Gazi Üniv. Müh. Mim. Fak. Der.
Cilt 24, No 3, 499-507, 2009

J. Fac. Eng. Arch. Gazi Univ.
Vol 24, No 3, 499-507, 2009

MOBİL ORTAMLARDA BİLGİ VE HABERLEŞME GÜVENLİĞİ ÜZERİNE BİR İNCELEME

Şeref SAĞIROĞLU ve Hülya BULUT
Bilgisayar Mühendisliği Bölümü, Mühendislik-Mimarlık Fakültesi, Gazi Üniversitesi, Maltepe 06570, Ankara
ss@gazi.edu.tr, hulya.bulut@gazi.edu.tr

(Geliş/Received: 20.10.2008 ; Kabul/Accepted: 28.07.2009)

ÖZET

Bilgisayar teknolojileri gelişip yaygınlaştıkça, günlük iş ve işlemler elektronik ortamlara taşınmakta ve kolaylaşmaktadır. Son yıllarda, artık bilgisayarlarla aynı fonksiyonelliğe sahip olan mobil cihazlar, bilgisayarlar gibi pek çok işlemi yürütmekte ve aynı hassasiyete sahip bilgileri taşımaktadır. Genişletilmiş çevre ortamı, bilgileri taşıma, gönderip-alma ve depolama kolaylığı gibi özellikler mobil cihazların hem kişisel, hem de kurumsal kullanımını yaygınlaştırmıştır. Karşılaşılan tehditler gerek sayı gerekse çeşitlilik açısından arttığı için mobil elektronik ortamlarda taşınan bilgilerin güvenliğinin sağlanması ön plana çıkmıştır. Mobil Cihazın işletim sistemindeki güvenlik açıklarını kullanarak cihaza kurulmuş çeşitli uygulamaların içerisinde kötücül yazılımlar yüklenerek ya da mobiliteyi sağlayan ortam ve diğer sistemlerin zayıflıklardan faydalanan saldırganlar, kullanıcıların bilgi ve haberleşme güvenliğini tehdit etmektedir. Bu çalışmada, mobil ortamları tehdit eden mobil kötücül yazılımlar, mobil cihazlara saldırı yöntemleri, veri iletişimini dinleme gibi mobil ortamlardaki güvenlik tehditleri incelenmiş ve alınabilecek önlemler sunulmuştur.

Anahtar Kelimeler: Mobil cihaz, güvenlik, açıklıklar, saldırılar, korunma yöntemleri.

AN ANALYSIS OF INFORMATION AND TELECOMMUNICATION SECURITY IN MOBILE ENVIRONMENTS

ABSTRACT

Widespreading of computer technology has helped so much to improve our life and daily works or processes in electronic environments. In recent years, mobile devices provide communications as well as supporting many functionalities as computers do. Personal and institutional usage of mobile devices has become widespread because of their services such as extended environment, information carriage and ease of storage and sending-receiving information. As a result of this, the information carried out in the electronic environments becomes important and needs to be secured from the threats increased both as count and as diversity. Attackers threat information and communication security of mobile devices by using the vulnerabilities generally occur due to operating systems, the applications installed in device, malware or fail of wireless technology providing mobility and security. In this study, the security threats to mobile devices like malware which threats mobile environments, methods of attacking the mobile devices, data communication interception have been reviewed and precautions were presented.

Keywords: Mobile device, security, vulnerability, attacks, protection.

1. GİRİŞ (INTRODUCTION)

Elektronik ortamların hızla yaygınlaşmaya başladığı günümüzde, dünya internet kullanımı %21.9 [1] iken dünya cep telefonu abonesi 2008 yılı itibariyle %50 artış göstererek 3,3 milyarı geçmiştir [2]. Research and Markets adlı araştırma şirketinin raporuna göre [2], Türkiye'de bu yıl sonunda 70 milyon 800 bin olması beklenen mobil telefon kullanıcı sayısı 2010 yılında 81 milyon 700 bine ulaşacaktır. Bu süreç içerisinde, Bulgaristan, Danimarka, Finlandiya, Fransa, İrlanda, Hollanda, Polonya, Türkiye, İngiltere, Çek Cumhuriyeti, Almanya, Macaristan, İtalya, Rusya, İspanya ve Ukrayna'yı kapsayan araştırmanın

sonuçları Türkiye'nin Polonya'yla beraber Avrupa'da cep telefonu abone sayısında en yüksek artış oranına sahip ülke olduğu tespit edilmiştir. Bilgi Teknolojileri ve İletişim Kurumunun yaptığı bir araştırmanın sonucu olarak ülkemizde mobil telefon kullanımının sabit hat kullanımından daha yaygın olduğu belirtilmiştir [3]. Bu Kurumumuzun yayınladığı son verilerine göre bugün için cep telefonu penetrasyonunun 70 milyona yaklaştığı belirtilmektedir.

