini karşı tarafın yerine koyması gerekmektedir. Zararlı yazılımlar geliştirerek kullanıcılara zarar vermek geliştirici için eğlenceli bir durum olabilir. Ama kullanıcılara verebileceği zararlar onları mutsuzluğa doğru itecektir. Bu da hoş bir durum değildir.

b) *Gerçek hayatta sürdürülen benzer davranışlara bağlı kalmak*

Başkalarının görüşlerine saygı gösterilmesi ve yasanın ihlal edilmesi gibi gerçek yaşamdaki durumlar, İnternet iletişim etik kuralları ile aynı ahlaki yasal standartlar içerisindedir. Gerçek dünyadaki insanların büyük çoğunluğu yasalara saygılıdır ve uymaya özen gösterir. Eğer sanal dünyada yasadışı bir şey yapmaya çalışırsanız, şansınız yoktur ve kuralları çiğnemiz olursunuz

c) *Siber dünya'da nerede olduğunun öğrenilmesi*

Sanal dünyada tartışmaya atlamadan önce neye, hangi olaya karışıldığının iyice bilinmesi gerekmektedir. Yeni bir alan içerisine girildiğinde, kişinin etrafını iyice bir göz atması onun yararına olacaktır. Sohbet etmek, yazışmak veya tartışma içerisine girmeden önce kısa bir süre dinlenilmesi ve ortamın keşfedilmesi önerilmektedir. Hâlihazırda ortamda bulunan diğer kişilerin nasıl davrandıklarını izlenmesi ve kendisini o ortama uygun gördüğü takdirde katılması her zaman iyi bir durumdur. Öyleki sanal dünyada yapılan tartışmaların birçoğunda insan unsuruna sahip nesneler bulmak, anlaması kadar zordur.

---

[21] Nazlı Alkan, Hakemli Yazılar Kütüphanecinin Felsefi Düşünme Eyleminin Önemi ve Etkileri, Türk Kütüphaneciliği 24, 4 (2010), 596-643

d) *Başkalarının zamanına ve bant genişliğine saygı gösterilmesi*

Bant genişliği, bilgisayarları birbirine bağlayan kablo ve ağlarının taşıma kapasitesidir. Yani, iletişimin kapasitesini belirler. En ileri teknolojiye sahip kablolar bile taşıyabilecekleri bilginin bir sınırına sahiptir, bu nedenle sanal alan içerisinde fiziksel sınırların olabileceği gerçeği unutulmamalıdır. Gönderilen e-posta iletisinin veya tartışma grubunda yazılmış bir mesajın, okunma ve cevap verme süresi bulunmaktadır. Günümüzde her birey yogun ve hareketli bir yaşama sahiptir. Saçma ve gereksiz e-postaları veya tartışma ortamındaki yayınlarını okumak veya cevaplamak için zamana sahip değiller. Sanal bir dünya yer alan her kullanıcı, yazmış olduğu kelimelerini düzgün seçmeli ve okurken de harcanan zamanın boşa gitmediğinden emin olmalıdır.

e) *İyi görünmek ve mantıklı olmak*

Sanal ortamda bir içerik paylaşılmadan önce, dilbilgisi ve yazım denetiminin kontrol edilmesi gerekmektedir. Ne dediğinin anlaşılması, önceden bilinmesi ve mantıklı olunması çok önemlidir. İçeriğin beğenilmesi ve hoşlanılması, yazının kalitesiyle değerlendirilir.

f) *Bilginin paylaşılması*

Internet ve bilgi teknolojilerinin asıl kurulma amacı ve gelişmesindeki etken, bilginin paylaşılmasıdır. Eğer cevaplanmamış bir soru hakkında bilgi sahibi iseniz, bunu diğerleri ile paylaşmak en büyük atılımdır. En güncel bilgi hakkında sorular sormak, cevaplar aramak ve bunların diğerleri ile paylaşılması bilginin gelişmesini sağlar.

g) *Tepkilerin kontrol altında tutulması*

Internet ortamında duygularının kontrol edilmesi gerekmektedir. Öfke dolu bir içerik bir başkasında gönderilmeden önce dikat edilmelidir. Tansiyonu yükseltecek yorumlarda ve yazılarda bulunulmaması gerekmektedir. Eğer yanılıyor veya başkası durumdan rahatsız oluyorsa özür dilemekten asla çekinilmemesi gerekmektedir.

h) *Başkalarının mahremiyetine saygı gösterilmesi*

Başkalarının mahremiyetine saygı gösterilmesi en doğru davranıştır. E-posta iletileri, sosyal platformlardaki yazışmalar, özel mesajlar veya diğer kişilerden gelen özel bilgileri okumak ya da paylaşmak hiçde hoş bir

durum değildir. Bilginin yanlış kişilerin eline geçmesi utanç verici bir durum olabileceği gibi, iş kaybı gibi ciddi boyutlara da ulaşabilir.

i) *Gücün kötüye kullanılmaması*

Sanal ortamda gücün kötüye kullanması çok yanlış bir harekettir. Sahip olunan güç ne kadar büyükse, kullanmak o kadar önemlidir. Ve ne kadar çok kullanılırsa, önemide bir okadar artar. Diğerlerinden daha fazla şey bilmek, onlardan yararlanmak hakkını vermez. Forum veya sohbet ortamını yöneten kişi ya da kişiler bu duruma örnektir.

j) *Başkalarının hatalarının bağışlanması*

Sanal ortamda herkes aynı tecrübeye sahip olamayacağı gibi yukarıda sıralı diğer kuralları da bilmek zorunda değildir. Saçma sorular, uzun yanıtlar, dilbilgisi hatalarının olduğu anlamsız cümleler, bunlar sıkça görülür ve eklenmeye de devam eder. Eğer paylaşılan bir içerikte hata görülüyorsa, bunu herkese açık bir forumda belirtmek yerine özel bir mesaj veya e-posta ile bildirilmesi gerekmektedir.

II. Oyun ve Uygulamaların Sınıflandırılması

Uygulama mağazasındaki yazılımlar, belli kurallar çerçevesinde değerlendirme sistemleri üzerinden etkilenmiştir. Bu sistem kullanıcıların uygulamaya ne derece güvenebileceğini, hedef kitlesini ya da yaş aralığını belirtir.

Şu anda uygulama mağazalarında kullanılmak üzere, iki temel uluslararası uygulama yönetim yöntemi bulunmaktadır. Bunlardan ilki sansür sistemidir. Uygulama gözden geçirilmeden önce, yönetmelik hükümlerince ilgili devlet dairelerine atıfta bulunuyor mu ya da yasadışı içerik barındırıyor mu, bunların incelenmesidir. Diğer ise listeleme yani sınıflandırma işlemidir. Sınıflandırma işlemi ülkeden ülkeye değişebileceği gibi, içerik türü ve kitlesine göre de değişebilir. Bunun bir örneği olarak, Amerika Birleşik Devletleri'nin oyun ve uygulamalara karşı tutumu çok açıktır. ABD çevrimiçi oyun ve uygulama endüstrisinde kendisini sürekli geliştirmekdedir. Korsanla mücadele politikaları çıkarma, kullanıcıların çıkarlarını koruma ve şiddet içeren içerik ya da yazılımlar ile mücadele edebilmek adına derecelendirme sistemini güçlendirme gibi işlemlerde bulunabilir. Bölgelere incelenmek istendiği zaman ise, farklı ülkelerde farklı derecelendirme sistemi de görmek mümkündür. Bunun bir örneği, Google Play uygulama marketinde görülebilir. Google uygulama marketinde farklı

derecelendirme sistemi kullandığı gibi ülkere göre de derecelendirme sistemlerini değiştirebiliyor. Mesela, Avrupa'da PEGI sistemini kullanırken, Kuzey Amerika'da ESRB sistemi kulanmaktadır. Bu durum bağlı olduğu ülkenin de kabul ettiği sistemle alakalıdır. Google Earth Android uygulamasında bunun bir örmeğini görebiliriz.

Şekil 12 İçerik derecelendirme sisteminin bölgere göre değişmesi [22]

a. ESRB

ESRB, 1994 yılında Entertainment Software Association (ESA) tarafından kurulan ve kar amacı gütmeyen bağımsız bir kuruluştur. [23] Dilimizde, Eğlence Yazılım Derneği olarak da söylenmektedir. Misyonu, eğlence yazılımı endüstrisinin desteğiyle etkileşimli eğlence yazılımı ürünleri için standart bir derecelendirme sistemi geliştirmektir. Kuzey Amerika'dan sorumludur. ESRB derecelendirmesi, kullanıcıları, özellikle ebeveynleri için satın oyun veya yazılımların satın alım sırasında uygun olup olmadığını belirleyebilmelerini sağlamak için

[22] Orijinal çizim için bknz. https://andro4all.com/2016/07/pegi-edad-google-play-aplicaciones-ninos

[23] Robertson, K. (2008). An analysis of the video game regulation harmonization effort in the european union and its trans-atlantic chilling effect on constitutionally protected expression. BC Intell. Prop. & Tech. F., 2008, 90802-102902.

kullanılmaktadır. Tüketiciye hangi ürünün satın alınmasını söylemek yerine, yazılım içeriğinin uygun olduğu yaşı söylemesidir.

Bu sistem, tüketicilere, özellikle ebeveynlere yazılım ve video oyunlarının yaşa uygunluğu ve içeriği hakkında kısa ve tarafsız bir rehberlik sunar, uygun gördükleri oyunlarla ilgili açık ve net kararlar verebilmelerini sağlamak üzere tasarlanmıştır. Böylece tüketici, oyun satın alındığı sırada oyunun kendisi ya da ailesi için uygun olup olmadığını belirleyebilir.

ESRB derecelendirme sistemi 3 kategoride incelenmektedir. [24]

- Derelendirme kategorisi: Önerilen yaş aralığını belirtir.
- İçerik tanımlayıcı: belirli bir derecelendirmeye neden olabilecek ya da ilgi çekici olabilecek içeriği belirtmektedir.
- İnteraktif unsurlar: uygulama sırasında alınabilecek izinleri belirtir.

Derelendirme kategorisi'nde hiyerarşik olarak farklı kademelerde logolar kullanır ve bunlar direk kullanıcıların yaş aralığı ile ilgilidir.

(+3) 3 yaş ve üzeri
Küçük çocuklar için tasarlanmıştır.
Ebeveyinlerin uygun bulmadığı içerikleri içermez.

(+6) 6 yaş ve üzeri
İçerik genellikle her yaş için uygundur.
Minimum karikatür, fantezi veya hafif şiddet
ve / veya hafif dili nadiren kullanabilir.

(+10) 10 yaş ve üzeri
Daha fazla çizgi film, fantezi veya hafif şiddet,
hafif dilli ve / veya minimal önermeli temalar içerebilir.

[24] ESRB RATINGS GUIDE, https://www.esrb.org/ratings/ratings_guide.aspx

(+13) 13 yaş ve üzeri

Şiddet, düşünce temaları, kaba mizah, minimal kan,
ve / veya kumar oynamama temaları içerebilir.

(+17) 17 yaş ve üzeri

İçerik, genellikle 17 yaş ve üstü için uygundur.
Şiddet, kan ve / veya cinsellik içerebilir.

(+18) 18 yaş ve üzeri

Yalnızca 18 yaş ve üstü yetişkinler için uygun içerik.
Şiddet, cinsellik ve / veya gerçek para ile
kumar oynanan temalar içerebilir.

Derecelendirme bekleniyor

Ürün ve yazılım onayı için ESRB'ye bilgi gönderildi
ve kendilerinden son derecelendirme bekleniyor.
Bir video oyunuyla ilgili reklam, pazarlama ve tanıtım
materyallerinde gösterilebilir.

İçerik tanımlayıcı unsurlar ise derecelendirmenin nedeni ve içeriği belirtir. Alkollü içecekler, kan'ı tavsir edebilen görüntüler, şiddet, çizgi roman, kaba mizah, uyuşturucu, dil, hakaret, cinsellik, tütün ve ilaç kullanımı gibi konular yer alır. İnteraktif unsurlar ise uygulama sırasında alınabilecek bilgi ve izinleri içermektedir.

Lokasyon paylaşımı, kullanıcılar arasında etkileşim (sosyal ağlarda paylaşım veya diğerleri ile iletişim kurabilme durumu), dijital ürün satın alımı ya da ürünün internete erişim iznin istemedir.

b. PEGI

PEGI (Pan European Game Information) 2003 yılında pek çok ülke standartlarına göre sınıflandırarak yerini almış ve Avrupanın birçok ülkesinde

kullanılan derecelendirme sistemidir. [25] Yasal bir yetkisi yoktur. Avrupa İnteraktif Yazılım Birliği tarafından geliştirilmiştir. "PEGI sınıflandırması, oyunun zorluk derecesini değil; hangi yaşa uygun olduğunu tarif etmektedir." [26] "PEGI sistemi, formatı veya oyun platformu ne olursa olsun Avrupa Ekonomik Alanı içinde sistemin standartlarını imza eden bütün şirketlerce satılan veya dağıtımı yapılan bütün interaktif yazılımlara, video oyunlarına ve bilgisayar oyunlarına uygulanır." [27] Üç önemli oyun üreticisi (Microsoft, Sony ve Nintendo) ve diğer birçok Avrupalı yayıncı firma ve geliştirici tarafından desteklenmiştir. Tasarım şirketi desteği. PEGI iki katmanlı bir yapı kullanır; biri, +3, +7, +12, +16 ve +18 yaş üzeri durumları desteklemektedir. İkincisi ise, ürünün içeriği ile ilgili olabilecek; şiddet cinsellik, korku, küfür, ayrımcılık ve benzeri ipuçlarının ürün ambalajı içerisinde tanımlayıcı bilgi olarak yer vermesidir.

(+3) 3 yaş ve üzeri
Bu seviye, tüm yaş grupların için uygun kabul edilir. Ebeveynin uygunsuz olduğunu düşündüğü herhangi bir içeriği barındırmamaktadır.

(+7) 7 yaş ve üzeri
Normalde 3 yaş ve üzeri olarak değerlendirilen, ancak az da olsa şiddet ya da korku içeren temalar bu seviyede görülebilir.

(+12) 12 yaş ve üzeri
Grafik olmayan gerçek hayattaki karakterlere (insan, hayvan) yönelik şiddet uygulanması, biraz cinsellik temasının olması ve küfür olmayan ama sert bir dil kullanılması bu seviye de görülebilir.

(+16) 16 yaş ve üzeri
Çıplaklık ve şiddet temasının gerçek hayat ile birebir aynı olması, aşırı kötü dil kullanımı, uyuşturucu, suç faaliyetleri, tütün ve alkol kullanımının olduğunu belirtir.

(+18) 18 yaş ve üzeri
Yetşkin sınıfına girer. Şiddet temasının en üst seviyede olduğunu belirtir Uyuşturucu, kumar, aşırı kötü dil kullanımı, cinsellik ve şiddet kullanımı bu seviyede görülür.

[25] What is PEGI? http://www.pegi.info/en/index/id/28/
[26] Gülbin Ayşı ATEŞ (2011). İletişim Alanında Çocuklara İlişkin Ulusal ve Uluslararası Hukuki Düzenlemelerin Değerlendirilmesi
[27] Özhan, S. (2011). Dijital Oyunlarda Değerlendirme ve Sınıflandırma Sistemleri ve Türkiye Açısından Öneriler. Sosyal Politika Çalışmaları Dergisi, 25(25).

