Akıllı Telefonlarda Gizlilik ve Mahremiyet: Durum Saptaması ve Öneriler

Enis Karaarslan[1], Meltem Demir[1], Vedat Fetah[2]

[1] Muğla Sıtkı Koçman Üniversitesi Bilgisayar Mühendisliği Bölümü, Muğla

[2] Ege Üniversitesi BİTAM Network Yönetim Grubu, İzmir

enis.karaarslan@mu.edu.tr , demirmeltem50@gmail.com , vedatfetah@gmail.com

Özet: Akıllı telefonlar hayatımızı kolaylaştırmakta ama aynı zamanda hayatımız hakkında çok çeşitli ve güncel bilgiler toparlamaktadır. Bu bilgilerin bizim isteğimiz dışında başka kişilerin eline geçme olasılığından dolayı hayatımızın gizliliği ve mahremiyetimiz ciddi bir tehlike altındadır. Bu çalışmada, akıllı telefonların ne tür bilgileri toparladıklarının tanımlanması hedeflenmiştir. Akıllı telefonlara yönelik ana tehditler ve saldırılara örnekler verilmiştir. Bu tür sistemlerde alınabilecek güvenlik ve mahremiyet önlemleri anlatılmıştır. Bu çalışmada ele alınan uygulamalar ve konfigürasyonlar MSKÜ NetSecLab Mobil Bilişim Labında (http://netseclab.mu.edu.tr/mdevlab.html) Android ortamında gerçekleştirilmiş ve edinilen deneyim paylaşılmıştır. Tasarımdan güvenli telefonlara örnekler verilmiştir. Bu çalışma bir durum tespiti yapmakla kalmayıp gizlilik ve mahremiyeti sağlamak için önerilerde bulunmayı hedeflemektedir.

Anahtar Kelime: mobil bilişim, akıllı telefon, Android, mahremiyet.

Privacy and Secrecy in Smart Phones: A Case Study and Recommendations

Abstract: Smart phones are making our lives easier, but they are also gathering various and updated information of our lives. Secrecy and privacy of our lives is under serious threat because of the possibility of our lives getting into the hands of persons other than our desire. This study aims to identify what type of information is gathered by the smartphones. Examples of the main threats and attacks on smartphones are given. Security and privacy measures that can be taken in such systems are described. Applications and configurations discussed in this study, are implemented on Android devices in the MSKU NetSecLab Mobile Computing Lab (http://netseclab.mu.edu.tr/mdevlab.html) and gained experiences are shared. Examples of phones which are secure by design are given. This study is not only a case study, but also aims to make recommendations to ensure confidentiality and privacy.

Keywords: mobile computing, smart phone, Android, privacy .

1. Giriş

Akıllı telefonlar, telefon ve görüntülü iletişim, internet, konum bilgileri, fotoğraf ve video gibi birçok hizmetle hayatlarımızı kolaylaştırmakta, hayatımızın vazgeçilmez bir parçası haline gelmektedir. Bu cihazların hayatımız hakkında toparladıkları bu bilgilerin çeşitliliği, güncelliği ve bu bilgiler ile oluşturabilecek kişisel profil çok önemlidir. Bu bilgilerin özellikle o anda bulunduğumuz konumumuz ile birleştirilmesi ile çok daha anlamlı hale gelmektedir. Kimlerle ne kadar sıklıkla ve ne zaman konuştuğumuz bilgisi de eklenmektedir. Bu bilgiler telefon servis sağlayıcısı, işletim sistemi ve programlar tarafından toplanmaktadır. Bu bilgilerin, bizim isteğimiz dışında başka kişilerin eline geçme olasılığından dolayı gizlilik ve mahremiyetimiz ciddi bir risk altındadır.

Bu çalışmada ilk bölümde konuyla ilgili temel kavramlar; toparlanılan veriler, ana tehditler ve saldırılar açıklanmıştır. Sonraki bölümde Android ortamında alınabilecek bazı uygulamalar ve konfigürasyonlar ele alınmıştır. İlerleyen bölümlerde mobil güvenlik için öneriler verilmiş ve tasarımdan güvenli telefonlara örnek verilmiştir.