Elektronik ortamlarda yapılan işlemlerin tamamına yakını, cep telefonları kullanılarak ta yapılabilmektedir. Günümüzde artık mobil telefonlarla internette sörf yapabilmekte, eposta alıp-gönderebilmekte, chat yapılabilmekte, MSN kullanılabilmekte ve çeşitli programlar, şarkılar, videolar indirilip çalıştırılabilmektedir. Ayrıca mobil telefonlar bilgisayarda saklanan bilgilere göre daha fazla, kişisel ve önem derecesi yüksek bilgi içermektedir. Masaüstü bilgisayarlarla karşılaştırıldığında, mobil telefonların çalışmaz duruma gelmesi kullanıcılara daha fazla zarara yol açmaktadır [4]. Buna ek olarak, kişisel bilgisayar kullanıcılarının, kötücül yazılımlardan (örneğin, çok miktarda istenmeyen posta göndererek ağ trafiğini tıkayan trojanlardan büyük rahatsızlık duymalarına rağmen), bu durumun finansal bir kayıpla doğrudan ilişkisi yoktur. Diğer taraftan, cihazında benzer bir trojan barındıran mobil kullanıcı, kendisini ay sonunda kabarık bir faturayla başbaşa bulabilir [5].

Mobil ve kablosuz iletişimdeki bu olağandışı hızlı gelişme beraberinde ciddi güvenlik problemlerini de getirmiştir. Bunlar aşağıda başlıklar halinde özetlenmiştir.

- Mobil ve kablosuz iletişimin fiziksel zayıflığı ve sınırlamalarının sadece performans üzerinde değil güvenlik üzerinde de etkili olması [6]
- Kullanılan cihazların kötü niyetli saldırılara ya da şüpheli sayılabilecek kazalara sıkça uğramaları [6]
- Mobil ve kablosuz ortamlardaki güvenlik bilincinin yetersizliği.
- Yüksek hata oranı, dışsal çakışmadan kaynaklanan beklenmeyen hataların fazlalığı [6]
- Geliştirilen cihazlarda güvenlik seviyeleri her geçen gün artmakta olsa da kullanıcıların mevcut teknik ekipmanlarını kısa sürede güncellememesi.
- Günümüz teknolojilerinin donanımdan yazılıma kayması.
- Geliştirilen yazılımlarda güvenli kodlama, güvenlik testleri gibi koruma adımlarının kullanılmaması.
- Mevcut cihazlara kapasite sınırlamasından dolayı anti-casus ve anti-virüs yazılımları gibi güvenlik yazılımlarının kolayca kurulmaması ve/veya güncellenememesi.
- Bazı servislerin kullanıcılara kolayca bağlantı kurup iş yapabilmenin yanı sıra yer bilgisi bulma, içeriğe erişme gibi tehditleri de beraberinde getirmeleri
- Sunulan hizmetlerin sağladığı içeriklerin cihazlara yüklenirken ve çoğunlukla kullanıcının dikkatini çekmeden kötücül yazılımları da cihazlara bulaştırabilmeleri.
- Çok az kayda değer yazılım platformu olması ve bunlar hakkında kısa sürede çok daha fazla bilgi edinilebilmesi [4].
- Kullanılan platformların genel kullanıma açık ve iyi belgelendirilmiş geliştirme araçlarının varlığı, saldırı becerisinin kazanılma sürecini hızlandırması ve kolaylaştırması [4].
- Mobil cihaz açıklarının ve bunlardan nasıl faydalanılabileceğinin Internetten kolaylıkla öğrenilmesi ve açıklardan faydalanmak için gerekli yazılımlara kolaylıkla erişilmesi ve indirilmesiyle oluşabilecek tehditler.