Ayrıca, PEGI sınıflandırma yaparken kullandığı ölçütleri şu şekilde sıralamıştır,

- Şiddet
- Ayrımcılık
- Cinsellik ya da çıplaklık
- Uyuşturucu madde
- Korku
- Kaba, cinsel içerikli ya da aşırı kötü dil kullanımı
- Kumar

Bu bilgiler uygulama marketi üzerinde tanımlayıcı bilgi olarak yer almaktadır. Kullanıcılar uygulamaları satın alınmadan ya da cihazlarına kurmadan önce kendi güvenliğini korumak adına bu bilgilere dikkat etmeleri gerekmektedir.

4. Aşırıya Kaçılan Uygulama Erişim İstekleri

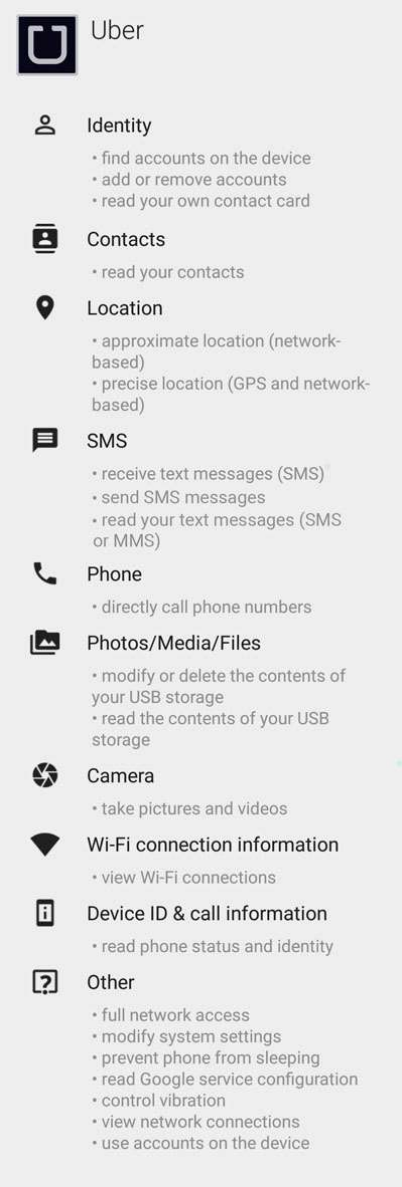
Çok sayıda kullanıcı bazı uygulamaları kurduğu sırada değişik isteklerle karşılaşabilmektedir. Örneğin bir gıda uygulamasının konum bilginize erişim istemesi dışında, SD card okuma/silme veya telefon rehberi okuma gibi izin istekleri olabilir. Eğer onaylamazsanız, uygulamayı yükleyemez ya da kullanamazsınız. Peki, bu alınan aksiyon sonucunda telefon gerçekten sizin kontrolünüz dâhilinde bir cihaz mıdır?

Geliştiriciler, uygulama geliştirme evresinde farklı aksiyonları sağlayabilen izinlerde ekleyebilir. Siz uygulamayı kurmak ve biran önce denemek isterken bu durumu göz ardı etmiş olabilirsiniz. Mesela, el feneri uygulaması sizden telefon rehberine de erişimek isteyebilir. Ama siz, kurulum aşamasında sadece "Evet" onayını vererek atlamış oluyorsunuz. Mevcut teknik yöntemler ile uygulamanın kurulu olduğu cihaz kullanıcı farkında olmadan kontrol edilebilir hale gelebilir ve mümkündür. Bu şekilde uygulamanın kurulu olduğu cihaza ait, internet, kısa mesaj ve telefon rehberi gibi kayıtlara erişmek bir geliştirici için kolay hale gelir.

Ne yazık ki, "izin isteklerinde aşırıya gidilmesi" gerçeği uygulamalarda halen görülmekte olan bir sorundur. Uygulama yöneticileri, reklam verenler ve yazılım geliştiriciler kullanıcıların gizli bilgilerini kötüye kullanabilecekleri gibi arkaplanda çalışan eklentiler ile de bu durumun sürekliliğini sağlayabilirler.

Mesela, kullanıcı işi bittikten sonra kullandığı uygulamayı kapatmak isteyebilir. Bu işlem sonrasında uygulama kapatılsa bile, cihazın arkaplan'ın da çalışmaya devam edebilir. Uber uygulaması ve lokasyon izninin aktif halde çalışıyor olması bunun bir örneğidir. Uber uygulaması istemiş olduğu izinlerde aşırıya kaçmış olduğu görülür. Amacının dışında kullanıcıdan talep ettiği izinler yer almaktadır. Örneği, cihazın kamerasına erişimek istemesi gibi. Uber bilindiği üzere özel araçlar ile hizmet sunabilen bir sistemdir. Mobil platform üzerinden kullanılabilen bu sistem ile kullanıcılar bir yerden başka bir yere kısa sürede ulaşmayı planlar. Yalnız bir sorun vardır. Uygulamayı kullanan kullanıcılar daha ilk uygulama kurulum aşamasında belli kuralları kabul ederek sisteme dahil olurlar. Bu durum uygulamanın kurulum aşamasında kullanıcıdan talep etmiş olduğu erişim izinlerini ve sonrasını kapsamaktadır. İzinleri kabul etmiş ve cihazlarına kuran kullanıcılar, sahip oldukları kişisel verileri farkında olmadan uygulamanın bağlı bulunduğu firma ile paylaşmış sayılırlar. Firma öncesinde, kişisel verilerin korunması ile ilgili düzenlemeleri, o kullanıcının ülkesinde kontrol eder. Eğer iç işlerinde bu duruma ilişkin özel düzenlemeler yok ise, kullanıcıdan alınan veriler üçüncü kişiler ve şirketlerle paylaşabilmesi durumuna imkân tanır. Şirket bu verileri kullanarak özel yazılım ve analizler yapabilir, kullanıcı profili oluşturabilir, onlara uygun reklam modelleri oluşturabilir ya da sosyal medya hesapları uzerinden erişim sağlayarak kendi lokasyonuna en yakın uygulama kullanıcı profilini bulabilir.[28]

[28] YETİM, S. (2015). UBER, HUKUKİ SORUNLAR VE ÇÖZÜM ÖNERİLERİ. Uyuşmazlık Mahkemesi Dergisi (6).



Şekil 13: UBER Android Uygulaması [29]

5. Kaos İçindeki Google Play Örneği

Android platform'unda geliştirilen uygulamaların çoğu legal yani yasal olarak Google Play uygulama marketi üzerinden indirilmektedir. Pazarın büyük bir kısmına bu market üzerinden hizmet verilmektedir. Her ne kadar yasal ve tekel gibi görünse de kendi içerisinde yapısal bozukluklar yok değil. İçerisinde çok sayıda korsan ve spam uygulama barındırmaktadır. Ayrıca programların ödemeleri de açık bir şekilde yapılmaktadır. Yazılım geliştirici, herhangi bir kredi kartından 20 dolar

[29]Orjinal çizim için bknz. https://www.uber.com/legal/other/android-permissions/

ödeme yaparak bu markette geliştirici olarak yer alır ve Google Play hesabı açabilir. Aynı şekilde ödeme yaparak da istediği bir uygulamayı da indirebilir.

Google Play politikası, önce çevirimci ol, sonra görüntüle ve değerlendir şeklinde işler.[30] Uygulamalarda ciddi bir inceleme veya tarama yapılmamaktadır. Ayrıca bu duruma ilişkin tedbir ve cezalar da oldukça hafiftir. Sadece uygulama kullanımdayken kullanıcıya uyarı verir. Sonrasında sorun teşkil ederse, Google Play selektif olarak geliştiricinin hesabını dondurma kararı alabilir. Fakat hesabı dondurduktan sonra geliştirici tekrar ücret ödeyerek yeni hesap açabilir. Buradan ulaşılabilecek sonuç şudur ki, uygulamalar denetlenmediği gibi fikri mülkiyet ve gizliliğin korunmasını esas almıyor.

6. WhatsApp ve Almanya Örneği

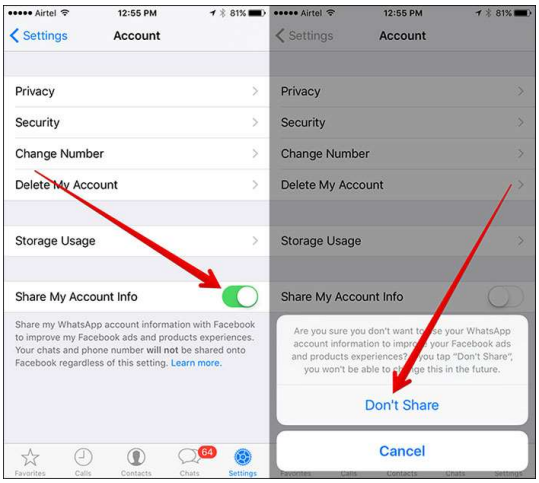
2014 yılında Facebook tarafından 16 milyon dolara satın alınan WhatsApp firması, kişisel verileri izinsiz paylaşamakla suçlandı. Whatsapp, Facebook ile paylaşacağı bilgiler sayesinde, kullanıcılarına uygun arkadaş profili ve kullanıcıyı ilgilendiren reklamlar gönderilmesine izin vereceğini ve spam mesajlarında önüne gececeğini açıkladı. Öte yandan ise bilgi paylaşımı istenirse kapatılabileceği söylendi. Yani WhatsApp, kullanıcının uygulamayı ne zaman kullandı bilgisini paylaşırken, şifrelenen mesaj içeriklerine ulaşılamayacağı bilgisini, kullanıcılarına da iletebilecek. WhatsApp şirket sayfalarında "Şifrelenen mesajlarını özel kalacak ve hiç kimse onları okuyamayacak. Ne WhatsApp, ne Facebook, ne bir başkası"[31] bilgisini paylaştı. WhatsApp kişisel verilerini facebookla paylaşmasının ardından, Almanya'nın veri güvenliği kurumu bu duruma karşı çıkarak, Facebook ve WhatsApp'dan elde ettiği bilgileri paylaşmamasını ve silmesini istedi. Veri güvenliği kurumunun hazırladığı rapora göre WhatsApp kişisel verileri toplamaya başladığı anda politikalarını değiştirmeden önce kullanıcılarını haberdar etmeyip üstelik bir onay da talep etmemişlerdir. Bu olay karşısında kurum yetkilileri ise Facebook'dan Almanya'da yaklaşık olarak 35 milyon kullanıcıyı ilgilendiren durumun düzeltilmesini istedi.

WhatsApp'da yer alan kullanıcı bilgilerinin, Facebook ile paylaşılmaması engelenebilir bir durumdur. Kullanıcı isterse bilgilerinin Facebook ile

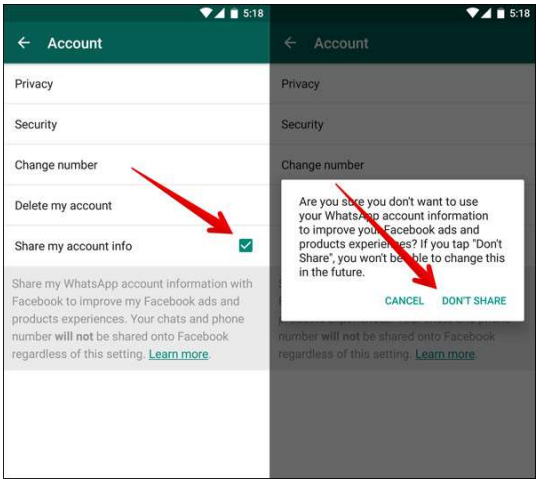
---

[30] Google Play Hizmet Şartları (https://play.google.com/intl/tr_tr/about/play-terms.html)
[31] WhatsApp'a da reklam geliyor (http://www.bbc.com/turkce/haberler-37190266)

paylaşılmasının önüne geçebilir. WhatsApp kullanım koşulları gizliğinde değişiklik yaptığı zaman, size yeni kurallarla ilgili değişiklik sunarken hemen "kabul et" seçeneğini onaylamadan önce kullanım şartlarını sonuna kadar okumalı ve "facebookla paylaş " kutucuğunun kaldırılması gerekir.



Şekil 14: IPhone WhatsApp'da, Facebook ile bilgi paylaşımının kapatılması [32]



Şekil 15: Android WhatsApp'da, Facebook ile bilgi paylaşımının kapatılması [33]

7. Erişim İzinlerinde Hukuki Zemin

Kişisel veri tanım olarak, kişiyi tanımlayan kişi hakkında her türlü özel ve genel olacak şekilde bilgiyi kapsayan, verilerin tamamını kapsar. Bu kapsamda kişinin

[32] Orjinal çizim için bknz. https://www.igeeksblog.com/how-to-stop-whatsapp-sharing-phone-number-with-facebook-on-iphone/
[33] Orjinal çizim için bknz. https://www.megebyte.com/how-to-stop-whatsapp-sharing-phone-number-with-facebook-on-android/

adı soyadı ve kimlik bilgilerinin yanısıra kişinin ailevi bilgileri, sosyo ekonomik ve kültürel bilgilerini ve kişisel bilgilerinide kapsar. En temel anlamıyla, kişiyi doğrudan ya da dolaylı yoldan ilgilendiren kişinin hak ve özgürlüklerinin korunmasına yönelik veriler bütünüdür. Günümüz bilişim teknolojilerinde, eski ve gelenekçi yöntemlerin aksine bilgiye ulaşmak daha kolaydır. Farklı yerlerde ve birbirinden bağımsız olan pek çok sayıdaki ölçülemeyen verinin biraraya gelmesi ve işlenmesi oldukça basittir. Bilişim teknolojileriyle verilerin eşleştirilmesi, analiz edilmesi ve yeni verileri üretebilme kapasitesi oldukça artmıştır. Ve sonuç olarak veri erişim ve transferleri daha basit hale gelmiştir. Kişisel verilerin özel ve ticari amaçlı kurum ya da kuruluşlar tarafından önem kazanması sonucunda veri sahibine ait riskler geçmişten bugüne daha önemli duruma gelmiştir. Öte yandan terör ya da organize edilmiş suç örgütlerinin kişiye ait bilgilere ulaşma faliyetleri ciddi tehlike boyutlarına ulaşmaktadır.

Kişisel Verilerin Korunması ile ilgili kanun tasarısı 24.03.2016 tarihinde TBMM genel kurulunda kabul görülerek ve 07.04.2016 tarihli 29677 sayılı Resmi Gazetede yayımlanarak yürürlüğe konuldu. Bu tasarıyla beraber bir bakıma kişinin hakları koruma altına alınmıştır. Türkiye'de çeşitli devlete bağlı kurum kuruluşlarda ya da özel kurumlarda kişiye ait verilerin paylaşılması, veri sahiplerinin haklarını görmezden gelinmekteydi. Bu kanun ile veri sahiplerinin bilgileri korunur hale gelmiştir. Anayasa Mahkemesi almış olduğu kararda yapmış olduğu tespitlerin sonucu olarak gelişen teknoloji ve sonrasında oluşan sınırsız olanakları, kişisel verilerin üst seviyede korunmasını zorunlu kılar.

8. Mobil Teknolojiler

Kullanmış olduğumuz uygulamalar ve bu uygulamaları edinmek için başvurduğumuz siteler zararsız gibi görünse de, bunun doğruluğunu asla garanti edemeyiz. Çünkü bu yazılımlar, tıpkı orjinallerine benzer imzalara sahip olabileceği gibi, aynı özellikleri de gösterebilir. Hatta taktit edebilirler. Ancak dikkat edildiği zaman, farkına varılabilir. Örneğin cihazınızda güvenliğinizi koruma adına kullanacağınız Antivirüs güvenlik yazılımları, bu tür uygulamaları farketmenizi sağlayabilir.

