Mobil Uygulamaların Güvenliği ve Mobil Yaşam

Hanım Eken1
1 TÜRKSAT, Kurumsal Bilgi ve Siber Güvenlik Yönetimi Direktörlüğü, Ankara
eken.hanim@gmail.com

Özet: Mobil cihazların artması ve internetin mobil cihazlarda kullanılmasının artması ile mobil uygulamaların kullanımı artmaktadır. Mobil cihazların taşınmasının ve kullanılmasının kolay olması ile insanların yaşamının her alanında yer almaktadır. Bu nedenle günümüzde mobil yaşam büyük önem taşımaktadır. Uygulamaların hızla artması ile mobil uygulamaların güvenliği de önemli hale gelmektedir. Çünkü mobil cihazları kişiler kişisel bilgilerini içeren uygulamalar içinde kullanılmaktadır. Bu nedenle mobil uygulamaların güvenliği daha önemli hale gelmiştir. Bu tür uygulamaların bilgi güvenliği açısından zafiyet içermesi güvenlik açısından daha büyük risk oluşturmaktadır. Bu çalışmada mobil uygulamaların insanların yaşamındaki yerinden ve mobil uygulamaların güvenliğinin sağlanması için ne gibi önlemlerin alınması gerektiğinden bahsedilmektedir. Öncellikle mobil cihazların insanların hayatındaki yerinden örneğin yolda yürürken, toplantıda, yemekte, toplu taşımada devamlı akıllı telefonlarla veya mobil cihazların insanların hayatında nasıl yer aldığından bahsedilecektir.

Daha sonra mobil işletim sistemleri hakkında bilgi verilecektir. Mobil uygulamalara yapılan saldırı türlerinden bahsedilecektir. Mobil uygulamaların ne gibi riskleri barındırdığı konusunda bilgi verilecektir. Mobil uygulamalarda yer alan güvenlik açıklıklarından bahsedilecektir. Yer alan güvenlik açıklıkları için neler yapılması gerektiğinden ne gibi güvenlik önlemleri alınması gerektiğinden bahsedilecektir. Mobil cihazların kişilerin aynı zamanda kişisel cihazları olduğu ve kafelerde, havalimanlarında, otellerde kullanıldığı için insanların kişisel bilgilerini korumak için ne gibi önlemler alması gerektiğinden bahsedilecektir.

Anahtar Sözcükler: Mobil, Mobil Yaşam, Mobil Cihazlar, Mobil Uygulamalar, Mobil Uygulamaların Güvenliği

Abstract: The use of mobile applications increase with the increasing use of mobile devices and the internet on mobile devices is increasing. With the ease of use of the transport of mobile devices and is located in all areas of people's lives. Nowadays, it is therefore of great importance mobile life. Security of mobile applications with increasing number of applications are becoming important. Because mobile devices are used in applications involving people's personal information. Therefore, the security of the mobile application has become more important. Contain weaknesses of such practices in terms of information security is a greater risk in terms of security. In this study, what measures such as to ensure the security of mobile applications and mobile applications over the life of the people is mentioned as necessary. Foremost over the life of the people walking on the way of mobile devices, meeting, dinner, will discuss how being involved with the continuous public transport smart phone or mobile device in people's lives.

1. Giriş

Teknolojinin gelişmesi ile elektronik cihazlar değişerek gelişiyor. Ayrıca elektronik cihazlar küçülmeye başlıyor. Elektronik cihazlar konusunda en büyük değişim bilişim sektöründe yaşanıyor. Bilgisayarlar giderek küçülmesi ile rahat taşıyabileceğimiz hatta cebimize koyabilecek boyutlara kadar küçülmüştür. Bu cihazlar hayatımızda mobil cihazlar olarak yerini almıştır. Gündelik yaşamımıza giren ve hayatımızı kolaylaştıran ilk mobil cihaz cep telefonlarıdır.