2.Temel Kavramlar:

2.1. Gizlilik ve Mahremiyet

Gizlilik (confidentiality), bilginin yetkisiz kişilerin eline geçmeme ve yetkisiz erişime karşı korunmasıdır. Mahremiyet (privacy), ise bilginin uygun görülen kişiler dışındaki kişilerin görmesinden uzak tutulması durumu, isteğidir[9]. Burada bilginin gizliliğinden çok, o kişi için özel olması yani özel yaşama ait olması durumu vardır. Özel hayat hakkı, uluslararası sözleşmelerle korunan temel bir haktır. Kural olarak dokunulmaz, vazgeçilmez, devredilem ez niteliktedir, ancak yasayla sınırlanabilir ama bu sınırlama da hakkın özüne dokunulmayacak şekilde yapılmalıdır [10-11].

2.2. Mobil Bilişimin Veri Akışına Göre Modellenmesi

Akıllı cep telefonlarıyla Mobil bilişim, veri akışına göre aşağıdaki alt maddelerden oluşmaktadır:

- İşletim Sistemi
- Mobil cihazda bulunan sensör, kamera gibi donanımsal aparatlar.
- İşletim cihazı üzerinde çalışan uygulamalar
- Uygulamaların veri gönderip aldıkları dış sunucular
- İnternet Erişimi
- Yedekleme için bulut altyapısı
- Operatör üzerinden ses iletişimi

2.3 Mobil Cihazların Kaynaklara Erişim Yöntemleri:

Android işletim sisteminde uygulamalar kurulurken ihtiyaç duyacakları kaynakları belirtmekte ama ne zaman ve ne şekilde kullanacaklarını belirtmemektedir. Android'in yeni çıkan "M" yazılım versiyonunda[7] izin verilen kaynaklara(kamera, ses) programın erişimi sırasında gerekli kullanıcı bilgilendirmelerinin yapılacağı belirtilmiştir.

Bu özelliğin şu ana kadar olmaması ciddi bir eksiklikti, lakin bu yazılımın ancak bazı modellerde (nispeten yeni cihazlarda) çalışabileceği de ilginç bir detay olarak karşımıza çıkmaktadır.

Uygulamalar hangi tür bilgileri, ne için topladıklarını, hangi amaçlarla ve ne şekilde kullanacaklarını belirttikten sonra kullanıcıların rızasını istemelidir. Buna örnek teşkil edebilecek bir uygulama [3]'de verilmiştir**.**

2.4. Mobil cihazların toparladıkları bilgiler

Toparlanılan verileri, kimin toparladığına göre şu şekilde özetlemek mümkündür:

<u>İşletim sistemi tarafından toparlanılan veriler:</u> İşletim sistemleri birçok veri toparlamakta, toparlanılan verilerin silinmesi de çok kolay olmamaktadır. Bu konuda ayrıntı bir sonraki bölümde verilmiştir. Uygulamalarımızda test kullanıcı hesapları ile giriş yapılmıştır [8].

<u>Operatör tarafından toparlanılan veriler:</u> Cep telefonu operatörleri geriye yönelik olarak hattınızla ilgili tüm verileri (Kimlerle konuşulduğu, kimlerle mesajlaşıldığı, konumlarınız ve mobil veri (data) kullanılarak internette yapmış olduğunuz gezintilerin bir kopyasını) tutmaktadır.

<u>Uygulamalar tarafından toparlanılan veriler:</u> Uygulamalar konum bilgisi dahil olmak üzere programlar kurulurken erişim istedikleri kaynaklardan çok çeşitli bilgiler toplamaktadır.