Mobil teknolojideki hızlı büyüme ve uygulamaların çeşitliliği, birçok yeni tehditi de beraberinde getirmiştir. Platformların ve yeni teknolojilerin işlevselliği, daha geniş bir saldırı yüzeyi sunmaya ve kullanıcıları kendisine çekmeyi

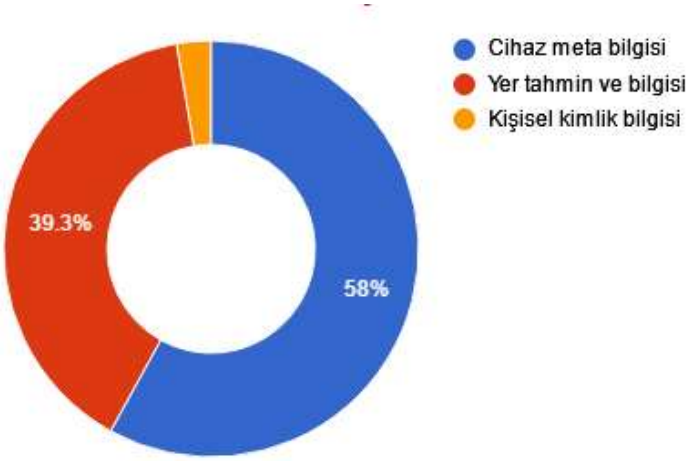
başarmıştır. Bu durum, güvenlik alanındaki çalışmaları, yalnızca mobil teknolojilerin değil, kullanıcıların taleplerine de ayak uydurmaya itmiştir. Kritik güvenlik testleri ve kullanıcılara sunulan öneriler her ne kadar güncel ve sağlam verilere dayansa da, saldırganlar bu güvenlik sistemlerini atlatmış ve kişisel özel verileri elde etmeyi başarmışlardır.

Zscaler adlı dijital güvenik firmasının araştırma raporuna göre mobil cihazlardaki artış miktarı ve uygulama geliştirme pazarı beraberinde veri kayıplarını ve güvenlik ihlallerine de yol açtı[34]. Gizlilik içeren bilgilerin çoğunluğu bu 3 kategoriden birine denk gelmektedir.

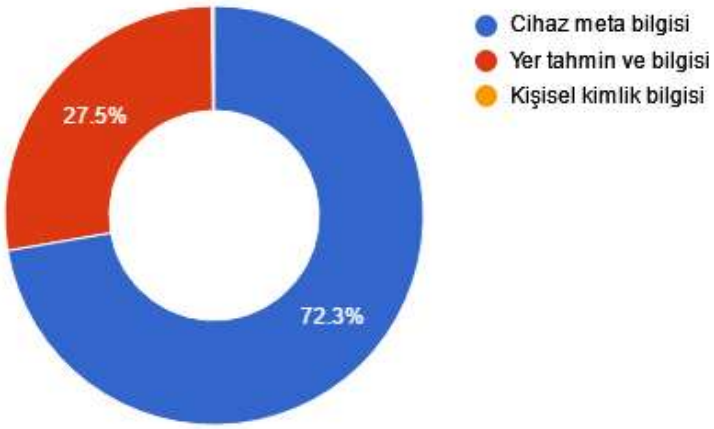
- *Cihaz meta bilgileri*: IMEI, MAC, IMSI numaraları, şebeke, işletim sistemi, SIM kartı bilgileri, üretici firma gibi. Sunucularına veya reklam sunucularına düz metin olarak gönderir. Bu tür veriler, cihazı izlemek ve hedefli saldırılar oluşturmak için kullanılabilir.
- *Yer tahmin ve bilgisi*: Cihazın tam enlem ve boylam koordinatları bilgilerini içerir.
- *Kişisel kimlik bilgisi*: Kullanıcının cep telefonu numarası ve e-posta adresleri de dahil olmak üzere tüm özel giriş bilgilerini içerir.

Rapora göre Android ve iOS cihazlarda veri gizliliği değişik şekillerde ele alınıyor. Cihazların sahip olduğu meta bilgileri yani MAC, GSM, IMEI, IMSI, UDID gibi donanım tanımlayıcı bilgiler küresel olarak benzersiz sayılıyor. Ve cihazın ömrü boyunca değişmeyecek bilgilerdir. Bu tanımlayıcı kimlikler, mobil gizlilikten, hedefli hizmetin reddine kadar bir dizi saldırıda kullanılabilir. Örneğin, saldırgan kişi kurbanının IMEI'sini kullanarak, uzaktan SMS hizmet saldırısı (SMS denial-of-service) ya da SIM Card sistem yetkisini ele geçirme gibi durumları gerçekleştirebilir. Yer tahmin ve bilgisi ile kullanıcıların yoğun olduğu bölgeler tespit edilerek kitlesel saldırılar gerçekleştirilebilir. Küresel çağda son derece değerli bilgilerdir. Telefon numaraları ve e-posta adreslerinin ise, herhangi bir şahsa ulaşmak için en hızlı yol olduğunu, spam mesajlar ve phishing saldırıları için kullanılabileceği söyleniyor.

[34] Are mobile apps a leaky tap in the enterprise? (https://www.zscaler.com/blogs/research/are-mobile-apps-leaky-tap-enterprise)



Şekil 16 Veri Gizliliği Analizi - Android [35]



Şekil 17 Veri Gizliliği Analizi - iOS [36]

Uygulama mağazası açısından gerçek şu ki, Android uygulama mağazası Apple'ın uygulama mağazasından çok daha fazla modifiye edilmiş, dolandırıcılık ve zararlı yazılım barındıran bir yapıya sahiptir. Özellikle finansal uygulamaları saldırılara karşı savunmasız bırakılmıştır. Çoğu durumda, geliştirici eğer kötü biri iyi ise, kendi geliştirdiği uygulamayı kullanıcı kimliğini çalma, kötü amaçla çalıştırma veya içerisinde kullandığı reklam içerikleri ile kullanıcıları kandırma gibi hareketlerde bulunabilir. Ve bu uygulamayı, güvenli olduğunu düşününülen çok sayıda farklı uygulama mağazına yükleyerek insanlara ulaştırabilir. Yapılan bir araştırma sonucunda 2014 verilerine göre iOS cihazlardaki finansal

[35] Orjinal çizim için bknz. https://www.zscaler.com/blogs/research/are-mobile-apps-leaky-tap-enterprise
[36] Orjinal çizim için bknz. https://www.zscaler.com/blogs/research/are-mobile-apps-leaky-tap-enterprise

uygulamaların %70'i saldırganların hedefi haline gelirken, bu durum Android cihazlarda %95'e kadar çıkmıştır. [37] Özellikle, finansal uygulamalara yapılan saldırılar kullanıcılar arasında endişe verici hale gelmiştir. Çünkü kullanıcılar bu uygulamalara güveniyor ve onlara banka hesapları ve parolalar gibi yaşamsal kişisel veriler sunarak işlemlerini gerçekleştirebiliyorlar.

Genelleme yapılmak istenirse, Google Play uygulama yükleme mağazası kendi içerisinde rahatsız edici uygulamalar olmasına rağmen elbette sansürcü bir zihniyete sahip değildir. Apple'ın Apple Store uygulama yükleme mağazasında ise kendi içerisindeki uygulamaların hemen hepsi meşru sayılır. Apple, tüm uygulamaları inceler ve uygun görürse mağazasına girmesine izin verir. Aksine, Google kendi mağazasında bulunan herhangi bir uygulamanın, kullanıcılar tarafından kötü amaçlı bir program olarak algılanıp ve şikayet edilmesi durumunu değerlendirir ve o uygulamayı mağazasından siler. Her iki platformda da kullanıcının telefonuna yüklenen kötü amaçlı yazılımları geriye dönük olarak kaldırmak için "killswitch tool" denen özelliği kullanır. Bu özellik olası sorunları en aza indirmek, hırsızlık ya da çalıntı gibi durumları büyük ölçüde azalmasına neden olmaktadır.

Son 10 yıla bakıldığı zaman, kötü niyetli yazılım veya malware olarak bilinen program ve virüslerin[38] giderek arttığını, kendisini geliştirip güçlendiğini görebiliriz. Malware, kötü amaçlı bir yazılımdır. Sahibinin izni olmadan, üzerine bulaşmış herhangi bir cihazı kullanmak üzere tasarlanan tehlikeli, müdahaleci, can sıkıcı yazılım veya program kodudur. Bu kötü amaçlı yazılım, özelliklerine göre aşağıdaki ana kategorilere ayrılabilir

- Virüs
- Worm (Solucan)
- Trojan (Truva Atı)
- Rookit
- Botnet

Bu zararlı yazılımlar, SMS bağlantıları, MMS ekleri, Bluetooth kanalı, E-posta iletimi ya da sisteme kurulabilecek herhangi bir uygulama yoluyla bulaşabileceği

[37] Most of the Top iOS and Android Apps Have Been Cloned to Spread Malware in 2014 (http://news.softpedia.com/news/Most-of-Top-iOS-and-Android-Apps-Have-Been-Cloned-to-Spread-Malware-in-2014-465310.shtml)
[38] GÜNGÖR, Murat. "ULUSAL BİLGİ GÜVENLİĞİ: STRATEJİ VE KURUMSAL YAPILANMA." (2015).

gibi çeşitli vektörlerle de yayılabilir. Akıllı telefonları hedef alan kötü amaçlı yazılımların ana hedefleri her zaman ortakdır; kullanıcının kişisel verileridir.

2004 yılında ilk mobil malware sayılabilecek uygulama oluşturulmuş ve symbian işletim sistemine sahip birçok cihaz bundan zarar görmüştür. 2009 yılında, iOS işletim sisteminde bulunan bir güvenlik açık sayesinde, ilk mobil botnet[39] saldırısı gerçekleştirilmiştir. 2010 yılında Android işletim sistemine sahip cihazlar üzerinde, ilk android mallware yazılımı keşfedilmiş, kullanıcılar adına önceden ayarlanmış numaralara SMS mesajları gönderdiği farkedilmiştir.

Şekil 18: 10 years of malware for mobile devices [40]

2011 ve 2014 yılları arasında ise, Android tabanlı cihazlarda malware denebilecek zararlı yazılımların etkileri büyük ölçüde hissedilmiş, birçok kullanıcıda maddi olarak ciddi zarar vermiştir. 2015 yılında ise, Android cihazlarda yakın tarihin en büyük güvenlik açığı tespit edilmiş ve Android işletim sisteminin tüm versiyonları, gelen saldırılara karşı savunmasız bırakılmıştır. Bu açık Android işletim sistemindeki Stagefright[41] adındaki bir bileşendeki güvenlik açığından yararlanılarak oluşturulmuştur. Söz konusu güvenlik açığı, kullanıcıya özel olarak oluşturulan bir MMS iletisi üzerinden ulaşıyor ve kullanıcıya kendisini yükletebiliyor. Bu şekilde kurbanı tehlikeye düşürebiliyor. Bunu önlemek için, otomatik MMS indirmelerini kapatmak ve bilinmeyen kullanıcılardan gelen ekleri açmamak veya tıklamamak bir çözüm gibi görünebilirdi. Ancak, saldırganlar

[39] ÖğÜN, M. N., & Adem, K. A. Y. A. (2013). Siber güvenliğin milli güvenlik açısından önemi ve alınabilecek tedbirler. Güvenlik Stratejileri Dergisi, 9(18), 145-181.
[40] Orjinal çizim için bknz. https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-mobile-security-threat-report.pdf
[41] Allen, S. G. Mobile Malware in the Enterprise.

amacına ulaşmış olmalı ki, bu güvenlik açığı üzerinden yaklaşık olarak, toplam Android cihazın %95'ine[42] ulaşmayı başarmışlardır.

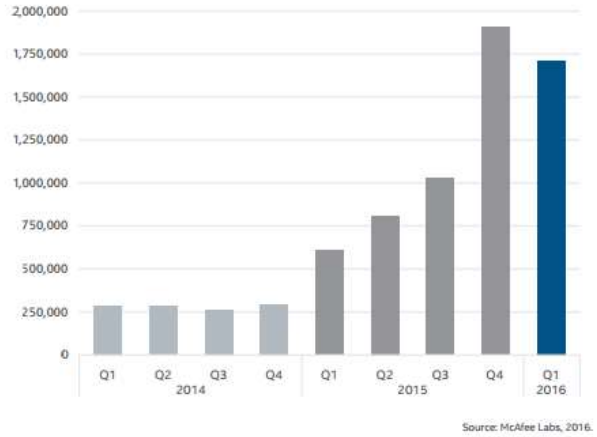
Mobil cihazlarda yüklü uygulamaların davranış biçimlerini hiçbirimiz farkedemeyiz. Masum gibi görülebilir ve kullanıcının beklentilerinin çoğunu karşılayabilirler. Saldırganların beklentileri de aynen bu yönde olması gerekiyor. Bunun için ürettikleri yazılımlar olabildiğince amacına uygun, düzgün görünümlü, anlaşılabilir ve de beklentileri karşılayabilecek türde olması için uğraş vermektedirler. 2014 yılında, Gartner araştırma şirketinin yapmış olduğu araştırmaya göre, mobil uygulamaların %75'inden fazlasının 2015 yılına kadar temel güvenlik testlerinde, başarısız olabileceğine işaret etmiştir. [43] Yine aynı yıllarda yapılan başka bir araştırmaya göre, bu zararlı yazılımlara karşı Android uygulamaların yaklaşık %42'sinin savunmasız olduğu gözlemlenmiştir. [44] Uygulamalar cihazlara yüklendikleri andan itibaren, aynı işletim sisteminde yüklenmiş diğer uygulamalar tarafından gözlemlenebileceği gibi, amacından da saptırılabilir. Örneğin Sms gönderim uygulaması, her yeni bir ileti gönderdiğinde bir kopyasını bir başka kişiye de gönderebilir. Bu ve benzer durumlara sebep olabilecek zararlı yazılımlar, kurulum öncesinde kullanıcı erişim izinleri aldıkları için hiç sıkıntı yaşamadan istedikleri gibi hareket edebilme yetenekleriyle donatılmışlardır. Bu zararlı sayılabilecek yazılımları geliştirebilen kişiler, yazılımın alabileceği tüm aksiyonları hesaba katarak cihazlara bulaştırmaktadırlar. Ve her geçen yıl biraz daha kendini yenilemiş ve teknolojiye ayak uydurabilir hale getirilmiştir. Resimde görülebileceği üzere, 2016'nın ilk çeyreğinde 1,75 milyona yakın yeni mobil malware örneği bulundu. Bu sayı her geçen yıl daha da artmaktadır.

---

[42] What you need to know about the new Android vulnerability, "Stagefright"; (https://blog.lookout.com/blog/2015/07/28/stagefright/)

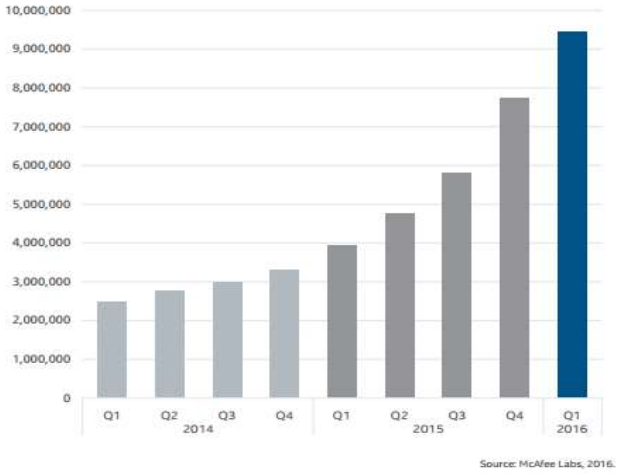
[43] N.a (n.d.). Gartner Says More than 75 Percent of Mobile Applications will Fail Basic Security Tests Through 2015. Gartner.com. Retrieved from http://www.gartner.com/newsroom/id/2846017

[44] Mobile Threat Report https://www.webroot.com/shared/pdf/WR_MobileThreatReport_v4_20140218101834_565288.pdf



Şekil 19: Yıllara göre mobil zararlı yazılım (malware) adedi [45]

Her yıl büyüyen kötü amaçlı yazılımların sayısı, mobil platformlarda güvenlik konularının ciddiye alınması gerektiğini göstermektedir. Aynı şekilde, araştırma raporlarının gösterdiği verilere dayanarak, şu ana kadar 9 milyondan fazla mobil malware örneğinin var olabileceği söylenebilir.