Cep telefonları ilk olarak dünyada 1983 yılında kullanılmaya başlanılmıştır. Fakat ağırlıkları sebebiyle taşıma amaçlı kullanılmamıştır. Boyutlarının küçülmesi ile hafiflemiştir. Şimdi ise hayatımızın vazgeçilmez bir parçası olmuştur.

Türkiye'de ise ilk cep telefonu görüşmesi 23 Şubat 1994 tarihinde gerçekleşti. Dönemin Cumhurbaşkanı Süleyman Demirel ve Başbakanı Tansu Çiller cep telefonundan ilk görüşmeyi yapmışlardır[1].

Cep telefonun ilk büyük adım ise 1994'te ilk cep telefonu operatörü Turkcell'in sektöre girmesi ile olmuştur. İlk başlarda hem boyut olarak büyük olan hem de ağırlıkları fazla olan cep telefonların küçülmesi ile kullanımı da yaygınlaşmıştır. Ericson marka cep telefonunu markasından sonra Nokia'nında Türkiye pazarına girmesi ile cep telefonu kullanıcısında büyük artış görülmüştür. Günümüzde 65 milyon SIM kart ve 35 Milyon'da cep telefonu kullanıcısı olduğu tahmin ediliyor[1].

Günümüzde ise cep telefonların gelişmesi ile birçok özellik eklenmiş ve akıllı telefonlar olarak insanların kişisel bilgisayarı haline gelmiştir. Ayrıca akıllı cep telefonlarının yanında birçok mobil cihazlar üretilmiştir. Bu cihazları insanlar kullanmaktadır.

Bu çalışmada mobil işletim sistemlerinden, mobil cihazlara yapılan saldırılardan, mobil cihazları saldırılardan korumak alınması gereken önlemlerden bahsedilecektir.

2. Mobil İşletim Sistemleri

Mobil işletim sistemlerinin geliştirilmesi ile akıllı cep telefonların üretilmesine başlanmıştır. Ayrıca tabletler ve diğer mobil cihazlarda bu işletim sistemleri bulunmaktadır.

Geçmişte ve günümüzde mevcut olan mobil işletim sistemleri şunlardır: [2]

- Google: Android
- Apple:Iphone OS (iOS)
- Microsoft :Windows Mobile
- RIM :BlackBerry OS
- Symbian Vakfı :Symbian
- Palm :Web OS
- Linux Vakfı :MeeGo
- Samsung :Bada

Android

Gooogle,Open Handset Alliance ve özgür yazılım topluluğu tarafından geliştirilen Linux tabanlı, mobil cihaz ve cep telefonları için geliştirilmiş olan mobil işletim sistemidir.
Android, aygıtların fonksiyonelliğini genişleten uygulamalar yazan geniş bir geliştirici grubuna sahiptir. Android için halihazırda 1 milyondan fazla uygulama bulunmaktadır. Google Play Store ise, Android işletim sistemi uygulamalarının çeşitli sitelerden indirilebilmesinin yanı sıra, Google tarafından işletilen kurumsal uygulama mağazasıdır. Geliştiriciler, ilk olarak aygıtı, Google'ın Java kütüphanesi aracılığıyla kontrol ederek Java dilinde yazmışlardır.

iOS

Apple tarafından geliştirilen Mac OS X (Unix türevli) işletim sistemi ailesinden gelmiştir. Apple marka mobil cihazlar için özel tasarlanmıştır. Sadece parmak etkileşimi ile çalışacak biçimde tasarlanmıştır. Çoklu dokunma özelliğini desteklemektedir[2].

Windows Mobile

Windows CE (Compact Edition) çekirdeklidir. İleri düzey altyapıya sahip olması ve Windows tabanlı olmasına rağmen masaüstünde kullanılan Windows uygulamalarını çalıştıramaz. Tescilli bir işletim sistemidir fakat değişik üreticilerin ürünlerinde de bulunabilir[2].
Diğer cihazlarla da uyumlu olması gerektiğinden optimizasyon miktarı rakiplere oranla düşüktür. İlk sürümlerde çoklu dokunuş desteği bulunmamaktaydı. 7. sürümüyle beraber çoklu dokunuşu da desteklemeye başlamıştır. Multitasking özelliğini desteklemektedir. C++ tabanlıdır. Microsoft Office programlarıyla mükemmel uyumu Windows Mobile'in önemli bir artısıdır.