2.5. Mobil Cihazlardaki Ana Tehditler ve Saldırılar

Ana tehditleri şu şekilde özetlemek mümkündür:

<u>Veri toparlama:</u> İşletim sistemi veya programlar aracılığı ile çeşitli verilerin toparlanması önemli bir tehdittir. Örneğin Antivirüs programları tüm verilerinizi taramaktadır ve telefonunuzda her şeye erişim iznine sahiptir [23]. Çeşitli markalar veya telefon servis sağlayıcılar, telefondan kaldırılamayan programları bir nevi ajan yazılım olarak kullanarak verilerinizi toparlamakta ve sizin kullanım alışkanlıklarınızı kayıt altına almaktadırlar.

Programların mahremiyet ayarlarının yeni işletim sistemi veya uygulama versiyonlarıyla değişmesi de ciddi sorunlardan birisidir.

Verilerin Silinememesi: Veriler gerçekte kolay bir şekilde silin(e)memektedir. Örneğin Android sistemlerinde, bir Google hesabına bağlı olmak gerektiği için; öncelikle var olan hesabın silinmesi için "Google Apps" in silinmesi ve farklı bir hesapla login olunması gerekmektedir. Böyle yapıldığında bile diğer birçok işletim sisteminde olduğu gibi Android sistemlerde de veriler temelli olarak silinememekte ve birçoğu geri döndürülebilmektedir. Cep telefonlarını farklı kılan, insanların içindeki verileri sildiklerini düşünerek bu cihazları satmalarıdır. Avast'ın bu konudaki çalışmasında[22], internet üzerinden satın alınan ikinci el Android cihazlardan çeşitli mahrem verilerin elde edilebileceği gösterilmiştir.

Internet erişim güvenliği: WiFi erişiminde internet ile cihaz arasına girilerek verilerinizin çalınması. Bunun yanı sıra, bağlantılarınızın servis sağlayıcılar tarafından kayıt altına alınması ve cevrimiçi mahremiyet sorunu.

Konum güvenliği: Telefon servis sağlayıcı ve birçok uygulama konum bilgisini toplamaktadır. Konum bilgisi kullanma izni alan uygulamalar aracılığıyla yapılan işlemlerde, konum bilgisinin diğer kullanıcılarla paylaşılması da söz konusu olmaktadır.

Sahte uygulama tehditi: Google Play Store'da sahte uygulamalar bulunabilir. Bu uygulamalar güvenlik için büyük tehdit. Konum, veri ve diğer bilgiler bu uygulamalar aracılığıyla kullanılabilir.

Cep telefonlarında olabilecek saldırılar çok çeşitlidir. Uzak saldırıların temelinde internet bağlantısı olan telefonlar üzerinden veri aktarımı vardır. Saldırganlar bu sayede cep telefonu mikrofonu ile ortam dinlemesi yapabilir, kameradan görüntü alabilir, gps ile konumu izleyebilir, telefon konuşmalarını detayları ile öğrenebilir, anlık mesajlaşma yazışmaları ile yazılanlar takip edilebilir. Telefon hattının kullanımı ile başkalarına saldırı düzenlenmesi de mümkündür.

3. Uygulama

Mobil cihazlarda kurulabilecek uygulamalar ve yapılabilecek konfigürasyonlarla güvenlik ve mahremiyeti bir seviyeye kadar sağlamak mümkündür. Şirketlerin internet trafiğini izleyerek nasıl kullanıcı profilleri oluşturdukları ve çevrimiçi mahremiyetin önemi bir önceki çalışmamızda[1] incelenmişti. Guardian Project (https://guardianproject.info/), mahremiyet ve güvenlik özellikleri içeren programların geliştirildiği ve ücretsiz olarak dağıtıldığı bir projedir. Bu bölümde bu projede geliştirilen yazılımlardan bazıları da tanıtılacaktır.