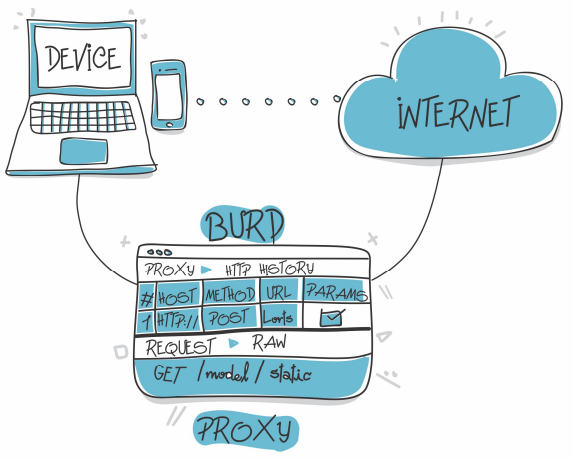


Şekil 20: Toplam mobil zararlı yazılım (malware) adedi [46]

Mesela bankadan kredi çekmek istiyorsunuz ve kredi taksit miktarını hesaplamak adına ufak bir uygulamaya ihtiyaç duydunuz. Android uygulama yükleme mağazasından bu türde bir uygulama edindiniz ve kullanmaya başladınız. Uygulama basit anlamda, sizden kurulum öncesi bazı izinleri almış olmalı ki cihazınızda özel verilere erişebilsin. Başta kullanıcı bu durumu göz ardı edecektir,

[45] Orjinal çizim için bknz. https://www.mcafee.com/tw/resources/reports/rp-quarterly-threats-may-2016.pdf
[46] Orjinal çizim için bknz. https://www.mcafee.com/tw/resources/reports/rp-quarterly-threats-may-2016.pdf

çünkü bu izinlerin ne anlama geldiğini bilmez, uygulamanın masum olup olmadığını bilemez ya da pek aldırış etmez. Peki, uygulama yüklendi ve kullanıcıdan neler alabilir. En başta, kimlik bilgilerini alabilir. Eğer kullanıcının kullanmış olduğu cihazda, başka diğer uygulamalara bağlı hesaplarda var ise onlara erişip kullanıcıya farkettirmeden saldırganın kendisine gönderebilir. Bu yazılımcı için zor bir işlem değildir, sadece cihazın izin politikasını aşması, güvenlik tarafını geçmesinde yardımcı olur. E-posta, bankacılık ya da diğer önemli sayılabilecek uygulamaların veritabalarına erişerek kişisel veri sayılabilecek tüm verileri kendine iletebilir. Kişinin tam adı soyadı, adresi, varsa kimlik numarası, adres defteri, konum verileri, kredi kartı hesapları, cihazın içerisinde saklı tüm erişim verileri gibi alınabilecek her bilgi saldırgan için değerlidir. Kullanıcı uygulamayı kullandığı anda bu durumun asla farkına varamaz. Onun için tek önemli sayılabilecek unsur, uygulamanın vereceği hizmetten faydalanmaktır. Saldırganın bu bilgileri, cihazın kullanılmadığı zaman alabileceği gibi, kullanım sırasında da edinmesi çok da zor olmaz. Örneğin yine aynı kullanıcı kredi notunu öğrenmek üzere uygulamayı başlatıyor, uygulama içerisinde yeralan form alanlarına kişisel bilgileri girmeye başlıyor. Anlık olarak gireceği her bilgi saldıganın kurmuş olduğu altyapı üzerinden takip edilebileceği gibi, ağ trafiği de izlenebilir. Şimdi, bu Sniffing attack[47], yani türkçesi koklamak olarak da tabir edilen bu saldırı durumunu ele alalım. Bu metodu uygulayabilen kişiler, kolayca ağ üzerinden gelip giden veri paketlerini okuyabilir ve onları manipüle edebilir.



[47] Security Threats and Defense Approaches in Wireless Sensor Networks: An Overview http://www.ijaiem.org/Volume2Issue3/IJAIEM-2013-03-15-033.pdf

Şekil 21: Uygulama dinleme yöntemi [48]

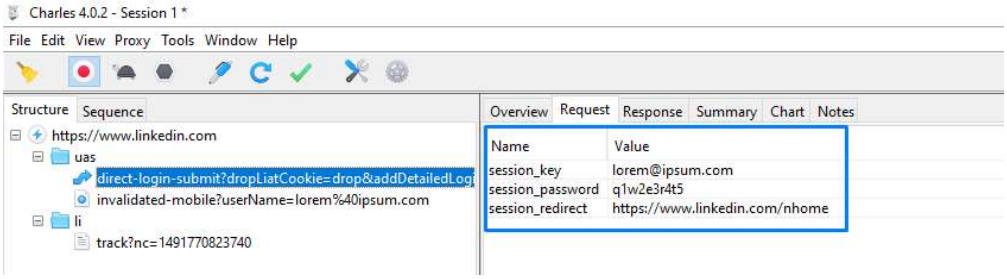
Paket algılama, belirli bir ağ arabirimi üzerinden geçilebilecek tüm veri paketlerini yakalayan, tanıyan ve çözebilen programlar ile yapılabilir. Bir paket dinleyicisi, bulunduğu ortamda bazen ağ izleyicisi veya ağ analizörü olarak görülebilir. Genellikle ağ veya sistem yöneticisi tarafından ağ trafiğini izlemek ve gidermek için de kullanılabilir. Bununla birlikte, bazen de kötü niyetli davetsiz misafirler tarafından bir kullanıcının şifre kartı numarası şifresini çalmak gibi yasadışı amaçlar için kullanılmaktadır. [49] Resim de de görüldüğü üzere, kullanıcının mobil cihazı üzerinde kullanmış olduğu uygulama verilerinin aslında tam olarak hangi adrese gönderildiğini bilemez. Bunu ancak uygulamayı dinleyerek bulabilir. Eğer saldırgan uzman bir geliştirici ise, kodlama içerisine zararlı sayılabilecek türden eklemelerde bulunarak, kendi oluşturduğu bir bağlantı üzeriden akan tüm internet trafiğini izleyebilir. Ve verileri kod bilgisi olmadan değiştirilebileceği gibi, art niyetli olarak da kullanılabilir.

Örneğin kullanıcı mobil cihazından Linkedin uygulamasını başlatmak istedi. Uygulama daha ilk açılışında, sisteme erişim için kullanıcının bilgilerini talep edecektir. O anda, kullanıcı arka planda çalışan diğer zararlı uygulamalardan habersizdir. Kullanıcı formu doldurmaya başladığı andan itibaren form verileri, işlenmeye başlayacaktır. Veriler karşı tarafa iletilmeye başlamadan önce, zararlı sayılabilecek yazılımlardan geçerek, bir kopyasını saldırgana iletmiş olur.

[48] Orjinal çizim için bknz. https://stanfy.com/blog/monitor-mobile-app-traffic-with-sniffers/
[49] Packet Sniffer Animated Simulator (http://williams.comp.ncat.edu/IA_visualization_labs/security_visual_tools/packet_sniffer/packet_sniffer.html)

Şekil 22: Android Linkedin uygulaması [50]

Aşağıda görülebileceği üzere, kullanıcı tarafından yapılan her bir işlem ve işlenen her bir veri kullanıcı arada dinleyici modunda duran saldırgan tarafından takip edilmekte hatta kayıt altına alınmaktadır. Kullanıcı bu durumun farkına varmaz. Uygulama da normal akışında çalışmaya devam eder. Sunucu tarafı ise, uygulamadan gelebilecek istekleri aynı şekilde karşılar ve geri döner. Saldırgan ise sadece olup biteni izler.



Şekil 23: Charles Proxy: Ağ oturum trafiğini yakalama uygulaması [51]

Bu ve benzeri örneklerin doğurabileceği pek çok sonuç vardır. Kullanılabilecek her türlü araç, kötü birer aktör haline gelmiştir. Bu ayrıcalığın verilmesini sağlayan hiç kuşkusuz; Jailbreak (iOS) ve Rooting (Android) yapılmış mobil cihazlarda alınan yetkisiz erişimler olmuştur. Kullanıcılar, mevcut kullanmakta olduğu cihazlarını bir adım öteye taşıyarak cihaz üzerinde tam yetki sahibi olmak istemektedirler. Bu durumu günümüz deyimiyle cihazı garanti kapsamı dışına çıkarmaktır. Yani, tüm yetki bende, güvenliği kendim sağlıyor olacağım anlamına da gelmektedir. Her türlü uygulama bu yol ile cihaz içerisine yüklenebilir, kullanıcının izni olmadığı halde izin alınmış gibi gösterilebilir ya da arka planda sessizce çalışarak cihazı dinleyebilir. Bunun örnekleri çok fazladır.

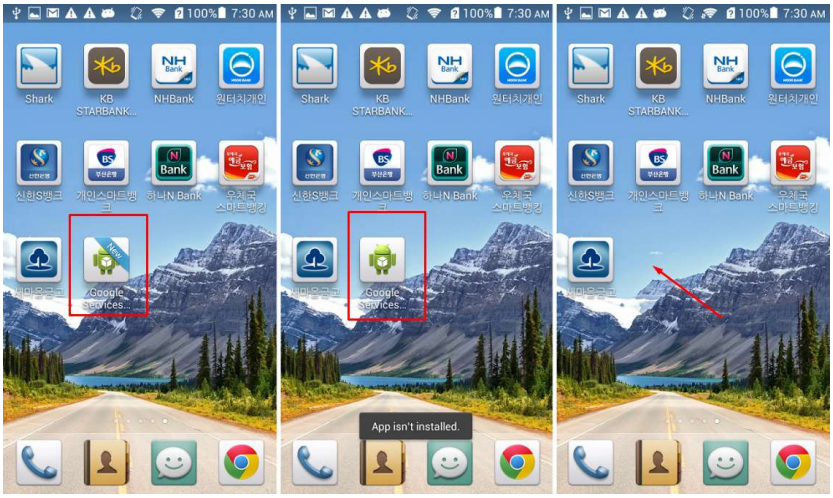
Saldırganlar yetkisiz olarak erişebildiği ve uygulamalarını çalıştırabileceği uygun ortamları yakaladıkları zaman, farklı türlerde saldırı stratejilerini deneyebilirler. Bunun en etkili sonuçları mobil cihazlarda yapılan ödeme işlemleri sırasında görülür. Yetkisiz çalışabilen zararlı uygulamalar, öncelikli olarak kullanıcının banka hesaplarına, yüksek koruma gerektiren özel bankacılık uygulamalarına ve mobil ödemenin yapıldığı uygulamalara erişmek için kimlik bilgisi edinmeye çalışırlar. Saldırılarını başarıya ulaşırsa, bir kişiden değil kitleye

[50] Android Linkedin Uygulaması, https://play.google.com/store/apps/details?id=com.linkedin.android&hl=en
[51] Charles Proxy: Ağ oturum trafiğini yakalama uygulaması

yönelik bir saldırı anlamı taşımaktadır ki, bu bağlamda pek çok ödeme kimlik bilgisi toplamış olacaktır. Bu riskin en büyük örneğini 2014 yılında görebiliriz. Siber suçlular farklı türde bankacılık ve dolandırıcılık hilelerini tek bir çatı altında toplayarak HijackRAT[52] adında yeni bir malware tipi geliştirmeyi başardılar. Sadece Android cihazlar üzerinde çalışabilen bu zararlı yazılımın özellikleri arasında,

- SMS'i bilgilerini edinebildiği gibi ve sms gönderimi de yapabilmesi,
- Kendisini sürekli güncel tutabilmesi,
- Telefon rehberine erişebilmesi,
- Kurbanın bankacılık uygulamalarını tarayıp, onları taklit edebilemesi,
- Bankacılık bilgilerini çalması,
- Özel veri hırsızlığı
- Cihazın veri akışını kontrol edebilmesi,
- Ve cihaz ile uzaktan erişimi sağlayabilmesiydi.

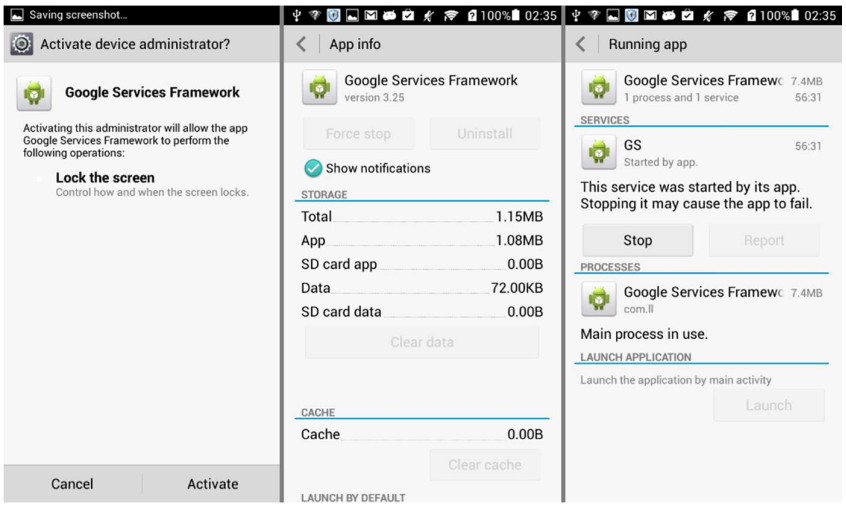
Bu yazılım o kadar etkiliydi ki, 65 antivirüs firmasından sadece 5 tanesi tarafından tespit edilebildi. Cihazlara, Google Service Framework adıyla kendini yükleniyor ve ardından tam yetki talebi için kullanıcıdan erişim izni istemekteydi.



Şekil 24: HijackRAT - Sahte "Google Service Framework" ikonu [53]

[52] Etaher, N., Weir, G. R., & Alazab, M. (2015, August). From zeus to zitmo: Trends in banking malware. In Trustcom/BigDataSE/ISPA, 2015 IEEE (Vol. 1, pp. 1386-1391). IEEE.
[53] Orjinal çizim için bknz. https://www.fireeye.com/blog/threat-research/2014/07/the-service-you-cant-refuse-a-secluded-hijackrat.html

Kullanıcı bu izni verdikten sonra kendisini sistem uygulaması gibi görerek, uygulama ikonunu ekrandan kaldırıyor ve arka planda çalışmaya başlıyordu. Yazılım artık aktif ve görevini yapmaya hazır haldedir.