Yukarıda sayılan maddelerden de açıkça görülebileceği gibi mobil ve kablosuz teknolojiler kullanıcılara çok farklı hizmeti kolaylıkla sunarken, pek çok tehlikeyi de beraberinde getirmektedir. Bu da mobil ortam güvenliğini sağlamak için yüksek seviyede bir güvenlik altyapısı geliştirmeyi, çeşitli güvenlik politika ve stratejileri belirlemeyi ve uygulamayı zorunlu kılmaktadır.

Bu makalenin 2. bölümünde mobil tehditler gözden geçirilmiş, karşılaşılabilecek tehdit ve tehlikeler özet olarak verilmiş, özellikle casus yazılımlar, doğrudan saldırılar ile veri iletişimini dinleme detaylı olarak sunulmuştur. 3. Bölümde ise mobil ortamlardaki tehdit ve tehlikeler kısaca gözden geçirilerek alınması gerekli önlemler ile önerilerimiz sunulmuştur.

2. MOBİL TEHDİTLER (MOBILE THREATS)

Bilgisayar teknolojileri gelişip yaygınlaştıkça, günlük iş ve işlemler elektronik ortamlara taşınmakta ve kolaylaşmaktadır. Bunun sonucu olarak elektronik ortamlarda taşınan bilgilerin güvenliğinin önemi ve karşılaşılan tehditler, gerek sayı gerekse çeşitlilik açısından artmaktadır. Kötücül (malware) ve casus (spyware) yazılımlar ise bunların en başında gelmektedir. En önemli tehditlerden olan kötücül ve casus yazılımlar üzerine ülkemizde yapılan bir kitap çalışmasında; bu yazılımlar sınıflandırılmış; sahip oldukları temel özellikler ve taşıdıkları riskler detaylı olarak sunulmuştur [7]. Canbek ve Sagiroglu [7] tarafından hazırlanan bu kitabın, kötü niyetli olarak geliştirilen yazılım türlerinin daha iyi bilinmesi, tanınması ve gerekli önlemlerin alınmasına büyük katkılar sağlayacağı değerlendirilmektedir.

Kötücül yazılım (malware, İngilizce "malicious software"in kısaltılmışı), bulaştığı bir sistemde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış yazılımların genel adıdır [8]. Bu kötücül yazılımlar;

virüsler, solucanlar (worm), Truva atları (Trojan horse), arka kapılar (backdoor), mesaj sağanakları (spam), kök kullanıcı takımları (rootkit), telefon çeviriciler (dialer), korunmasızlık sömürücüleri (exploit), klavye dinleme sistemleri (keylogger), tarayıcı soyma (browser hijacking) ve casus yazılımlar (spyware) en genel kötücül yazılımlardır. Kirli yazılım (scumware) olarak da ifade edilen kötücül yazılımlar, hemen hemen her programlama veya betik (script) dili ile yazılabilmekte ya da birçok dosya içinde taşınabilmektedirler [9].

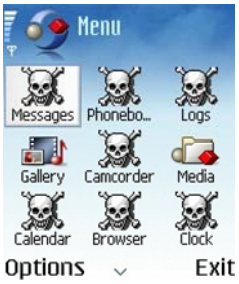
Sıradan kullanıcıları ve sistemleri tehdit eden kötücül yazılımlar, özellikle İnternet ve ağ sistemlerinin getirdiği hareket kolaylılığı ile hızla yaygınlaşmaktadırlar [7]. Bu durum, iyi ve kötü adamların karşı karşıya geldiği teknolojik bir savaşa benzetilebilir. İnsanlar bu mücadele sırasında "kötücül yapıları" bulup temizlerken; verilerini, üretken olabilecekleri zamanlarını ve paralarını kayıp etmektedirler. Kötücül yazılımlardan korunma konusunda; araştırmacıların ve profesyonel güvenlik uzmanlarının bu tür zararlı öğeleri saptayıp, yeni yok etme yollarını geliştirmelerine; kullanıcıların eğitilip, bilinçlendirmesine; saptanan güvenlik boşluklarının kapatılmasına ve koruyucu, tarayıcı ve önleyici yazılımların kullanılması ve güncellenmesine rağmen, kötü niyetli kişilerin saldırıları ve saldırı yöntemleri her geçen gün daha da artmaktadır [9].

Günümüzde pek çok insanın hala kötücül yazılımların neler yapabildiğinin farkında olmaması ve mobil kullanım ortamlarının hızla yaygınlaşmasından dolayı bu ortamlarda da büyük tehdit oluşturmaktadır [10]. Mobil ortamlarda oluşan tehditler aşağıda verilen alt başlıklarda açıklanmıştır.