Bu bölümde özellikle Android sistemlerde yapılabilecekler örnek olarak verilecektir. Bu yazılımlar mobil cihazlarımıza kurulmuş ve denenmiştir. Ele alınacak uygulamalar aşağıdaki gibidir:

1. Saldırı uygulaması denemesi
2. Cihazda yönetici (root) olma
3. Cihazdaki verileri şifrelemek
4. İnternet Trafiğini Şifreleme Teknolojileri
5. Program İzinlerini Denetim Altında Tutmak
6. Sohbet ve Arama Motoru Programları

3.1 Saldırı Uygulaması Denemesi

Bir saldırı programı ile WiFi ile cihaz arasına girilerek verilerin çalınması denenmiştir. Kullanılan programın oldukça popüler bir yazılım olduğunu ve arayüz kullanımının kolaylığı nedeniyle tercih edildiğini belirtmek isteriz. Bu programın ile yapılabilecekler şunlardır:

1. Ortadaki adam (Man In The Middle) saldırısı yapılabilmektedir. Bu sayede bağlı bulunulan wi-fi router'ın diğer kullanıcılarının trafiği izlenebilmektedir.
2. SSL strip özelliği ile sslli siteleri http sitelere yönlendirebilmektedir. Bu sayede kullandığınız google facebook gibi uygulamaların ssl bağlantılarını düşürmeye zorlayarak düz metin formatında şifrelerinizin ve verilerinizin gitmesini sağlamaktadır.
3. İstediğiniz bir adresi istediğiniz bir ip adresine yönlendirmek,

4. Değiştirilmesi istenilen bir resmi kendi belirlediğiniz resim ile değiştirmek,
5. İndirilen bir dosyayı kendinize de çekmek,
6. İndirilmesi istenilen dosyanın sizin istediğiniz bir dosya ile değiştirmek,
7. İstenilen web sayfasının içerisine önceden hazırlanan html kodunu enjekte etmektir.

3.2. Cihazda Yönetici (root) Olma

Mobil cihazlar yönetici (root) yetkisine sahip olmadan satılır. Satın alınan cihazın sistemi üzerinde değişiklik yapılamaz, verilen sistemi kullanılmak mecburiyetindedir. Üretici şirketler bunu bir tür güvenlik önlemi olarak görmektedir. Linux işletim sistemlerinde root olmak , yönetici (administrator) olmaktır. Root, sistem dosyalarının bulunduğu kök dizine ulaşmamızı sağlar böylece sistem üzerinde her türlü hakimiyet kurmak, örneğin dosyaları değiştirme, silme gibi yetkilere sahip olunacaktır.

Mobil cihazlarda yönetici olmanın faydaları aşağıdaki gibidir:

- Farklı bir işletim sistemi (rom) yüklenebilir,
- Kök dizindeki tüm dosyaları görülebilir,
- Uygulamaların performansı arttırabilir,
- Güvenlik önlemleri arttırabilir. Size karşı saldırıları önleyebilecek uygulamalar yüklenebilir.

Android cihazlara farklı bir işletim sistemi kurulabilir. Aynı şekilde iphone marka cihazlarda "jailbreak" denilen yöntemle yeni ve telefon üzerinde tam hakimiyet sağlayabilecek bir özellik eklemiş olursunuz. Android cihazlarda bu işleme root'lama denilmektedir. Donanım üzerinde yazılımı rootlamak iki şekilde olabilir:

1. Cihazınız üzerinde bulunan sistem değiştirilmeden root yetkilerini açılabilir.
2. Rootlanmış özel romlar kurularak yapılabilir.

Alternatif işletim sistemi kurmanın bazı sakıncaları olabilir:

- Cihazınızın garanti kapsamı dışında kalmasına neden olursunuz.
- Bir aksilik durumunda telefonunuzun bir daha açılamayacağı riskini göz önünde bulundurmanız gerekmektedir.
- Bazı ülkelerde bu işlem yasadışı olabilir.