Şekil 25: HijackRAT - Arka plan çalışma isteği [54]

Trojenler (Truva atları), "eklendikleri program dosyasının çalıştırılması sonucu aktif olurlar ve kullanıcıların kopyalamasıyla yayılırlar. Sistemlere uzaktan erişim sağlayarak bir backdoor kodunu, eski bir bilgisayar virüsünü ya da yepyeni bir solucanı kaydedebilirler. Truva atlarını diğer virüslere göre tespiti çok daha zordur. Herhangi bir şekilde bulaşmadıkları için ve herhangi bir etkide bulunmadıkları için ancak etkisini gösterdikten sonra anlaşılabilir. Truva atları, internet hızını yavaşlatır ve yerleştikleri sistemi kullanarak web'in geri kalanına yayılabilirler" [55]. Ve bu zararlı yazılımlar, tıpkı normal yazılımlar gibi yetişkinlere uygun içeriklere sahip olabileceği gibi ve aynı uygulama mağazası üzerinden indirilebilirler.

Bir diğeri, Malware yani zararlı yazılım bulaştırmadır. Kullanıcının cihazı üzerine yerleşmiş olan zararlı yazılım, kullanıcının yakın çevresine de bulaşabilir. Bu işlemi telefon rehberi üzerinden yapabileceği gibi, iletişimi sağlamak için kullandığı ağ ortamı üzerinden de gerçekleştirebilir. Tıpkı bulaşıcı bir hastalık gibi, varlığını ve etkileşimini bu yol ile sürdürebilir. Ona yüklenen komutlar

[54] Orjinal çizim için bknz. https://www.fireeye.com/blog/threat-research/2014/07/the-service-you-cant-refuse-a-secluded-hijackrat.html
[55] Uslu, T. (2007). İnternet güvenliği ve risk yönetimi (Doctoral dissertation, İstanbul Kültür Üniversitesi/Fen Bilimleri Enstitüsü/Bilgisayar Mühendisliği Anabilim Dalı).

sayesinde, hareket edebildiği gibi varlığını da sürdürebilmektedir. Bu sayede, saldırgan kişiyi ve ya yakın çevresi izleyebilir, kimlik bilgilerini çalabilir.

Üçüncü strateji, saldırgan uzak bir bağlantı üzerinden kullanıcının cihazını kontrol edebilir ve istediğini yaptırabilir. Zombi yani köleleştirme olarak da nitelendirilen bu yol ile etki altına giren cihazlar aldıkları komulara tepki vermek üzere programlanırlar. Amaçları, sadece kişisel veri hırsızlığı değildir. Sistemlere zarar vermek, onları durdurma noktasına getirmek hatta kişinin değil, kişinin üzerinden sistemin verilerini edinmek üzere de programlanabilirler. Örneğin kullanıcıya farkettirmeden, malware aracılığı ile cihaza uzaktan bağlanılıyor. Ve yapılaması planlanan DDOS saldırısı cihaz üzerinde gerçekleştiriliyor. Bilindiği üzere, "DDOS, bilişim sistemlerini işlemez hale getirmek için kullanılan bir ağ saldırı yöntemidir." [56] Bu ve benzeri saldırı yöntemleri üzerinden, erişilmek istenen sistemler hedef alınır ve cevaplayabileceğinden çok daha fazla istek göndererek sistemi durma noktasına getirilmesi hedeflenebilir. Mobil cihaz kullanıcısı ise habersizdir ve ağ bağlantısı olduğu sürece saldırıyı sürdürmeyi devam eder.

9. Mobil Cihazlarda Karşılaşılan Sorunlar

Güvenlik, hassas bilgiler içeren ve internet'e erişebilen her bir bilgi işlem aygıtı için önemli bir konudur. Önceleri bu durum pek önemsenmese de, günümüz mobil aygıtları için büyük bir sorun haline gelmiştir. Mobil cihazlarda ve bu cihazlarda kurulu uygulamalarda karşılaşılan sorunlar, güvenlik uzmanları tarafından kategoriler halinde kullanıcı ve geliştiricilere sunulmuştur. OWASP[57] adı verilen güvenlik projesi, web ve mobil uygulamalarının güvenliğini artırmaya yönelik uluslararası bir kuruluştur. OWASP güvenlik alanındaki birçok ilgili projeye sponsorluk yapmaktadır. Bu kuruluş, her yıl dünyadaki en iyi 10 web uygulamasının güvenlik riskini ve ne gibi sonuçlar doğurabileceğinin bir listesini yayımlamaktadır. Liste, her yeni güvenliğinin zaafiyetini açıklamakta, oluşabilecek türde örnekler vermekte ve bunlardan kaçınmak için öneriler sunmaktadır. Resmi olarak Haziran 2013'te yayınlanan ilk 10 listenin en son sürümü 2010 güncelledi. 2013 en iyi 10 listesi, yüzlerce organizasyonda

[56] Kaya, M. B. (2009). Türk hukukunda ve mukayeseli hukukta internet erişiminin engellenmesi (Doctoral dissertation, İstanbul Bilgi Üniversitesi).
[57] OWASP - Open Web Application Security Project, https://www.owasp.org

500.000'in üzerinde güvenlik açığı bulunan yedi uygulama güvenlik firmasının verilerini temel almaktadır. OWASP ilk 10 listesinde, bunların nasıl istismar edilebileceğini, tespitlerini ve etkilerini açıklamaktadır. Yine aynı kuruluş, mobil teknolojiler için de çalışmalarını sürdürerek, en iyi 10 listesini mobil güvenlik üzerine de sunmuştur. OWASP tarafından 2012 ve 2013 yılları arasında ilk en iyi 10 mobil güvenlik listesi yayınlandı[58]. Mobil cihazlarda oluşabilecek sorunları, doğabilecek sonuçları ve önerileri anlatılmaya çalışıldı. Ancak liste net değildi, geliştirilmeye açık ve resmi olmayan veriler üzerine kuruluydu. Daha sonra, ilk mobil güvenlik bildirimini "resmi olarak" 2014 yılında bildirmiştir. Bu bildiriminde, mobil teknolojileri kullanan kullanıcıların karşılaşabileceği sorunları ve riskleri üzerine detaylı olarak değinmiştir. Ve veriler ile geçerliliğini ispatlamıştır. Bu liste 2016 yılında ise liste güncellenmiş ve önemli eklemelerde bulunulmuştur. Bir önceki senelere göre daha güncel konular ve riskler listeye dahil edilmiştir.

2014 raporuna göre, en önemli sayılabilecek 10 güvenlik riskleri şu şekildedir [59];

M1: Güvensiz Sunucu Uygulamaları (Weak Server Side Controls)

M2: Güvensiz Veri Depolama (Insecure Data Storage)

M3: Yetersiz Bağlantı Güvenliği (Insufficient Transport Layer Protection)

M4: İstenmeyen Veri Sızıntısı (Unintended Data Leakage)

M5: Yetersiz Yetkilendirme / Kimlik Doğrulama (Poor Authorization and Authentication)

M6: Yetersiz Kriptografi / Kimlik Denetimi (Broken Cryptography)

M7: İstemci Taraflı Enjeksion (Client Side Injection)

M8: Güvensiz Girdilierin Tetiklediği Hassas İşlemler (Security Decisions Via Untrusted Inputs)

M9: Güvensiz Oturum Bilgisi (Improper Session Handling)

M10: Uygulama Koruma Eksikliği (Lack of Binary Protections)

I. M1: Güvensiz Sunucu Uygulamaları

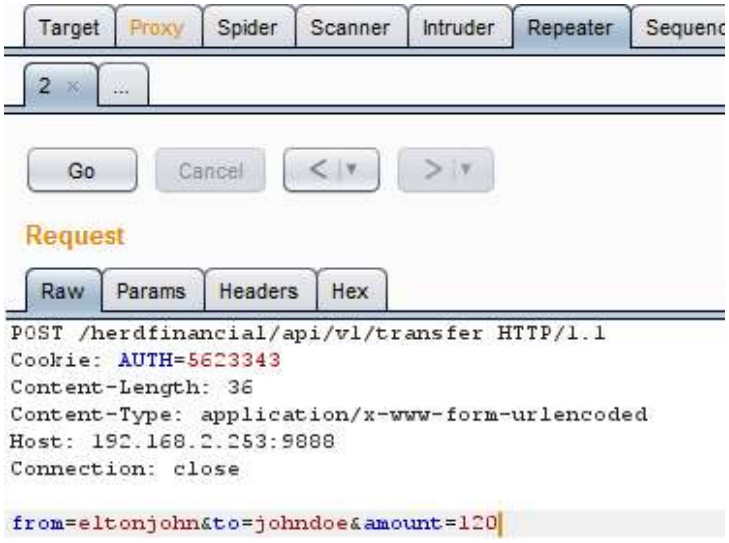
Genel olarak mobil uygulamalar, arkasında sunucu çalışan API ya da Web Servis hizmetleri gibi uç birimler ile iletişim kurmaya çalışırlar. Uygulamanın

[58] Phil, P. R. (2014). OWASP Top 10: The Top 10 Most Critical Web Application Security Threats Enhanced with Text Analytics and Content by PageKicker Robot Phil 73.

[59] OWASP En iyi 10 Mobil Güvenlik Riskleri, ayrıntılı bilgi için bknz. https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

güvensiz bir arka uç ile iletişim kurması, yetkisiz kullanıcıların burada depolanan verilere erişmesine izin vermesi demektir. Bu güvenlik açığının etkisi, sunucu tarafındaki ilgili güvenlik açığının etkisine bağlıdır. Bu sorunlar, sunucu tarafındaki yazılımdan ya da sunucunun kendi güvenlik zafiyetinden kaynaklanabilir. Saldırganlar bu açıkları kullanarak; SQL Enjeksiyon, XSS ve yetkisiz erişim gibi saldırılara sebebiyet verebilirler. Sunucu tarafındaki güvenlik açığının türüne bağlı olarak hem kullanıcıların hem de sunucuların ele geçirilmesi sağlanabilir. Hassas verilere erişim, kişisel veriler, itibar kaybı ve ya fikri mülkiyet hırsızlığına neden olabilir. Ayrıca dikkat edilmez ise müşteri kaybına hatta maddi hasarlara da yol açabilir.

Örneğin bir finans uygulamasını ele alalım. Kullanıcı mobil cihaz üzerindeki bu uygulamayı çalıştırırak para transferi yapmak istesin. Kullanıcı, sunucu ile cihaz arasında dinleyici konumundaki saldırgan habersizdir ve uygulamayı kullanmaya devam eder. Bu noktada saldırgan kullanıcının yapmış olduğu tüm işlemleri habersiz izlemektedir.



Şekil 26: Güvensiz sunucu uygulama analizi

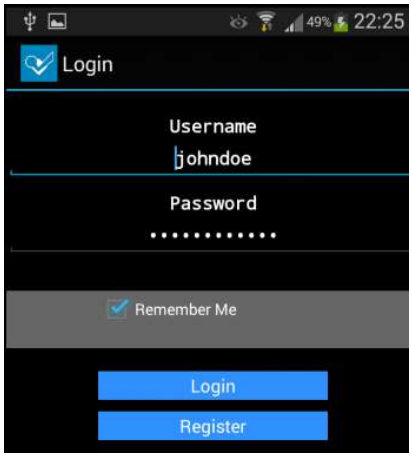
Sunucu tarafında yapılan bir istekde saldırgan, kullanıcı hesabındaki akışı istediği gibi değiştirebilir. İsterse bakiyeyi görüntüler, isterse de işlem akışını kendi istediği yönde yürütebilir. Bu durumdan az zarar ile çıkmanın birkaç yolu vardır. Öncelikle, sunucu tarafı olarak istemciye yani mobil cihaz kullanıcılarına asla güvenilmemesi gerekmektedir. Sunucu tarafındaki servis hizmetlerinin güvenliğinin sağlanması ve güvenlik kontrollerinin sık sık yapılması gerekir. Ve

en önemlisi, uygulamaların güvenli bir şekilde kodlanması ve geliştirme sonrası güvenlik taramasından geçirilmesi sorunları azaltacaktır.

II. M2: Güvensiz Veri Depolama

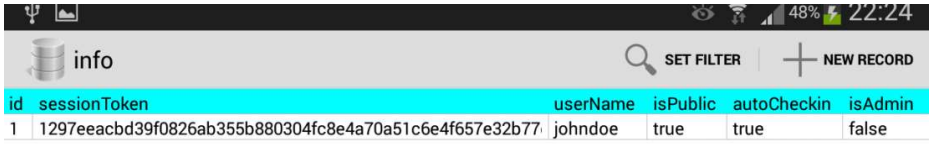
Bu güvenlik açığı, veriler cihazda güvensiz bir şekilde depolandığında ve başka bir kullanıcının mobil cihazını ele geçiren saldırganlara karşı savunmasız bırakıldığı zaman ortaya çıkmaktadır. En basit anlamda, geliştiriciler bazen kullanıcıların bu bilgilere erişemeyeceğini varsayarak kullanıcı tarafındaki bilgileri (kullanıcı telefonu içerisinde) saklarlar. Kullanıcılara ait hassas sayılabilecek veriler, mobil uygulamalar içerisinde güvensiz olarak deponlanması, kullanıcıların şifreleri, kredi kartları, finansal bilgileri ve kişisel bilgilerine (adres, sosyal güvenlik numarası, tam adı) başkaları tarafından erişilebilir hale gelmesine neden olabilir. Öyleki, cihazda saklanan verilere kullanıcılar veya zararlı yazılımlar tarafından erişilemeyeceği varsayıldığı için, veri güvenliği genel olarak doğru bir şekilde uygulanmaz.

Örneğin kullanıcı her uygulama açılışında tekrar tekrar erişim bilgisi girmek istemez. Başta bir kez bu bilgileri girer ve sistemin hatırlaması için beni hatırla seçini seçerek uygulamayı kullanmaya devam eder. Uygulama, bir daha bu bilgileri sormadan bir sonraki aşamaya geçer.



Şekil 27: Güvensiz veri depolama analizi - kullanıcı giriş ekranı

Yalnız kullanıcının dikkat etmediği bir durum vardır, uygulama kendi içerisinde yapılan her işlemi bir veritabanı içerisinde saklayıp kullanmaktadır. Kullanıcının erişim bilgileri de dâhil olmak üzere tüm bilgiler burada tutulmaktadır. Saldırgan, uygulamanın verilerine erişmek istediği zaman ilk bakacağı yerlerden birisi de bu veritabanıdır.



Şekil 28: Güvensiz veri depolama analizi - kayıtlı kullanıcılar

Bu nedenle, hassas sayılabilecek veriler genel depolama alanlarında doğru şifreleme kullanılmadan ya da şifrelenme uygulanmadan saklanmaktadır. Mobil cihazlarda güvensiz sayılabilecek depolama alanları, SQLite veritabanları, log (kayıt) dosyaları, XML dosyalar, Cookie sayılabilecek dosyalar ve SD kartlar. Bu durum'dan korunmanın yolları vardır,

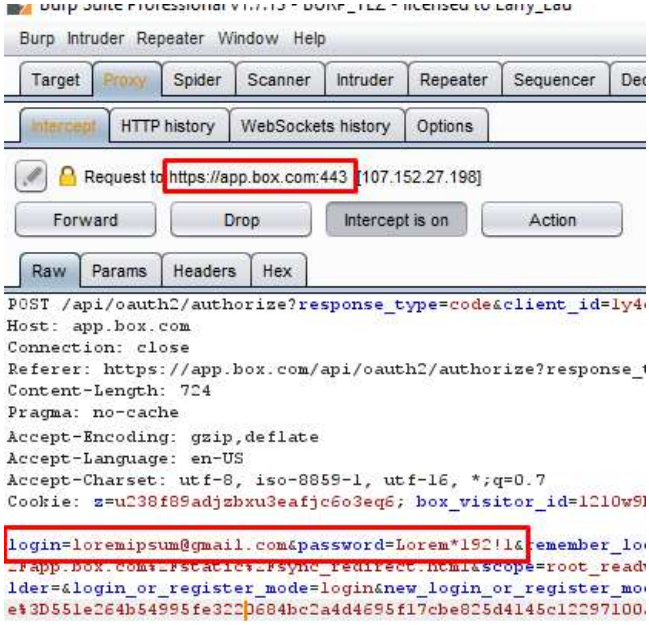
- Hangi verilerin depolanması gerektiği belirlenmeli ve kesinlikle gerekli olabilecek durumlarda veriler bu alanlarda saklanmalı,
- Gerekmedikçe hassas verilerin mobil cihazlarda saklanmaması,
- SD kart gibi genel depolama alanlarında bu verilerin bulunmaması,
- Uygulama içerisinde saklanan tüm hassas bilgileri ve verileri şifrelenmesi, gerekirse özel bir şifreleme sistemi kullanarak bu işin yapılması gerektiği öngörülmektedir.