3. Mobil Cihazlara Yapılan Saldırılar

Mobil cihazların kullanımın artması ile mobil cihazlara yapılan saldırılarda artmıştır. Bilgisayarlara yapılan saldırıların aynısı mobil cihazlara da yapılmaktadır.
Mobil cihazlarda gerçekleşen başlıca saldırı tipleri; Kötücül Yazılım (Malware), Doğrudan Saldırı (Direct Attacks),Araya Girme (Data Interception), Açıklık Kullanma ve Sosyal Mühendislik (Exploitation ve Social Engineering) olarak sıralanmaktadır. Bu atakların çoğunda daha önceden tespit edilmiş açıklıklar (vulnerabilities) ve bu açıklıkları kullanan kod parçaları (exploit) kullanılmaktadır[3,4].

Kötücül Yazılım (Malware)

Kötücül Yazılım (Malware); virüs, worm (solucan), trojan ve spyware (casus yazılım) olarak bilinen zararlı yazılımların tümüne verilen isimdir. Bu zararlı yazılımların etkili olmasının nedeni mobil cihazlar hızla yayılırken bu cihazlar için gerekli güvenlik yazılımlarının bu oranda geliştirilmemesi ve yaygın olmamasıdır. Bilgisayarlarda olduğu gibi mobil cihazlarda da bu yazılımlar cihazdan cihaza bulaşabilir ve kendini otomatik kopyalayabiliyorlar.
Bu zararlı yazılımlar internet, cihazın bağlandığı bilgisayar üzerinden, MMS mesajı, depolama birimleri (SD, MMC cards) ve mobil cihazlar arasındaki veri aktarımı (wireless,bluetooth, in-

frared) ile yayılabilmektedir. Kötücül yazılımlar yayılarak bulaştıkları cihazlarda sms atma, veri toplama, çağrı kayıtlarını loglama, klavye girişlerini kaydetme (keylogger), yasadışı yazılım yükleme, cihazdaki sertifikaları ele geçirme, ortam dinleme, GPS konum bilgisini kaydetme gibi faaliyetleri gerçekleştirerek kullanıcıya zarar verirler ve bilgilerini izinsiz ele geçirirler[5].

Doğrudan Saldırı (Direct Attacks)

Doğrudan Saldırı olarak adlandırılan bu yöntemde saldırgan bilinen bir uygulama açıklığını ya da işletim sistemindeki açıklığı kullanarak yetkisiz erişim sağlamayı ve bilgi elde etmeyi hedefler. Doğrudan saldırı yöntemi kötücül yazılım (malware) 'dan farklıdır çünkü bu yöntemde cihaza herhangi bir yazılım yüklenmez. Bu yöntemde bir zayıflık bulunur ve bu zayıflık nedeniyle sistemin normal bir etkileşime beklenenin dışında bir tepki vermesi ile zarara uğratılır.
Bu zafiyetler en fazla doküman okuma uygulamaları ve multimedya uygulamalarında görülmüştür[5,6].

Araya Girme (Data Interception)

Hızla kullanımı artan yöntemlerden birisi de veri iletişiminde araya girme (data interception) yöntemidir. Bu yöntemde ağ üzerindeki paketler toplanarak analiz edilir, protokollerine göre ayrıştırılır ve gerekiyorsa şifreli trafik çözülerek aktarılan veri ele geçirilir[6,7].

Açıklık Kullanma ve Sosyal Mühendislik (Exploitation and Social Engineering)

Mobil cihazlardan bilgi elde edilmesinde
sosyal mühendislik ve cihazlarda yapılan açıklık kullanma (exploitation) yöntemleri de kullanılmaktadır. Örnek olarak bilinmeyen bir numaradan gelen sms ile oltalama (phishing) saldırısına maruz kalabilirsiniz. Bu teknikle saldırgan sizden gizli bilgilerinizi alabilir[6,7,8].