Cihazların çoğunluğu root'lanabilir. Bu işlem telefon şirketleri tarafından onaylanmadığı için root olmak için yapılması gerekenler vardır. Uygulama örneği olarak, cyanogenmod anlatılacaktır. Android işletim sisteminde cyanogenmod yüklenerek telefon rootlanabilir. Cyanogenmod yükleyerek cihazda saf ve güncel bir Android deneyimi sağlanmaktadır. Yapılabilecekler aşağıdaki gibidir:

- İstenilen uygulamalar (Dağıtıcının ve ağ operatörünün kaldırılamayan yazılımları dahil) kaldırılabilir hale gelecektir.
- İletişim geçmişi telefonunuza kaydedilmemektedir. Bu özelliği sağlayan anonimleştirmiş özel bir modu vardır.
- Yüklenen cihaz OTA (over transfer air) destekleyeceği için artık çok hızlı bir şekilde telefonunuzu flashlamadan yeni android sürümlerine hızlıca geçilebilinecektir.

Bu hız cihaz üreticisinin yeni işletim sistemini yayımlamasından önce bile sistemi güncellemek anlamına gelmektedir.

3.3. Cihazdaki Verileri Şifrelemek

Cihazın farklı kişilerin eline geçmesi durumunu düşünerek (çalınma, satılma, anlık kullanma vb) gizliliği sağlamak için verileri şifrelemek gerekmektedir. Tüm diski şifreleme özelliğinin Android 6 Marshmallow ile yapılacağı söylenmektedir. Sadece telefonu şifreleme yöntemleri yeterli olmayabilir, dosyaları, uygulamaları da şifrelemeliyiz[25]. Sd card gibi çıkarılabilen bellekler özellikle şifrelenmelidir. Android'in güvenlik ayarları üzerinden bunu gerçekleştirmek mümkündür[24]. Yedekleme anında iletilen verileri şifrelemek için kullanılabilecek yazılımlar bir sonraki bölümde ele alınmıştır.

3.4. İnternet Trafiğini Şifreleme ve Anonimleştirme Teknolojileri

İnternet trafiğini şifrelemek ve interneti daha güvenli kullanmak için yöntemler bulunmaktadır. Kullanımı kolay ve çoğu ücretsizdir. İnternet trafiğini şifreleme ve anonimliğini sağlamak için aşağıdaki çözümlerden söz etmemiz mümkündür:

- Tor
- Vpn
- Şifreleme Yazılımları

TOR

Tor ağı hali hazırda görünmez olarak surf yapmanıza izin verir. Uygulamaları tor network ünde şifreleyerek yeriniz belli olmadan kullanmaya olanak sağlar. Bu işlem için Orbot [16], Orweb[17] yada Gibberbot[18] gibi yazılımları mobil cihaza kurmak gereklidir. Bu sayede mobil cihazınızda kullanacağınız bütün uygulamalar rastgele seçilen tor sunucuları üzerinden gönderilebilecektir.

Orbot'a yönetici erişimi "superuser acess" vermek için "rooted" bir cihaza ihtiyacınız olmaktadır. Cihazı ancak "root"layınca "Transparent Proxying" özelliği gelecek ve bütün trafik tor altyapısından gönderilecektir. Aksi taktirde Orbot'a uyumlu yazılımlar kurulması gerekmektedir. Örneğin Firefox için [20] de anlatılan privacy ayarlarının yapılması ve özellikle "ProxyMob" eklentisinin kurulması önerilmeketdir.

VPN

Kimlik gizleme yazılımları arasında en popüler olan diğer bir uygulama ise vpn ağına dahil olmaktır. VPN, Virtual Private Network (Sanal Özel Ağ) internete başka bir IP adresi üzerinden bağlanmayı sağlar. VPN, bağlantıları gizli ve güvenli hale getirir. Herhangi bir ağa bağlanırken kimliği gizler ve bağlanıyı şifreler. Bu işlemi yapabilmek için mobil cihaza vpn hizmeti veren firmaların sağladığı vpn client [19] yazılımlarını kurmak gereklidir. Hotspot shield en yaygın olarak kullanılan bilinen yazılımdır. Hotspot Shield cihazınızı Amerika'daki sunucular üzerinden bağlayarak tüm sitelere girmenizi sağlar.