III. M3: Yetersiz Bağlantı Güvenliği

Genellikle, bir mobil uygulama tasarlandığında, veriler istemci ve sunucu modeli arasında gezdirilir. Bu veri akışında, bilgiler hem bir ağ şebekesini hem de internet ağını dolanarak daha fazla katmana ulaşır. Veri akışı sırasında, veri gizliliğini ve bütünlüğünü koruyabilmek, kullanıcı açısından çok önemlidir. Mobil cihaz ile sunucu arasında kurulabilecek iletişimin güvenli bir kanal üzerinden yapılması gerekir. Bu noktada, iletişimin SSL / TLS ile yapılması en doğru olanıdır. "SSL protokolü internet iletişimi için yüksek seviyeli bir güvenlik sağlar. SSL web tarayıcınız ile web sunucusu arasında şifrelenmiş (kriptolanmış) bir iletişim oturumu sağlar. SSL hassas bilgilerin (örneğin kredi kartı numaraları, hesap bakiyeleri ve diğer özel finansal ve kişisel veriler) tarayıcınız ile bir web sunucusu arasında çevrimiçi işlemler esnasında gizli kalmasını sağlamaya yardımcı olur." [60]

Mesela saldırgan uygulama ile sunucu arasındaki güvenlik sistemini taklit ederek, güvensiz bir ortam oluşturur ve veri trafiğini izleyebilir.

[60] Kural, B. I. B. A. HSBC Şirket Bankacılığı.



Şekil 29: Yetersiz bağlantı analizi

Kullanılan bu protokolün zayıflığı, eksik veya güvensiz oluşu, her türlü veri kaybına neden olabileceği gibi mahremiyeti ortadan kaldırır. Yani, saldırgan olarak belirtilen üçünücü kişinin, mobil ve sunucu arasında yapılan iletişime sızması anlamına gelmektedir. Daha güçlü şifreleme sistemini kullanmak, bu sorunların önüne geçecektir.

IV. M4: İstenmeyen Veri Sızıntısı

İstenmeyen bir veri sızıntısı, bir geliştirici yanlışlıkla önemli bilgileri veya verileri cihazdaki diğer uygulamalar tarafından kolayca erişilebilen bir yere yerleştirdiğinde ortaya çıkar. Bu güvensiz yere aynı cihazda çalışan diğer kötü amaçlı uygulamalar erişilebilir ve böylece veriler için ciddi bir risk durumu ortaya çıkar. Bu hassas bilgiler, web sayfası oturumu, ekran görüntüleri, günlük dosyaları, geçici dosyalar, tarayıcı çerez nesneleri, kopyala/yapıştır önbellek bilgi ve istek-yanıt olarak URL önbellek bilgilerini içerir. Bunu önlemek için, cihaz tarafından toplanabilecek verileri, yalnızca ihtiyaç duydukları hallerde depolamak sorunu biraz azaltacaktır.

V. M5: Yetersiz Yetkilendirme / Kimlik Doğrulama

Zayıf kimlik doğrulama ve yetkilendirme, kullanıcıların belirli işlevleri kimliksiz veya sahte kimlik altında yürütmesine izin vermesi demektir. Yani, kullanıcının uygulama içerisinde gerçekleştirdiği işlemleri eksik ya da hatalı

kullanmasından kaynaklanmaktadır. En basit örneği, 2012 yılında Dropbox uygulamasında yaşanan güvenlik zaafiyeti ve sonuçları oldu. Yaşanan bu sorundan dolayı, yüzlerce kişinin hesaplarına yetkisiz olarak girilebildiği ve gizli proje belgelerine erişilebildiği saptandı. [61] Bu ve benzeri sorunlar genellikle sunucu tarafında yer almayan ve bir mobil uygulama içerisinde alınan güvenlik kararlarından kaynaklanabileceğini gösterir. Olası bir durumda oluşabilecek sorunların başında,

- Çevrimdışı kimlik doğrulama, cihaz içerisindeki gizli ve ya kaydadeğer bilgilerin bulanabileceğini ve bu bilgilerin kişiyi doğrulayabilecek bilgiler olduğu ifade eder. Saldırgan bu bilgiler üzerinden, kullanıcının gizliliğini ayıklayabilir ve bilgileri kullanarak giriş sistemlerinde kullandığı kimlik doğrulama mekanizmalarını atlayabilir.
- Eğer kullanıcı zayıf bir parola kullanıyorsa 4 hanei PIN numarası gibi, uzaktan cihaza erişim saldırgan için çok da zor olmayacaktır.
- Kullandığı hesapları, tıpkı kendi kullanıyormuş gibi devralabilir,
- Gizlilik ihlali yaratabilir, erişimin kısıtlı olduğu alanlarda yetkisiz kişilerin kötü niyetle yer almasına yol açabilir,
- Ve bir başkasının bilgisine sahip saldırgan hileli işlemler yaparak asıl kullanıcıyı suçlu duruma düşürebileceği gibi, ciddi zararlarda verebilir.

Sorunu çözebilmek için, kullanıcıların benzersiz kimlik bilgilerini doğrulama sistemlerde kullanırken dikkatli olması ve paylaşmaktan kaçınılması gerekir. Mesela, IMEI, IMSI, UUID gibi bilgiler tekildir ve sadece o cihaza özeldir. Sahtekârlar tarafından, kolaylıkla çalınıp üretilebilirler.

VI. M6: Yetersiz Kriptografi / Kimlik Denetimi

Şifrelemenin güvensiz kullanımı, şifrelemeyi kullanan çoğu mobil uygulamada yaygındır. Hem zayıf şifreleme algoritmalarının kullanımı hem de cihazda depolanan veya aktarılan verilerin şifrelenmesindeki süreçleri ifade eder. Bu durumu farkeden bir saldırganın, uygulama verilerinin sahip olduğu şifreleme sistemini çözebileceğini, ardından cihaza fiziksel olarak erişebileceğini, cihazdaki başka bir uygulama ile bunu yapabileceğini ya da ağ üzerinden verileri edip okuyabileceğini gösterir. Uygulama geliştiricilerin yaptığı en büyük hata, özel şifreleme algoritması kullanmak yerine (RSA, 3DES gibi), zayıf ve kırılabilecek

[61] Dropbox gets hacked... again (http://www.zdnet.com/article/dropbox-gets-hacked-again/)

şifreleme algoritmalarını tercih etmesi (RC2, MD4, MD5, SHA1) ve bunları kullanırken yanlış kullanmasıdır.

VII. M7: İstemci Taraflı Enjeksiyon

Normalde, uygulamalar diğer kaynaklardan gelen girdilerin güvenli olduğunu varsayar, bu nedenle bu verilerin doğruluğunu kontrol etme zahmetinde bulunmazlar. Bu risk sınıfı içerisinde, bir mobil uygulamada bulunabilecek tüm kod düzeyindeki sorunlar ele alınır. Bu sorunlar, arabellek taşmasına, bellek erişimi sorunlarına veya kullanılan programlama diline özgü biçim dizesi saldırılarına izin verebilecek kodları içerir. Bu kategorideki saldırılar, kullanıcı aygıtı üzerinde sınırsız uzak kod çalıştırabilmesine ve aygıtta bulunan tüm bilgilere erişmesine olanak tanır. Bu yol ile yapıbilecek istismarlar arasında, kullanıcıya ait şifreleme anahtarları, özel veya hassas sayılabilecek API bilgilerini cihaz belleğinden okunmasıda yer almaktadır.

Saldırı sınıfına girebilecek en tehlikeli yollardan biriside, SQL Enjeksiyon yöntemidir. Bilindiği üzere, modern sayılabilecek çoğu web ve mobil uygulamalar, bilgilerini veritabanı denen birimler üzerinde saklayarak, yönetirler. Bu birimler çok katmanlıdır ve sonsuz sayılabilecek bilgiyi içerisinde barındırıp depolayabilirler. Çoğu zaman ilk istek, uygulamanın yerel veritabanına, oradam sunucuya gider. Mobil cihazlarda veritabanı olarak SQLite denen ufak boyutlu veritabanı kütüphanesi kullanılır. Veritabanlar ile iletişim halinde bulunabilemek için SQL denen bir sorgulama dili kullanılır. SQL Enjeksiyon yöntemi ise, bir salgırganın mobil uygulama içerisinde oluşturulan ve kulanıcı girdileri üzerinden alınan SQL sorgularını, manipüle eden girişimde bulunmasıdır. Bu değişiklik sırasında özel değişiklik ve ifadeler eklenerek, hedeflenen adrese ve altında yatan sisteme erişilmesi amaçlanır. Bu tip bir enjeksiyon, veritabanı üzerindeki diğer tüm verileri görebilme tehlikesi yaratır. Eğer, uygulama içerisinde birden fazla kullanıcı varsa bu daha tehlikeli bir durumdur. Siz ücretsiz bir yazılım kullanıyorsunuz, ama aynı veritabanı içerisinde ücretli bir uygulama kullanan birbaşka da olabilir. Siz, o kullanıcının bilgilerine bu risk yolunu kullanarak yetkisiz olarak ulaşabilir, değiştirdirebilir, silebilir veya bilgisi olmadan kullanabilirsiniz.

Diğer bir risk durumu, JavaScript Enjeksiyonudur. Cross-site scripting (XSS) yani "Siteler Arası Komut Dosyası Çalıştırma" saldırısı olarak da bilinmektedir. Bu saldırı tipi, mevcut web ve mobil uygulamalarında en tehlikeli ve yaygın güvenlik açıklarından birisi olarak kabul edilmektedir. Bu saldırıda, saldırgan hazırlamış olduğu zararlı Javascript kodunu, web sitesi üzerinde bulduğu bir açık ile kullanıcının web tarayıcı içerisinde çalıştırmasıdır. SQL Enjeksiyon metoduna biraz benzer, ama karakteristik özelliği bakımından sunucu tarafında herhangi bir zarara neden olmaz. Aksine, istasyon görevi görmektedir. Hazırlanmış olan zararlı javascript kodunun, kullanıcı web tarayıcı üzerinden çalışması, saldırının amacına ulaşması için yeterlidir. Saldırgan bu metodu, tipik çerez hırsızlığı, zararlı yazılım yayılması (solucan saldırısı), oturum saldırıları ve zararlı yönlendirmeyi başlatmak için kullanabilir. Yapılabilecek çözümler arasında web tarayıcı tarafında filtre kullanmak ve biraz da kullanıcının dikkatli olması sorunları azaltacaktır.

VIII. M8: Güvensiz Girdilierin Tetiklediği Hassas İşlemler

Bu risk faktörü biraz, SQL Enjeksiyon vs Cross-site scripting (XSS) yani "Siteler Arası Komut Dosyası Çalıştırma" saldırılarına da benzemektedir. Uygulama içerisinde bir sorun oluşmadığı sürece, oturum ve web tarayıcısının oluşturduğu çerez bilgilerine, ortam değişkenlerine ve gizli form alanları gibi girdilere, başka bir mekanizma tarafından ulaşılamayacağı ya da değiştirilemediğini varsayabiliriz. Öyleki, bu güveni sarsabilecek en yanlış hareket, yabancı bir kaynaktan gelebilecek girdilerin güvenilirliği kontrol edilmeden işleme alınmasıdır. Bu risk sonucu, cihaz içerinde şifreleme ve güvenlik sistemin işlevsini yitirmesi ve sistem bütünlüğünü sağlayan denetiminin düzgün çalışmaması durumları ortaya çıkmaktadır. Diyelim ki, sisteme bir saldırgan sızmış olsun. Bu risk faktörü üzerinden, sistem içerisinde özelleştirilmiş istemcileri yani sistemin diğer aktif olarak çalışan mekanizmalarını veya bu mekanizmaları tetikleyecek girdileri değiştirebilir. Ne kullanıcı tarafından, ne de sistem tarafından bu değişiklik tespit edilemez. Kimlik doğrulama ve yetkilendirme gibi güvenlik kararları, bu girdilerin değerlerine dayanarak yapıldığında, saldırganlar yazılımın güvenliğini de atlayabilir. Verebileceği zararların içerisinde hassas verilerin çalınmasının yanı sıra, bir uygulama üzerinden başka bir uygulamayı kontrol edebilme yetsine de sahip olabilirler. Bunun yanı sıra, saldırganlar bu yol ile mobil ağ bağlantı ve dns ayarları, web

tarayıcı oturum ve çerez bilgilerini, sistem yapılandırma dosyaları, SMS ve URL çağrıları gibi durumları'da kontrol edebilir. Bu sorunu önlemenin yolları vardır. En başta, alınabilecek her türlü bilginin doğru olduğu varsayılmayıp, sistem tarafından mutlaka geçerliliğinin kontrol edilmesi ve güvenlik kontrolünden geçirlimes gerekilmektedir.

IX. M9: Güvensiz Oturum Bilgisi

Mobil uygulamalar kesintisiz olarak kullanılabilmek için kullanıcıdan almış olduğu oturum tanımlama bilgilerini sistemde saklar ve kullanırlar. Diğer bir deyişle, uygulama üzerinde kimlik doğrulaması yapıldığı zaman, çoğu uygulama kullanıcıya bir oturum çerezi gönderir. Bu durum, kullanıcının tekrar kimlik doğrulaması yapılamasına gerek kalmadan kullanmaya devam etmesi sağlar. Web hizmetleri, kullanıcıdan almış olduğu oturum tanımlama bilgisini uygulamaya gönderir. Uygulama ise, almış olduğu bu oturum bilgisi doğrular ve tekrar bilgi talebinde bulunmadan web hizmetini kullanmasına izin verir. Örneğin bankacılık uygulamalarında şifremi hatırla seçeneğinin olduğunu görebiliriz. Kullanıcı aynı uygulamayı tekrar açtığında uygulama güvenlik bilgisi talep etmeden açılmaya devam edecektir. Bu mekanizmanın bazı güvenlik zafiyetleri bulunmaktadır. Öncelikle, uygulama içerisinde oturum bilgisinin şifrelenmiş olarak tutulması, uygulama ile sunucu arasındaki iletişimi dinlemekte olan saldırgan tarafından çok kolay okunabilir olmasına sebep olacaktır. Bu durum, saldırgan rolündeki kullanıcının, uygulama içerisinde girilebilecek her türlü bilgiyi görebilir ve okuyabilir durumuna getirecektir. Diğer bir sorun, sistemde oturum sonlanma süresinin tanımlı olmamasıdır. Kullanıcı tarafından oturum bilgisi yapılmış ama aktif olarak kullanılmayan bir uygulamanın, sistemde geçerli oturum sonlanma süresinin olmamasından dolayı bir başkası tarafından kullanılmaya devam ediliyor olmasıdır. Belirgin bir süre aktif değildiniz, sistem sizin durumunuzu bilemeyeceği için oturumu açık tutmaya devam edecektir. Farkında olmadan bir başkası kullanıcının banka hesaplarını görebilir veya onun adına işlemler gerçekleştirebilir. Bu riski en aza indirmenin en kolay yolu, geliştiricinin oturum bilgisini şifrelenmiş olarak saklaması gerekiyor.