4. Mobil Cihazların Güvenliğini Sağlamak İçin Alınacak Önlemler

Mobil cihazların akıllanması ve internetinde kullanılır hale gelmesi ile mobil cihazların kişilerin bilgisayarlarından bir farkı kalmamıştır. İnsanlar bilgisayarlarında hangi işlemi yapmak istiyorlarsa aynı işlemleri artık mobil cihazlarda da yapabilmektedirler.

Bu nedenle artık mobil cihazlar içinde birçok güvenlik önlemi bulunmaktadır. Kullanıcılar bu önlemleri alırlarsa mobil cihazlarını daha güvenli hale getirebilirler.

Bir cep telefonu seçerken, güvenlik özelliklerini düşünün

Mobil cihazlar artık dosya şifreleme, uzaktan erişim, cihazdaki verileri yedekleme, kimlik doğrulama gibi güvenlik önlemlerini içermektedir. Ayrıca VPN bağlantısı ile mobil cihaza bağlanmak isterseniz mobil cihazın sertifika tabanlı kimlik doğrulamasını desteklenmesi gerekmektedir. Bu nedenle mobil cihazlar satın alınırken bu özellikleri içeren cihazlar tercih edilmeli[10].

Aygıtı yapılandırma daha güvenli olması için

Birçok mobil cihazda yanlış şifre girince birkaç denemeden sonra mobil cihaz kendini kilitlemektedir. Bu özelliğin aktif hale getirmeli. Ayrıca kullanıcı şifresini basit tercih etmemeli. Karmaşık şifre belirlemeli. Artık mobil cihazlar içinde antivirus yazılımları var bu programlar cihazlara yüklenebilir [10,11].

Güvenli bağlantı kullanmak için, web hesapları yapılandırın

Belirli web siteleri için Hesaplar (hesap seçenekleri sayfalarında "HTTPS" veya "SSL" arayın) güvenli, şifreli bağlantıları kullanmak için yapılandırılabilir. Birçok popüler posta ve sosyal ağ siteleri bu seçeneği vardır.

Şüpheli e-posta veya metin mesajları gönderilen bağlantıları takip etmeyin

Tanımadığınız kişilerden gelen e-postaları açmayınız. Eğer e-postayı açmışsanız gönderilen bağlantıyı takip etmeyiniz veya e-postada yer alan eklentiyi açmayınız. Bu bağlantılar zararlı web sitelerine neden olabilir.

Cep telefonu numarası ortak ortamlarda paylaşmayın

Cep telefon numaranızı herkese açık ortamda paylaşmayınız. Saldırganlar saldırıları hedef bu numaraları kullanın, sonra web cep telefonu numaralarını toplamak için yazılım kullanabilirsiniz.

Mobil cihazda bilgileri depolarken dikkatli düşünün

Mobil cihazınızda bilgileri depolarken dikkatli olunması gerekmektedir. Özel olan bilgileri mobil cihazda depolanmayabilir. Depolanırsa da güçlü şifreleme algoritmalarını kullanarak şifre-

lenmelidir. Çünkü saldırganlar cep telefonunuzu ele geçirdiğinde bütün bilgilere rahat bir şekilde ulaşabilir[10,11].

Uygulamaları yüklerken titiz olun

Mobil cihazlara uygulamaları yüklerken titiz davranılmalı. Çünkü mobil cihazlar için geliştirilmiş ve kötücül (malware) kod içeren uygulamalar ücretsiz olarak kullanılabilmektedir. Ayrıca uygulamayı yüklerden uygulamanın ihtiyacı olandan fazla izin istiyorsa izin verilmemeli gerekirse uygulamayı yüklememelidir.