Şifreleme Yazılımları

Tor ve Vpn kullanılmadığında, kişisel verilerini bulut üzerinde çeşitli depolama hizmetlerinde (Gdrive, dropbox ...) tutmak isteyenler için bu verileri internet üzerinden şifreli bir şekilde iletmeye yarayacak olan çeşitli şifreleme yazılımları vardır. Örneğin BoxCryptor yazılımı AES-256 ile verilerinizi şifreleyerek güvenli bir şekilde indirme ve gönderme işlemleri yapmaya olanak sağlamaktadır. BoxCrytor gibi kullanılan birçok yazılım bulunmaktadır. Android için kullanılan Cloudfogger[21] yazılımı da Dropbox, SkyDrive gibi birçok bulut depolama sağlayıcılarında şifrelemeyi sağlar.

3.5. Program İzinlerini Denetim Altında Tutmak

Privacy Guard[15] özelliği ile uygulamaların istediğiniz izinleri kullanmasına, diğerlerini kullanamasına neden olacaktır. Bu uygulamanın temeli aslında ilk android özelliklerinden App Ops'a dayanır. Google bu özelliği şu anki sürümlerde devreden çıkartmıştır. Bu özellik İOS kullanan cihazların temelinde bulunan özelliktir. İzinlerini engellediğiniz uygulama bu izinlerin dışına çıkmaya çalışırsa uygulama sizi direkt uyarmaktadır. Bu sayede uygulama yeniden gözden geçirilebilir.

3.6. Sohbet ve Arama Motoru Programları

Şifreli mesajlaşma için çeşitli programlar bulunmaktadır. Örneğin Chatsecure, şifreli mesajlaşma özelliği bulunmaktadır ve Orbot uyumludur. Telegram programının ise mahremiyet özelliği ve şifreli mesajlaşma özellikleri bulunmaktadır. Arama Motoru olarak Orbot uyumlu olan DuckDuckGo'dan söz edilebilir.

4. Mobil Güvenlik İçin Öneriler:

Akıllı telefonlar vazgeçilmeziniz olmamalıdır. Bu tür cihazlar etkin kullanıldığında, bir nevi zihniniz gibi sizin hakkınızda çok fazla bilgi içermeye başlamaktadır. Bu nedenle, sorun yaşamamanız için düzenli olarak yedeklemeniz ve çok önemli verilerinizi asla sadece telefonunuzda tutmamanız ilk kuraldır.

Güvenlik için verilebilecek önerileri şu şekilde özetlemek mümkündür:

- Özel verileri tutmamak: Bu cihazların başkalarının eline geçmesi durumunda sorun yaşamamak için gizli ve mahrem bilgiler telefonda tutulmamalıdır,
- Güvenlik kilitlerini etkinleştirmek: Cihaza fiziksel erişim durumunda, başka kişilerin telefonunuzu ele alıp zararlı yazılım yüklemelerine engel olacaktır. Tam bir koruma olmasa da size zaman kazandırır.
- Varsayılan güvenlik ayarları: Telefonunuzun varsayılan güvenlik ayarlarını değiştirmeyin (Ayarlar -> Gizlilik), çünkü telefon üzerinde yapılan bu gibi değişiklikler telefonu saldırılara karşı güvensiz hale getirebilir. Varsayılan güvenlik ayarlarında harici programların yüklemesi kapalıdır. Bu özellik kapalıyken uzaktan veya başka bir şekilde uygulama kurmak mümkün olmayacaktır. Bu ayarın değiştirilmemesi önerilmektedir.
- Güvenilir olmayan uygulama yüklememek: Market dışındaki (güvenilmeyen) kaynaklardan uygulama yüklemek beraberinde büyük güvenlik riskleri getirecektir. Mümkünse bundan kaçınılmalıdır.
- Uzaktan veri silme ve kilitleme özelliği aktive edilmelidir. Bu özellikleri kullanarak, kayıp ya da çalıntı olma durumunda kişisel verilerinizin başkalarının ellerine geçmesini engellemek mümkün olabilmektedir.
- Kablosuz ağ kullanımı: Kablosuz ağ kullanımında bankacılık gibi önemli verilerin kullanıldığı uygulamalar mümkünse kullanılmamalıdır. Kullanılması gerektiğinde şifre üreten farklı donanımlar kullanılmalıdır. Aksi takdirde birçok saldırı yöntemiyle bütün verileriniz, şifreleriniz başkaları tarafından ele geçirilebilir.
- Çevrimiçi mahremiyet programları: Çevrimiçi mahremiyet bir önceki çalışmamızda[1] ayrıntılı olarak incelenmişti. Mobil operatörlerin internet izlemelerinden kurtulmak için bir önceki bölümde anlattığımız mahremiyet programları kullanılmalıdır. Tor veya vpn benzeri kimlik gizleme yazılımları buna örnek olarak verilebilir. Veriler şifreli olarak gönderildiği için iletişimde araya giren ya da girmeye çalışanların gönderdiğiniz verileri izlemesini ve internet ortamına gireceğiniz her şeyin filtrelerle izlenmesini engelleyecektir.
- İnterneti ve gps'i kullanmadığınız durumlarda kapalı tutun. Bu hem pil ömrünüzü uzatacaktır hem de farkında olmadan telefonunuz ile sizden veri çalınmasını engelleyecektir.
- Hediye telefon almayın. En büyük tehlikelerden birisi de hediye olarak verilen telefonlara önceden yüklenen izleme yazılımlarıdır.