X. M10: Uygulama Koruma Eksikliği

Mobil uygulamalara yönelik en büyük tehditler listesinde yer alan son maddedir. Bu işlem, uygulamaları kırmak ve kaynak koda erişmek için kullanılan

en yaygın yöntemlerden biridir. Bir saldırganın, gizli kalması gereken ya da uygulamada ayrıcalıklı erişim izin gerektiren dosyalara ulaşması ve onlardan bilgi alması son derece tehlikelidir. Bu açığı kullanan saldırgan, şifreleme algoritmalarına, gizli yöntem ve işlemlere erişmiş demektir. Riskleri aza indirmenin bazı yolları bulunmaktadır. Uygulama kodunun, güvenli olmayan ortamlarda tutulmaması gerekmektedir. Ayrıca, geliştircinin uygulama kodu içerisinde şifreleme sistemlerini kullanması hataları azaltacak. Uygulama içerisinde cihazın ne durumda olduğunun bilinmesi uygulama güvenliği için çok önemlidir. Jailbreak algılama yani sistemin getirdiği kısıtlamaların aşıp, cihazın kişiselleştirilmesine olanak tanımak işlemi, sertifika işlemleri ve hata ayıklayıcı algılama kontrollerinin doğru bir şekilde kullanılması gerekmektedir. Örneğin bankacılık uygulamasının hiçbir zaman Jailbreak (iOS) ve Rooting (Android) yapılmış sistemlerin içerisinde çalışmayı kabul etmemelidir. Nedeni, bankacılık ve finans sistemleri bu tür işlemlerin yapıldığı cihazlarda, uygulamaların kullanılmasını doğru ve güvenli bulmamaktadır. Nedeni, yapılan işlemler izlenebildiği gibi sahtekarlık yapılabilme ihtimali de bulunmaktadır.

10. Örnek Uygulama Analizi

Funny Videos 2017 isimli video izleme uygulaması da, zararlı bir malware yazılımıdır. Uygulama, cihaz üzerine kurulduktan sonra, kullanıcıların eğlenceli videolar izlemesine izin verir. Siz uygulama üzerinden normal bir şekilde video izlemeye başladığınızda, yazılım aktif olmaya başlıyor. Arka planda SMS mesajlarını erişebileceği gibi, banka bilgilerini çalabilecek görevlerle donatılmıştır. Bankacılık uygulamalarını tespit etmeye başlar ve bulabilecek uygulamaların kod kısmına kendisini yazılımın bir parçası olarak eklemesi bu görevlerden sadece biridir. Malware, cihazda yetki sahibi olabilmek ve herhangi bir şeyi kontrol edebilmek için, öncesinde kullanıcıdan yönetim izinleri istemektedir. Sonra, saldırgan önceden yapılandırılmış bir liste ile (aralarında türk bankalarında bulunduğu yaklaşık 425 adet bankacılık uygulamasının bulunduğu özel bir liste) cihazdaki uygulamaları tanıyarak, kullanıcıların arabirimini taklit edebiliyor.

Bu yazılım hedefindeki bankacılık uygulamaları, aşağıda görüldüğü gibi özel bir liste üzerinden taranır ve yapılacak saldırıda ona göre belirlenir.

com.garanti.cepbank
com.getingroup.mobilebank
com.teb
com.hsbc.hsbcukcmb
com.ing.mobile
com.paypal.here
com.vakifbank.mobile

Son olarak, kullanıcının sisteminde yer alan bankacılık uygulamaları, eğer ki yukarıdaki liste ile eşleşiyorsa ve birde en başta kullanıcıdan tam yetki almış ise uygulamanın iç kısmına önce kendisini bir kopyalar. Daha sonra, bankacılık uygulaması içerisinde bankaya erişim için girilen kullanıcı adı ve parola kısmını taklit ederek, kullanıcının kimlik bilgilerinin bir kopyasını kendine alır ve saldırgana iletir. [62] Uygulama analiz edildiği zaman,

Dosya Adı: neoidea.funvideos2017_1.4.apk
Paket Adı: neoidea.funvideos2017
Alınan İzinler:

- android.permission.INTERNET: Uygulamalara ağ bağlantını açma izni verir.
- android.permission.RECEIVE_BOOT_COMPLETED: Bir uygulamanın, sistem önyüklemesi tamamlandıktan sonra otomatik olarak başlamasına izin verir.
- android.permission.RECEIVE_SMS: Bir uygulamanın SMS mesajları almasına izin verir.
- android.permission.QUICKBOOT_POWERON: Ön yükleyicinin hızlı açılmasına izin verir.
- android.permission.READ_SMS: Bir uygulamanın SMS mesajlarını okumasına izin verir.
- android.permission.WAKE_LOCK: İşlemciyi uyku modundan veya ekranın karartmasından korumak için Güç Yöneticisi Uyandırma Kilitlerini kullanmaya izin verir.

[62] Banking malware in Google Play targeting many new apps (https://securify.nl/blog/SFY20170401/banking_malware_in_google_play_targeting_many_new_apps.html)

- android.permission.ACCESS_NETWORK_STATE: Uygulamalara, ağlar hakkındaki bilgilere erişme izni verir.
- android.permission.GET_ACCOUNTS: Hesaplar Hizmetindeki hesapların listesine erişim izni verir.
- android.permission.USE_CREDENTIALS: Bir uygulama, herhangi bir hesapta oturum açmak için kullanıcının kimlik bilgilerini kullanabilir.
- android.permission.WRITE_EXTERNAL_STORAGE: Bir uygulamaya harici depolama alanına yazma izni verir.
- android.permission.ACCESS_COARSE_LOCATION: Bir uygulamaya yaklaşık konuma erişme izni verir.
- android.permission.READ_EXTERNAL_STORAGE: Uygulamanın harici depolama ortamından okuma izni verir.

AntiVirüs Taraması:

- AegisLab - Troj.Banker.Androidos!c
- McAfee - GW-Edition Artemis
- Alibaba - A.H.Ste.BankBot.A
- Trustlook - Android.PUA.Riskware
- Symantec - Android.Malapp
- ESET - Android/Fobus.CH
- Avira - ANDROID/Fobus.hmwwb
- McAfee - Artemis!37DF8602DF01
- Cyren - ZIP/Trojan.ULET-9
- TrendMicro - Suspicious_GEN.F47V0412
- DrWeb - Android.Packed.1
- Kaspersky - HEUR
- Qihoo-360 - Android mobile malware
- ZoneAlarm - HEUR
- Ikarus - Trojan-Spy.AndroidOS.BankBot
- Fortinet - Android/Fobus.CH!tr
- Antiy-AVL - Trojan[Banker]/Android.Asacub

Bulgular:

- Geçici dosyalarda ve günlük dosyalarında saklanan hassas veriler,
  [IMEI, AndroidL] 339271562426717,339271562426717
- Hassas bilgi veya verilere cihazdaki diğer uygulamalar tarafından kolayca erişilebilebilmesi,
  - @android:name = neoidea.funvideos2017.injectionService
  - @android:name = neoidea.funvideos2017.wakeService
  - @android:name = neoidea.funvideos2017.dom_chang
- Uygulama hızlı bir şekilde analiz edilerek paketlenebilir ve değiştirilebilir.

11. Güvenilir Uygulama Kurulum Önerisi

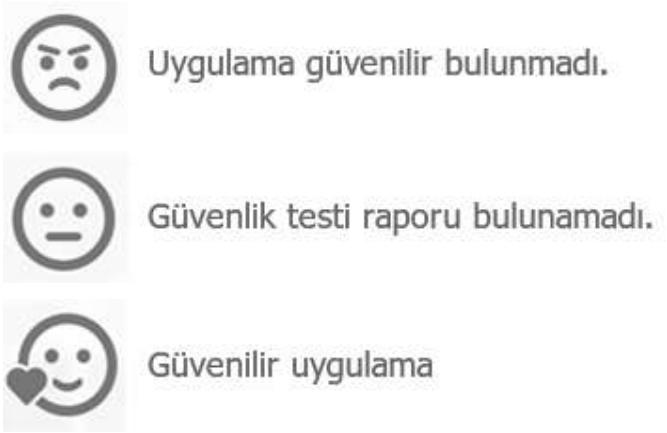
Uygulama marketlerinde yer alan her uygulama güvenilir değildir. Kullanıcılar cihazlarına yükledikleri uygulamaların neler yapabileceğini bilemedikleri gibi, arka tarafta habersizce işleyen mekanizmadan habersizdir. Bu durum tamamiyle geliştiricinin kontrolünde olan bir durumdur. Kullanıcı uygulamayı cihazına kurmaya başladığı anda, sistem içerisinde geliştirici için açık bir kapı aralanmış sayılır. Bu noktadan sonra sorulabilecek asıl soru, kontrol kullanıcıda mıdır yoksa uygulamayı geliştiren kişiyemi geçmiştir?

Kullanıcılar cihazlarında kurmak istediği uygulamayı seçmeden önce, uygulama hakkında fikir sahibi olabilmek adına, diğer kullanıcıların fikirlerinede başvururlar. Sosyal ortamlarda uygulama ile ilgili yapılan yorum ve paylaşılan deneyimler uygulamanın ne derece güvenilir olduğunu vurgulamaktadır. Gelebilecek her olumsuz yorum, uygulama için kötü bir not demektir. Ve bir başka kullanıcının karar verebilmesine yardımcı olur. Aksi durumlarda olabilir. Örneğin, çoğu kişinin olumlu olarak yorum yazdığı uygulama, denilenin aksine zararlı bir kod parçası da barındırabilir. Yapılan yorumların yanında, puanlama sistemi ve uygulama derecelendirme sistemi de kullanılabilir, hatta Google Play'de bu mevcuttur. Uygulama için yapılan yorumların paylaşılması, puanlama sistemi veya içerik seviyesi bir uygulamayı güvenilir kılmak için yeterlimidir, değildir elbette. Her kullanıcı bu bilgilerin doğruluğunu ölçemez ya da ne kadarı doğru bilemez. Uygulama marketleri biraz işin kolayında durarak, yönlendirmeleri yapılan deneyim ve ölçümlemelerle sağlamaktadır. Kendisi uygulama içeriğini kontrol etmediği gibi, zararlı mı onu da bilemez. Sadece, gelebilecek geri dönüşlerle hareket etmektedir. Öneri olarak şu yapılabilir, kullanıcılar bu bilgilerin

dışında uygulama marketinin yönlendirmesi ile de karar verebilmeli. Yani, uygulama marketi bu uygulama zararlı içerik barındırıyor ya da sorun görülemedi gibi bildirimleri kullanıcıya yansıtırsa, karar vermesinde yardımcı olabilir.

I. Bilgilendirme Tarafının Oluşturulması

Güvenlik mekanizmasının ilk aşaması şu şekilde çalışacaktır; kullanıcı yüklemek istediği uygulamanın market içerisindeki sayfasına girer ve orada uygulama ile ilgili bilgilerin bulunduğu bölümde uygulamanın güvenilirlik derecesini belirten 3 tip görsel betimleme ile karşılaşır. Bu görseller uygulamanın güven derecesini ya da daha öncesinde güvenlik testine girip girmediğini de belirtir.



i) Uygulama güvenilir bulunmadı.

Eğer daha önceden uygulama ile ilgili olumsuz bir test raporu ile yayınlandı ya da bildirildi ise uygulama güvenilir bulunmadı görseli, yükle butonunun yanında belirecektir. Kullanıcının detaylıca bilmesine gerek yoktur. Sadece, özet olarak kısa cümlelerle ne raporun ne demek istediği anlaşılabilir.

Örneğin,

- Uygulama tanımlanmayan bir URL adresine istek gönderiyor olabilir.
- İstek gönderilen URL adresi güvenilir (HTTPS) bir adres barındırmıyor.
- Erişim izinleri içerisinde bilinmeyen bir tanım geçmektedir.
- Uygulama cihaz üzerindeki SD karta erişmek istiyor.
- Uygulama ROOT yetkisi talep ediyor, gibi.
- Uygulama içerisinde uzaktan erişim gerektiren kod parçası bulundu.

- Uygulama malware olarak adlandırılan zararlı yazılım barındırmakta.
- Uygulama daha önceden zararlı yazılım sınıfında kara listeye alınan bir başka uygulama ile aynı türde kodlama içermekte, gibi.

Aynı zamanda bu testin zaman yapıldığı, kaç kişi tarafından talep edildiği, kaçının güvenilir bulduğunu da belirtmesi gerekir. Test bunun içindir. Uygulama marketi kullanıcıyı hiçbir şekilde zorlamamaktadır. Sadece bilgilendirme ve koruma amaçlı yapılan bu işlem kullanıcın yararınadır. Kullanıcı isterse yükleme işlemine devam eder, istemez ise etmez.

ii) Güvenlik testi raporu bulunmadı

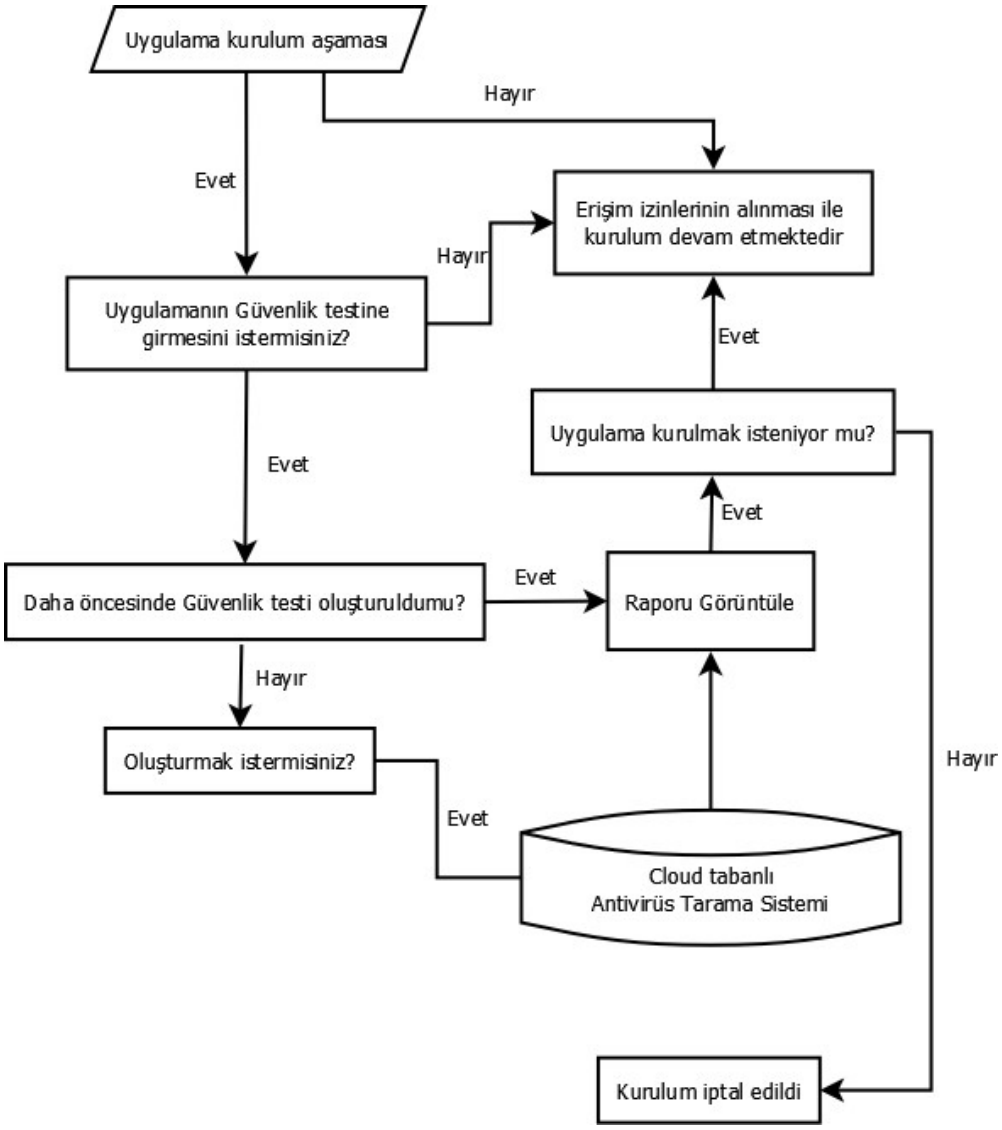
Her uygulama güvenlik testine girecek diye bir kaide yoktur. Eğer teste girmemiş bir uygulama yüklenmek isteniyorsa, bu simgeyi bilgilendir kısmının hemen yanında görebilir. Yeni bir test raporu oluşturulmak isteniyorsa 2 yol vardır, ya kullanıcı kurulum aşamasında bu isteği talep eder. Ya da bu görselin kullanıcı tarafından seçilmesi ile talep oluşturulmuş olur. Ancak, kullanıcının oluşturduğu bu talep için çok kısa süre beklemesi gerekebilir. Çünkü arka tarafta binlerce hatta milyonlarca başka istekler de olabileceği için, kullanıcı bu durumu biraz anlayışla karşılaması gerekmektedir.

iii) Güvenlir uygulama

Gerçekleştirilen güvenlik testi ve raporuna göre uygulama güvenlidir. Kullanıcı yeni bir istekte bulunarak bu talebi yinelebileceği gibi, rapor sonucuna bakarak da kurulum aşamasına geçebilir. Güvenlik testleri uygulama marketinin kendi bulut sunucularında güvenilir kaynaklar üzerinden yapılmaktadır. Sistemden çıkan sonuç, güvenirliği yansıtmıyorsa bu uygulama güvenilir olmadığının bir işareti olarak kabul edilir.