2.1. Mobil Kötücül Yazılım (Mobile Malware)

İlk mobil kötücül yazılım olan Cabir, Haziran 2004 açığa çıkmış ve o zamanlar en yaygın kullanılan işletim sistemi olan Symbian Series 60 işletim sisteminin kurulu olduğu cihazlarda görülmüş ve kendi kopyalarını Bluetooth yoluyla dağıtmayı başarmıştır [11]. Cabir, virüs yazmayı kendilerine amaç edinmiş olan 29A adlı uluslararası bir grubun üyesi olan Vallez tarafından geliştirilmiştir. Kopyalarını oluşturup Bluetooth üzerinden dağıtmanın yanı sıra kullanıcıya, cihazın pilini bitirme ve işlemciyi Bluetooth dağıtımı yapacak cihazlar arayarak meşgul etme gibi zararlar vermiştir. Bir süre sonra Cabir'in kodları yayınlanmıştır. Bu durumdan istifade eden virüs yazarları Cabir'in türevlerini üretmekte gecikmemişlerdir. Bundan sonra mobil kötücül yazılım çeşidi hızla artmış ve bilgisayar virüslerinde olduğu gibi hem çok hızlı yayılmış hem de teknik sorunların yanı sıra maddi kayıplara da yol açan zararlar vermiştir.

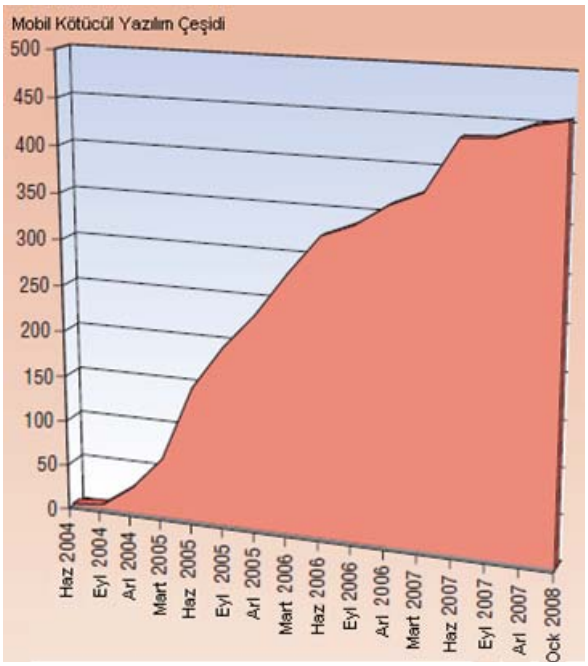
Virüsü bir cihazdan diğerine bulaştırmada Bluetooth'tan faydalanmaya alternatif bir diğer yöntem ise MMS kullanmaktır. Commwarrior, MMS yoluyla yayılan ilk virüs olma özelliğini taşımaktadır [11]. Aynı zamanda Bluetooth'la da yayılabilen bu virüs, Cabir gibi Symbian işletim sistemi kurulu cihazlarda etkili olmaktadır. Yayılım için hem MMS hem de bluetooth teknolojisini kullanmasına rağmen Commwarrior'un yayılımı çok hızlı değildir. Cardtrap ise telefonun hafıza kartına Windows işletim sistemi virüsü bulaştıran ve aynı zamanda kez olarak Windows kurulu bilgisayarlarda da etkin olmayı başaran ilk virüstür [11]. En çok türevi üretilen virüslerden biri de mobil cihaza bulaştığında verdiği zararların düzeltilmesi çok zor olan Skulls virüsüdür [11]. Skulls, bulaştığı cihazlarda ikonları kafatası ve çarpı şeklinde kemik resimleriyle değiştiren, uygulama dosyalarını silen ve değiştiren bir Symbian Trojandır. Şekil 1'de Skulls bulaşmış bir mobil cihaz ekranı verilmiştir.



Şekil 1. Skulls virüsü bulaşmış bir telefon ekranı [11]
(An infected phone's screen by Skulls virus)

Şekil 2'de 2008 yılı başında mobil kötücül yazılım çeşitlerinin 450'yi aştığı görülmektedir [13]. Mcafee'nin yayınladığı sonuçlarda ise 2008 Mart ayı itibariyle mobil kötücül yazılım sayısı 450'yi aşmıştır [12].