5. Tasarımdan Güvenli Telefonlar

Güvenlik ve mahremiyetin tasarım sürecinden itibaren dikkate alındığı çözümler bulunmaktadır. Blackphone ve "Privacy Phone" gibi donanım+yazılım ürünleri mevcuttur [4-6]. Örneğin Blackphone[13], güvenlik ve mahremiyet özelliklerine sahip bir telefondur. Blackphone, Android'den fork edilen ama açık kaynak olmayan PrivatOS[14] işletim sistemini kullanmaktadır. Ana özellikler olarak şunlardan söz edilebilir; anonim arama, mahremiyet özelliği aktif edilmiş uygulamalar, güvenilir hotspot'lar dışındaki Wi-Fi noktalarına bağlanmama, uygulama izinlerinde daha fazla kontrol ve özel iletişim (arama, kısa mesajlaşma, video sohbet, web, dosya paylaşımı ve konferans aramaları)dır [14].

Richard Stallman'in birçok konuşmasında da belirttiği üzere, mahremiyetten söz edilmesi için açık kaynak kodu destekleyen özgür yazılımların kullanılması gerekmektedir. Açık kaynak kodlu mobil işletim sistemleri bulunmakla birlikte[26], bu işletim sistemleri henüz olgunlaşmış değildir.

6. Sonuç

Mobil cihazlar, toplayabildikleri verilerin çeşitliliği ve bu verilerin bir araya getirilmesi ile oluşturdukları kullanıcı profilleri açısından ciddi bir mahremiyet sorunu oluşturmaktadır. Cihazlarda yapılabilecek ayarlarla toplanan verileri bir miktar azaltmak mümkündür. Yine de işletim sistemleri her koşulda veri toparlayabilmektedir. Bu cihazlara özgür yazılım lisansını destekleyen işletim sistemleri ve programları kurularak mahremiyet seviyesi arttırılabilir.

Bu tür uygulamalar günümüzde artmaktadır, bu çözümleri daha da geliştirmek mümkündür. Sonraki çalışmalarımızda farklı işletim sistemi çözümlerini ve bu çözümlerin karşılaştırılmasını vermeyi hedeflemekteyiz. Bu konuda bir cep telefonu üreticisiyle birlikte ortak bir çalışma sürecimiz de bulunmaktadır.

Kaynaklar

[1] Karaarslan E., Eren M.B. , Koç S., **Çevrimiçi Mahremiyet: Teknik ve Hukuki İncelemesi**, inet-tr 2014.