Mobil cihazın fiziksel kontrolünü sağlayın

Mobil cihazın fiziksel güvenliğini sağlayın. Mobil cihazların şifreleri var herkes kullanamıyor fakat çeşitli yollarla şifre ile giriş atlatılabilir ve mobil cihazınız başkasının kontrolüne geçebilir. Mobil cihazınıza giriş yaptıktan sonra casus uygulamalar yükleyip sizin mobil cihaz ile yaptığınız her şeyi takip edebilir. Mobil cihazınızı çalınabilir ve mobil cihazınıza kayıt ettiğiniz bilgiler ele geçirilebilir.

Bluetooth, kızılötesi veya Wi-Fi gibi iletişim araçlarını kullanmadığınız zaman devre dışı bırakın

Saldırganlar bu arabirimler kullanarak yazılım açıklarını istismar ederek mobil cihazınızı ele geçirebilir. Bluetooth açık bile olsa görünür olmayabilir[11,12].

Bilinmeyen Wi-Fi ağlarını ve ortak Wi-Fi etkin noktaları kullanmaktan kaçının

Saldırganlar mobil cihazlara bu ağlar üzerinden bağlanılırsa cihaza saldırı yapmaları daha kolay hale gelmektedir.

Atılmadan önce mobil cihazda depolanan tüm bilgileri güvenli silme yöntemi ile silin

Güvenli veri silme hakkında bilgi için cihazın üreticisinin web sitesini kontrol edin. Cep telefonu sağlayıcınız da güvenli Cihazınızı silme hakkında yararlı bilgiler olabilir.

Sosyal ağ uygulamalarını kullanırken dikkatli olun

Bu uygulamalar istenenden daha fazla kişisel bilgileri açığa ve istenmeyen taraflara olabilir. Konumunuzu izlemek hizmetlerini kullanırken özellikle dikkatli olun.

5.Sonuç

Mobil cihazların kullanılmasının artması ile mobil cihazlara geliştirilen uygulamalar ve uygulamalara ve mobil cihazlara saldırılır da artmaktadır. Bu mobil cihazların güvenliğini sağlamak önemli bir hale gelmektedir. Özellikle mobil cihazlar kullanıcıların kişisel eşyası gibi kullanıldığından dolayı daha çok kişisel bilgi ve hassas veriler içermektedir. Değerli bilgiler içermesinden dolayı da son zamanlarda birçok saldırıya maruz kalmaktadır.

Bu nedenle öncellikle mobil cihazların son kullanıcıları dikkatli olmaları gerekmektedir. Bu konuda kullanıcılarda farkındalık oluşturulmalı ve gerekli güvenlik önemleri alınmalıdır. Ayrıca mobil cihazlara uygulama geliştiren yazılımcılarında bilgi güvenliği açısından güvenli uygulama geliştirmek için gerekli çalışmaları yapmalıdır.

Bu çalışmada mobil cihazların bilgi güvenliği açısından var ola risklerden bahsedilmiştir. Ayrıca mobil uygulamalara yapılana saldırı türleri anlatılmıştır. Bu saldıklara karşı nasıl önlem alınması gerektiğinden bahsedilmiştir.

Kaynaklar

[1] Internet: http://www.mobiletisim.com/dosyalar/cep-telefonunun-tarihcesi

[2] Internet: http://web.firat.edu.tr/mbaykara/mobil.pdf

[3] Internet: http://www.veracode.com/products/mobile-application-security

[4] Internet: http://www.informationweek.com/mobile/mobile-applications/mobile-app-development-5-worst-security-dangers/d/d-id/1204488

[6] ESET Latin America's Research Team, Trends for 2014: The Challenge of Internet Privacy, 2014

[7] Souppaya M., Scarfone K., Recommendations of the National Institute of Standards and Technology, NIST, 2012

[8] Mobile Device Security, Understanding Vulnerabilities and Managing Risks, Insights on Governance, Risk and Compliance, January 2012

[10] Ruggiero P., Foote J., Cyber Threats to Mobile Phones, 2011 Carnegie Mellon University. Produced for US-CERT, a government organization, 2011