Cabir'in yazılmasından bu zamana kadar, mobil



Şekil 2. Mobil kötücül yazılım artış oranları [36]
(Mobile malware increase rates)

kötücül yazılımlar incelendiğinde kötücül yazılımların geliştirilmesi ve yayılımı üzerinde, mobil cihazlarda popüler olarak kullanılan işletim sisteminin mobil tehditlerin geliştirilmesi ve yayılımını doğrudan etkilediği açıkça görülmektedir. Bugün birçok mobil telefonda işletim sistemi Symbian OS'tur ve bu yüzden özellikle Symbian OS tabanlı mobil telefonları etkileyebilecek kötücül yazılım çeşidi ve sayısı çok daha fazladır. Tablo 1'deki kötücül yazılım tehditleri ve etkilerini gösteren sayısal bilgilerde de bu durum açıkça görülmektedir. 11 Haziran 7 Temmuz 2006 yılları arasında virüslü MMS sayısı 5184'den 4 hafta içerisinde yaklaşık %8 artarak 5541'e yükselmiştir.

Tablo 1. Mobil tehditler ve zararları [14]

Kötücül yazılımın adı	**Virüslü MMS sayısı**
Worm.SymbOS.ComWar.a	4733
Worm.SymbOS.ComWar.c	450
Trojan-SMS.J2ME.RedBrowser.b	1
11 - 17 Haziran 2006 Verisi	

Kötücül yazılımın adı	**Virüslü MMS sayısı/Önceki peryotla farkı**
Worm.SymbOS.ComWar.a	5498 (+765)
Worm.SymbOS.ComWar.c	854 (+404)
Trojan-SMS.J2ME.RedBrowser.b	1
18 - 24 Haziran 2006 Verisi	

Kötücül yazılımın adı	**Virüslü MMS sayısı/Önceki peryotla farkı**
Worm.SymbOS.ComWar.a	4564 (-934)
Worm.SymbOS.ComWar.c	756 (-98)
25 Haziran - 1 Temmuz 2006 Verisi	

Kötücül yazılımın adı	**Virüslü MMS sayısı/Önceki peryotla farkı**
Worm.SymbOS.ComWar.a	4837 (+273)
Worm.SymbOS.ComWar.c	698 (-58)
Worm.SymbOS.ComWar.d	6 (+6)
1 Temmuz – 7 Temmuz 2006 Verisi	

Son yayınlanan sonuçlar mobil tehdit sayısında son üç yıl ile karşılaştırıldığında en büyük artışın 2008 yılında gerçekleştiğini göstermiştir [38].

2.2. Doğrudan Saldırılar (Direct Attack)

Bu saldırılar en tehlikeli saldırılardan olup, mobil cihazlar herhangi bir kişisel bilgisayara, mobil cihaza veya bilgisayar ağına bağlıyken, internet hizmetinden faydalanırken ya da sadece açık durumdayken ve hatta kapalı durumdayken bile bu tür saldırılara maruz kalabilmektedir. Doğrudan saldırının yapılabilmesi için önce hedef cihazın bulunması gerekir ki bunun birden fazla yolu olduğu literatürde verilmiştir. Bunlar aşağıda kısaca özetlenmiştir [10], [15];

1. Basit bir şekilde, cihazın varlığının görülmesi (konuşulan veya sahip olunan telefonun elde fiziksel olarak görülmesi), kötü niyetli kişilerin iştahını kabartmaktadır.
2. Bir ağa, mobil cihazla doğrudan bağlanan cihazı tespit etme (Bazı durumlarda mobil cihaz genel kullanıma açılmış bir wi-fi hotspot üzerinden internete bağlanırken normalden daha fazla korumasız olur.) ile saldırganların, ağ üzerinde tarama yaparak mobil cihazın IP'sini kolayca elde edebilmeleri,
3. Bir saldırgan Internet üzerinde IP taraması yapabilir. Bu tarama sonucu IP'ler arasından mobil cihazlara ait olanlarının listesini elde edebilir. Sonuç olarak, dünyanın herhangi bir yerinde, herhangi bir şekilde internete bağlanmış olan mobil cihaz saldırılara açıktır.
4. Mobil telefonlara hizmet aksatma saldırısı (DoS – Denial of Service) yapmak mümkündür. Bu tür bir saldırıda, aşırı yükleme yaparak cihazı kullanılamaz hale getirilebilir.
5. Diğer bir hizmet aksatma saldırısı ise cihazın çeşitli yollarla fazla güç harcamasına neden olarak cihazın şarjını bitirmektir.