[2] The Problem with Mobile Phones, https://ssd.eff.org/en/module/problem-mobile-phones

[3] Privacy Dashboard, http://privacydashboard.s3.amazonaws.com/index.html

[4] Blackphone vs. FreedomPop's Privacy Phone: Security Showdown, http://www.tomsguide.com/us/blackphone-vs-freedompop-privacy-phone,news-18427.html, 10 Kasım 2015 tarihinde erişildi.

[5] FreedomPop, https://www.freedompop.com/theprivacyphone, 10 Kasım 2015 tarihinde erişildi.

[6] FreedomPop Announces The Privacy Phone, A Fully-Encrypted Smartphone For $10 A Month,

http://techcrunch.com/2014/03/04/freedompop-announces-the-privacy-phone-a-k-a-the-snowden-phone-a-k-a-the-terrorist-phone/, 10 Kasım 2015 tarihinde erişildi.

[7] Android 6.0 Marshmallow review: improved performance, battery life and features,

https://www.androidpit.com/android-m-release-date-news-features-name, 10 Kasım 2015 tarihinde erişildi.

[8] How to Log Out Of Google in Android, https://www.maketecheasier.com/log-out-of-google-in-android/, 10 Kasım 2015 tarihinde erişildi.

[9] Kaufman, Charlie, Radia Perlman, and Mike Speciner. ***Network security: private communication in a public world*. Prentice Hall Press**, 2002.

[10] Korkmaz, Ali. "**İnsan Hakları Bağlamında Özel Hayatın Gizliliği Ve Korunması**.", 2014

[11] Sevimli, K. Ahmet**, İşçinin Özel Yaşamına Müdahalenin Sınırları**, Legal Yayıncılık,İstanbul, 2006.

[12] Android Pay, https://www.android.com/pay/, 22 Ekim 2015 tarihinde erişildi.

[13] Blackphone, https://en.wikipedia.org/wiki/Blackphone, 22 Ekim 2015 tarihinde erişildi.

[14] PrivatOS, https://en.wikipedia.org/wiki/PrivatOS, 22 Ekim 2015 tarihinde erişildi.

[15] Privacy Guard, https://tr.wikipedia.org/wiki/GNU_Privacy_Guard, 24 Ekim 2015 tarihinde erişildi.

[16] Orbot, https://play.google.com/store/apps/details?id=org.torproject.android&hl=tr, 24 Ekim 2015 tarihinde erişildi.

[17] Orweb, https://play.google.com/store/apps/details?id=info.guardianproject.browser&hl=tr, 24 Ekim 2015 tarihinde erişildi.

[18] Gibberbot, **http://thgtr.com/guvenlik-gizlilik-uygulamalari-ve-eklentileri/18**, 24 Ekim 2015 tarihinde erişildi.

[19] VPN, http://www.vpnnedir.org/vpn/vnp-client, 24 Ekim 2015 tarihinde erişildi.

[20] Firefox Mobile: Privacy Enhanced, https://guardianproject.info/apps/firefoxprivacy/, 24 Ekim 2015 tarihinde erişildi.

[21] Şifreleme Yazılımları, https://www.cloudfogger.com/en/, 10 Kasım 2015 tarihinde erişildi.

[22]Verilerin Silinememesi, https://blog.avast.com/2014/07/08/tens-of-thousands-of-americans-sell-themselves-online-every-day/ 10 Kasım 2015 tarihinde erişildi.

[23] Antivirüs Programları, http://www.ilkehaber.com/haber/antivirus-programlari-guvenli-mi-11895.htm , 10 Kasım 2015 tarihinde erişildi.

[24] How To Encrypt Your Android Phone's External SD Card, http://www.techverse.net/encrypt-android-phones-external-sd-card/

[25]Cihazdaki Verileri Şifreleme, http://www.gezginler.net/android/cm-security-uygulama-kilitleme.html, 11 Kasım 2015 de erişildi.

[26] List of open-source mobile phones,

https://en.wikipedia.org/wiki/List_of_open-source_mobile_phones