İkinci aşaması ise, kullanıcı uygulamayı cihazına kurmaya başladığı anda gerçekleşir. Kullanıcının yükle butona basmasıyla, kısa bir süre beklemenin ardından güvenlik testi akışı şemaya uygun olarak ilerlecekdir. Bu işlem erişim izninin alınmasından hemen önce başlayacağı için, kullanıcı uygulamayı yükle dediği anda nasıl bir aksiyon alabileceğini de bilmesi gerekiyor. İlk olarak bu uygulama için güvenlik testine sokulmak isteniyor mu, kullanıcıdan bu sorunun

cevabı istenir. Kullanıcı eğer evet der ve daha öncesinde bir rapor oluşturuldu ise kullanıcı bilgilendirmek adına ekranda gösterilir.



Şekil 30 Güvenilir uygulama kurulum modeli

Kullanıcı raporu inceler ve uygun görürse kurulum bir sonraki aşama olan erişim izinlerinin alınması ekranına geçer. Eğer raporu tekrarlamak istiyorsa kurulum işlemi tekrar başlar. Bu adım çok çok kısa süre bekleme ile geçebilir. Kullanıcıyı caydırmak adına, bu bilgilendirme yapılacaktır. Rapor sonucuna göre kullanıcı uygulamayı uygun görmüyorsa sistemine kurmak istemez ve işlemi iptal

ederek çıkar. Süreç uzun gibi görülebilir, ama tamamiyle kullanıcıyu korumak ve güvenliğini sağlamak adına yapılmış bir sistemdir.

II. Diğer Öneriler

- Erişim izinleri en güncel Android işletimine sahip (Android Marshmallow 6.0 ve üzeri versiyonlarda) cihazlarda tek model üzerinden alınıyor. Yani, her bir izin talebi için yeni bir izin ekranı kullanıcı ekranına geliyor. Haliyle kullanıcı neye, hangi duruma izin verdiği apaçık görebildiği gibi, izni uygulamayada kapatabiliyor. Ancak, eski sürüm cihazlarda (Android Lollipop 5.0 ve altındaki versiyonlarda) bu erişim izin talebi tek sayfada bir kez alınıp, bir daha sorulmamak üzere kullanıma geçilmektedir. Google tarafından bir defaya mahsus olmak üzere güncelleme çıkılarak bu sorunun önüne geçilebilir. Ve eski sürümler mobil cihazlarda izinler tıpkı yeni sürüm cihazlar gibi tek tek talep edilmeye başlayabilir.

- Uygulama marketleri içerisinde derecelendirme sistemleri kullanılıyor olabilir. Ya da, ebeveyn himayesinde görülmesi istenen içerikler de kısıtlanmış olabilir. Ancak, şu kısımda bir eksiklik var, ya kullanıcı kimseye bağlı değilse ne olacak? Yani, mobil cihaz kullanıcısı herhangi bir ebeveyn tarafından gözlemlenmiyor olabilir. Ya da, yaşı reşit ama uygun olmayan içerikleri görüntülemek istemiyordur. Öneri olarak şu olabilir. Yine Google örneği üzerinden gidecek olursak. Google kullanıcıların profillerini, hareketleri, eğer yeterli veri toplayabildi ise cinsiyetini ve ya yaşını da tahmin edebilir. Kullanıcının bir işlem yapmasına gerek kalmadan, filtrelemeyi kendi tarafında bu verilere göre yapması belki sorunları azaltacaktır. Zaten PEGI ya da ESRB gibi ölçümlerde uygulama seviyesi bilinebiliyor. Bu sistem temel alınarak içerik gösterimi de filtrelenebilir. Örneğin, 7 yaşından küçük bir çocuğun sosyal medya ile bir ilgisi olamaz. Uygulama ilk açıldığı anda uygulama marketi içerisinde sosyal medya ile ilgili uygulamaları göremesin. Ya da, 12 yaşından küçük ve ebeveyn kontrolü dışında cihaz kullanabilen kullanıcılar için şiddet seviyesi yüksek oyunlar görüntülenmesin. Bu tamamı ile uygulama marketin kontrolünde olabilecek bir sistem olması gerekiyor. Bu yapılır

ise, zararlı yazılımların yayılmasının önüne geçilebilir, veri kayıpları azalabilir ya da daha az kullancı zarar görebilir.

12. Sonuç

Bugün internet gibi küresel bir dünyayı küçük kalıplara içerisinde cebimizde taşıyabiliyoruz. Peki, kalıplara soktuğumuz akıllı cihazları ne kadar tanıyoruz?

Son zamanlarda akıllı telefon kullanıcıları, uygulamaları güncellerken sıklıkla cep telefonlarına gelen "izin isteği" problemi ile karşılaşmaktadır. Bunu onayladığında, cep telefonu uygulamalarının öncelikli erişim hedefi olan kullanıcı telefon rehberi, mesaj kutusu, albümü veya konum bilgisine erişilmesine izin vermiş demektir. Onaylamadığı takdirde ise uygulamayı sorunsuz bir şekilde indiremez veya kullanamaz. Fakat uygulama için erişim izni verdiğinde ise kullanıcının tüm özel bilgileri yazılımı geliştiren kişinin eline geçmektedir ve bu durum büyük bir güvenlik riski arz etmektedir.

Cihazın uygulama fonksiyonları içerisindeki tüm erişim izinleri, amacına göre uçuca birbine bağlı sayılabilir. Gerçekten gerektirdiği izinler dışında, bazıları vardır ki birleştirildiği zaman, kişisel bilgilerin sızmasına yol açabilir. Mesela, telefon rehberindeki tüm kayıtlara, uzaktan erişilebilir olsun. Bunun için öncelikle, telefon rehberinin uygulama üzerinden erişime açık olması gerekiyor. Aynı şekilde, uzaktan bağlantı sağlanabilmesi de gerekiyor ki, kullanıcının cihazını internet üzerinden erişilebilsin. Bu iki yetki birleştirildiği zaman, bu cihaza bu uygulama üzerinden verilen yetkiler ile telefon rehberine interneten sızabileceği fikri doğmaktadır.

Akıllı cihazlarda güvenlik konusu, her zaman önemli bir konu olarak kullanıcılara hatırlatılmaktadır. Sadece erişim izinlerine dikkat etmesi onu güvenli kılmaz. Cihazlarda PIN kod kullanımı, cihazın sahip olduğu işletim sisteminde bozulma olup olmaması (rooting ya da jailbreak), veri güvenliğinin sağlanması ya da yedeklenmesi, uygulamaların güvenilir kaynaklardan yüklemesi, ve kullanılan kablosuz iletişim ağının (WIFI) ne kadar güvenlir olduğunun sorgulanması kullanıcı güvenliği için en iyi olacaktır.

Sonuç olarak, kullanıcı bilgilerinin dışa aktarımı güvenlik zaafiyetir ve kullanıcı açısından tehlikeli bir durumdur. Çözüm olarak ne tür yöntem sunulursa sunulsun, telefon erişim izinlerinde, hemen her kullanıcıyı tehdit eden büyük bir tehlike söz konusudur. Bu yüzden kullanıcıları bilinçlendirmek, mobil teknolojilerde

kullanılan yazılım geliştirmelerinin güvenlik derecesini arttırmak ve hukuksal olarak da yasalarsa daha geniş kapsamlı yaptırımlar sunmak doğru bir yöntem olacaktır.

KAYNAKÇA

1. Trend Micro Inc. (2011) "When Android apps Want More Than They Need" http://www.trendmicro.co.uk/media/misc/when-android-apps-want-more-than-they-need-ebook-en.pdf
2. 3G ile 4.5G Arasındaki Farklar Nelerdir? https://www.btk.gov.tr/tr-TR/Sayfalar/3G-ile-45G-Arasindaki-Farklar-Nelerdir
3. EULA, https://en.wikipedia.org/wiki/End-user_license_agreement
4. Chan, P. P., Hui, L. C., & Yiu, S. M. (2012, April). Droidchecker: analyzing android applications for capability leak. In Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks (pp. 125-136). ACM.
5. Lenhart, A. (2009). Teens and mobile phones over the past five years: Pew Internet looks back.
6. Peterson, E. Y. A., & Warrick, J. (2014). Leaks of nude celebrity photos raise concerns about security of the cloud.
7. Park, Y. (2016). Up in the Cloud.
8. Pennsylvania Man Charged with Hacking Apple and Google E-Mail Accounts Belonging to More Than 100 People, Mostly Celebrities (https://www.justice.gov/usao-cdca/pr/pennsylvania-man-charged-hacking-apple-and-google-e-mail-accounts-belonging-more-100)
9. YETİM, S. (2015). UBER, HUKUKİ SORUNLAR VE ÇÖZÜM ÖNERİLERİ. Uyuşmazlık Mahkemesi Dergisi (6).
10. Google Play Hizmet Şartları (https://play.google.com/intl/tr_tr/about/play-terms.html)
11. WhatsApp'a da reklam geliyor (http://www.bbc.com/turkce/haberler-37190266)
12. Most of the Top iOS and Android Apps Have Been Cloned to Spread Malware in 2014 (http://news.softpedia.com/news/Most-of-Top-iOS-and-Android-Apps-Have-Been-Cloned-to-Spread-Malware-in-2014-465310.shtml)
13. GÜNGÖR, Murat. "ULUSAL BİLGİ GÜVENLİĞİ: STRATEJİ VE KURUMSAL YAPILANMA." (2015).
14. ÖğÜN, M. N., & Adem, K. A. Y. A. (2013). Siber güvenliğin milli güvenlik açısından önemi ve alınabilecek tedbirler. Güvenlik Stratejileri Dergisi, 9(18), 145-181.
15. Allen, S. G. Mobile Malware in the Enterprise.
16. What you need to know about the new Android vulnerability, "Stagefright"; (https://blog.lookout.com/blog/2015/07/28/stagefright/)
17. N.a (n.d.). Gartner Says More than 75 Percent of Mobile Applications will Fail Basic Security Tests Through 2015. Gartner.com. Retrieved from http://www.gartner.com/newsroom/id/2846017
18. Mobile Threat Report https://www.webroot.com/shared/pdf/WR_MobileThreatReport_v4_20140218101834_565288.pdf
19. Shea, V. ,What is Netiquette, http://www.albion.com/netiquette/introduction.html
20. Nazlı Alkan, Hakemli Yazılar Kütüphanecinin Felsefi Düşünme Eyleminin Önemi ve Etkileri, Türk Kütüphaneciliği 24, 4 (2010), 596-643
21. Robertson, K. (2008). An analysis of the video game regulation harmonization effort in the european union and its trans-atlantic chilling effect on constitutionally protected expression. BC Intell. Prop. & Tech. F., 2008, 90802-102902.
22. Robertson, K. (2008). An analysis of the video game regulation harmonization effort in the european union and its trans-atlantic chilling effect on constitutionally protected expression. BC Intell. Prop. & Tech. F., 2008, 90802-102902.
23. ESRB RATINGS GUIDE, https://www.esrb.org/ratings/ratings_guide.aspx
24. What is PEGI? http://www.pegi.info/en/index/id/28/
25. Gülbin Ayşı ATEŞ (2011). İletişim Alanında Çocuklara İlişkin Ulusal ve Uluslararası Hukuki Düzenlemelerin Değerlendirilmesi
26. Özhan, S. (2011). Dijital Oyunlarda Değerlendirme ve Sınıflandırma Sistemleri ve Türkiye Açısından Öneriler. Sosyal Politika Çalışmaları Dergisi, 25(25).

27. Security Threats and Defense Approaches in Wireless Sensor Networks: An Overview http://www.ijaiem.org/Volume2Issue3/IJAIEM-2013-03-15-033.pdf
28. Packet Sniffer Animated Simulator (http://williams.comp.ncat.edu/IA_visualization_labs/security_visual_tools/packet_sniffer/packet_sniffer.html)
29. Etaher, N., Weir, G. R., & Alazab, M. (2015, August). From zeus to zitmo: Trends in banking malware. In Trustcom/BigDataSE/ISPA, 2015 IEEE (Vol. 1, pp. 1386-1391). IEEE.
30. Uslu, T. (2007). İnternet güvenliği ve risk yönetimi (Doctoral dissertation, İstanbul Kültür Üniversitesi/Fen Bilimleri Enstitüsü/Bilgisayar Mühendisliği Anabilim Dalı).
31. Kaya, M. B. (2009). Türk hukukunda ve mukayeseli hukukta internet erişiminin engellenmesi (Doctoral dissertation, İstanbul Bilgi Üniversitesi).
32. OWASP - Open Web Application Security Project (https://www.owasp.org)
33. Are mobile apps a leaky tap in the enterprise? (https://www.zscaler.com/blogs/research/are-mobile-apps-leaky-tap-enterprise)
34. Phil, P. R. (2014). OWASP Top 10: The Top 10 Most Critical Web Application Security Threats Enhanced with Text Analytics and Content by PageKicker Robot Phil 73.
35. OWASP En iyi 10 Mobil Güvenlik Riskleri, ayrıntılı bilgi için bknz. https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
36. Kural, B. I. B. A. HSBC Şirket Bankacılığı.
37. Dropbox gets hacked ... again (http://www.zdnet.com/article/dropbox-gets-hacked-again/)
38. Banking malware in Google Play targeting many new apps (https://securify.nl/blog/SFY20170401/banking_malware_in_google_play_targeting_many_new_apps.html)