Mobil telefonlar, üzerinde değişiklik yapılarak gizli bir şekilde ortam dinleme için uzak mikrofonlar haline getirilebilir [16]. Bu gizli dinleme işi için ağda herhangi bir değişikliğe ihtiyaç yoktur, sadece mobil telefonda değişiklik gerekmektedir. Bu tür saldırılarda hedef belirli bir cihazdır ve tektir. Saldırının yapılabilmesi için önceden herhangi bir yolla, kullanıcısının haberi olmadan mobil telefonda değişiklik yapılması gereklidir. Bununla birlikte önceden değişiklik yapılarak ortam dinleme amaçlı hale getirilmiş mobil telefonlar hedef kişiye hediye edilerek te şüphe çekmeden dinleme yapıldığı bilinmektedir. Casus telefon olarak da bilinen bu cihazların internet üzerinden satışı yapılmakta ve alıcılarına ortam dinlemenin yanında hedef cihazın gelen ve giden aramalarını dinleme, arama listesine ulaşma, gelen ve giden mesajlara ulaşma, SIM kart değişikliğini haber verme gibi imkanlar da sağlamaktadır [17], [18].

Diğer bir saldırı türü olan SMS hizmet aksattırma (DoS) saldırısını gerçekleştirmek için belirli mobil telefon numaralarını elde etmenin farklı yolları aşağıda özetlenmiştir [19]:

- Hizmet sağlayıcıların çoğu, belirli numara serilerini belli yerlere vermektedir. Belli bir yerde belli bir zaman aralığında satılan tüm SIM kartları aynı seri içinde olabilir. Küçük bir araştırma ile bir bölgedeki olası telefon numaraları belirlenebilir.

- Müşteri numaralarının tutulduğu ortak veritabanlarına erişmek bir başka yoldur. Artık, bankaların çoğu SMS uyarı hizmeti vermektedir ve buradaki veritabanları araştırmaya başlamak için iyi bir başlangıç olabilir. Tanıdıklar bu tür işlemleri yapmayı kolaylaştırarak, mobil numaraları elde etmeyi kolaylaştırabilir.
- Sosyal ağlar diğer bir güncel yaklaşım olup biraz programlama becerisi gerektirir. Birçok insan, profillerinde mobil numarasına da yer vermektedir. Küçük bir araç, belli bir topluluk ya da belli bir arkadaş listesindeki tüm mobil numaraları ortaya çıkarabilir.
- Bir mobil solucan ya da virüs kullanma diğer bir yaklaşımdır. Bunlar mobil telefondan bağlantı listesini okuyabilir ve kullanıcıların haberi olmadan tüm bilgileri merkezi bir sunucuya gönderebilir. Bazı bluetooth solucanları bunu yapabilmektedir.

Yeterince numara elde ettikten sonra, gerçek numaraları tespit etmek için listenin filtre edilmesi gerekir. Sahte bir gönderici ID'si ile tüm numaralara bir metin mesajı gönderip teslim raporlarını bekleyerek bu iş gerçekleştirilebilir. Bundan sonra mesajın ulaştığı tüm numaralara eş zamanlı olarak SMS gönderilebilir. Bunun için bir SMPP (Short Message Peer-to-Peer Protocol) ağ geçidi gereklidir [20]. Günümüzde pekçok firmanın bu tür hizmetleri verdiğini belirtmekte fayda görüyoruz. Bu durum ise çoğu zaman, gönderilen mesaj sağanağı (SPAM) ve SMS sayısının artmasına ve SMS DoS saldırılarının yapılmasına olanak tanımaktadır. Son yıllarda ticari ya da reklam amaçlı olarak, mobil kullanıcılara gönderilen istenmeyen mesaj sağanağı sayısında büyük artış olmuştur. Amerika'da mobil telefon kullanıcıları 2007 yılında 1.1 milyon mesaj sağanağı alırken, bu rakamın 2008 yılında 1.5 milyona ulaşacağı tahmin edilmektedir [21].

Mobil cihazın gücü pili ile sınırlıdır. Bu yüzden mobil cihazlar donanımı ve yazılımıyla birlikte pil ömrünün uzun olması için enerji tüketimi en az olacak şekilde tasarlanırlar. Güç yönetim sistemleri aktif, boşta ve uykuda olmak üzere değişik durumlara sahiptir. Aktif durumda cihaz, diğer iki durumun aksine, çeşitli işlemleri yürütmekle meşguldür ve bu yüzden daha fazla enerji harcar. Eğer bir saldırgan cihazı sürekli aktif durumda tutabilirse, pil ömrü beklenenden daha kısa olur [15]. Örneğin [22] nolu kaynakta MMS hizmetinin güvenlik açığından yararlanarak, mobil cihazın pilini normalden 2 kat daha hızlı bitiren ve dolayısıyla iş saati bitiminden önce, mobil cihazı kullanılamaz hale getiren bir saldırıya örnek verilmiştir. Mobil cihazın pilini bitirmek için birden fazla yol vardır ve bunlar genel olarak üç ana metot altında toplanırlar [23]:

1. Ağ hizmeti istek saldırıları (network service request attacks), saldırgan hedef cihazın sürekli bir ağ servisi isteği yapmasını sağlar. Eğer servis sağlanmıyorsa, mobil cihaz bunu değerlendirmek için enerji harcar.
2. İyi niyetli güç saldırılarında (benign power attacks), saldırgan, geçerli fakat büyük miktarda enerji harcanmasına sebep olan bir programın çalışmasını sağlar. Bu tür saldırılardan korunulması ve bunları virüs tarayıcılarının fark etmesi zordur çünkü herhangi bir şekilde değiştirilmemiş dolayısıyla kötücül yazılım şüphesi taşımayan geçerli kod üzerinde çalışırlar [24]. Örneğin, saldırgan aynı görüntüyü tekrar tekrar gösteren bir hareketli gif resmi oluşturarak böyle bir saldırı gerçekleştirebilir. Resim kullanıcıya hareketsiz görünür fakat aslında hareketli olan bu görüntü cihazı meşgul eder ve fazla enerji harcanmasına yol açar [15].
3. Kötücül güç saldırıları (malignant power attacks), saldırgan fazla enerji harcaması için çalıştırılabilir bir dosya oluşturur veya var olan çalıştırılabilir dosyayı bu amaçla değiştirir. Bu tür saldırılar virüs tarayıcıları tarafından tespit edilebilir çünkü değiştirilmiş ve geçerli olmayan programlardır [15].

Saldırı yapacak cihazı bulmanın bir diğer yolu ise bir cihaz tarafından alınan ve gönderilen sinyalin varlığını tespit etmektir. Bluetooth bunun en güzel örneklerinden biridir. Bir bluetooth-sniffing aracı ile bu sinyal tespit edilebilir. Bu tespit işi bir defa gerçekleştiğinde, bundan sonra, Bluetooth üzerinden gerçekleştirilebilecek tüm saldırı türleri uygulanabilir [10]. Aşağıda bluetooth teknolojisinden faydalanılarak gerçekleştirilen genel saldırı çeşitleri açıklanmıştır.

- **BlueJacking:** Bir kullanıcının kapsama alanı içerisinde başka bir kullanıcıya isimsiz olarak bir bluetooth mesajı göndermesidir. Gönderilen mesajlar resim ya da metin şeklinde olabilir. Amaç, dosyaları kopyalayarak veya değiştirerek, çalıştırılabilir bir dosya yükleyerek cihazı ele geçirmek ya da zarar vermek değildir [25].
- **BlueSnarfing:** Kullanıcının izni veya bilgisi olmadan bluetooth üzerinden telefon rehberi, eposta ve metin mesajları, kullanıcının takvimi gibi bilgilere ulaşmasıdır. Saldırganlar kablosuz cihazlar arasında bilgi alışverişini sağlamada kullanılan OBEX (object exchange) protokolündeki bir açıktan faydalanmaktadırlar [26].]. Şekil 3'te Bluesnarfer komutları verilmiştir.
- **BlueSpam:** Bluetooth üzerinden sağanağı, Bluetooth'la reklam gönderme işidir. Bluetooth cihazları taranır ve görünen cihazlara basit ASCII metin dosyalarından, jpg, gif vb. uzantılı resim dosyaları şeklinde olabilen VCFs (electronic business cards) ve ses ya da resim dosyaları gönderilebilir. Gönderme işi OOP (Obex Object Push) ve/veya OBEX-FTP (OBEX File Transfer Protocol) kullanılarak yapılır [27].

Şekil 3. Bluesnarfer Komutları [10] (Bluesnarfer commands)

- **BlueBug:** Bazı Bluetooth-etkin cihazlardaki Bluetooth güvenlik açığının adıdır. Kullanıcının bilgisi olmadan cihaz üzerinde çeşitli komutlar çalıştırılabilir [28]. Bu durumda saldırgan; çağrı yapabilir veya mesaj gönderebilir, takvim veya telefon rehberini okuyabilir, not yazabilir, telefon konuşmalarını dinleyebilir, internete bağlanabilir, telefonu belirli bir servis sağlayıcısını kullanmaya zorlayabilir ve daha benzer birçok işlemi gerçekleştirebilir [29].
- **BackDoor:** Arka planda cihazı, bir başka cihazla eşleştirmek. Bu şekilde istenildiği zaman, kullanıcının bilgisi olmadan, cihazla bağlantı kurulabilir [10].

Bir saldırganın cihazı ele geçirmesi demek, cihazla ilgili her türlü bilgiye ulaşması demektir. Bilgi hırsızlığı saldırısı yapılarak cihazın yer bilgisi, kullanım bilgisi, bazı teknik özelliklerinin yanı sıra cihazda saklanan resim veya video gibi çeşitli çoklu ortam dosyaları, notlar, alınan ve gönderilen mesajlar, adres defteri bilgileri gibi özel içeriğe de ulaşılabilir.

Mcafee'nin 2008 mobil güvenlik raporunda [30], kullanıcıların mobil telefonlarda güvenlik riskleri endişeleri sınıflandırılmış ve en çok endişe duyulan güvenlik risklerinden birinin mobil telefon faturalarındaki beklenmeyen artışlar olduğu tespit edilmiştir. Saldırganların, mobil cihazlar üzerinden binlerce SMS ve/veya MMS gönderebildiği ve mobil cihazlar üzerinden pahalı telefon konuşmaları gerçekleştirebildiği belirlenmiştir.

2.3. Veri İletişimini Dinleme (Data-Communication Interception)

Bazı durumlarda bir mobil cihaza saldırmanın en kolay ve en iyi yolu, dolaylı yoldan saldırı yapmaktır. Birçok cihaz artık diğer benzer cihazlarla, kişisel bilgisayarlarla ve ağlarla birçok farklı yoldan bağlantı kurabilmektedir. Kablosuz ve mobil bağlantı kurmada kullanılan en son teknolojilerden birkaçı Wi-Fi, EvDO, 3G, Kızılötesi, Bluetooth vb. teknolojilerdir. Bu teknolojileri kullanan kişilerin ve kurumların bağlantıları güvenli olmadığından, aktarımı yapılan tüm bilgilerin güvenli ve şifrelenmiş bir şekilde iletildiğinden emin olmaları gerekmektedir.

Son yıllarda havaalanları, tren istasyonları, kafeler, hareket halinde olan trenler ve uçaklar gibi yerlerde genel kullanıma sunulmuş Wi-Fi Hotspot hizmeti ile kişiler dizüstü bilgisayarları ya da mobil cihazları ile internete ulaşabilmektedir. Bu teknoloji ile veriler radyo dalgaları üzerinden gönderilmektedir. 5 yıl önce Dünya'da Wi-Fi Hotspot sayısı 20.000 iken, günümüzde bu sayı 200.000'in üzerindedir ve 2010 yılında 400.000'e ulaşması beklenmektedir [37]. Ağ güvenliğinin parolalarla korunmasına ve ağ iletiminin şifrelenmesine rağmen, çoğu Wi-Fi cihazı henüz bu şekilde bir güvenliğe sahip değildir [31]. Wi-Fi bağlantılarında güvenliği sağlamanın en iyi yolu WPA2 (Wi-Fi Protected Access 2) teknolojisini kullanmaktır [32]. Bu teknoloji ile güvenli bir şekilde ağa bağlanılabilir ve veriler şifrelenmiş olarak iletilir.

Araç kiti ve diğer Bluetooth sistemlerinin güvenlik açısından ne kadar zayıf olduğu geliştirilen 'Carwhisperer' projesinde gösterilmiştir [33]. Bu sistemlerin büyük bir kısmında sisteme erişim için dört haneli ve genellikle üreticiler tarafından sistemlerin tümü için tek bir kod belirlediği basit bir şifre kullanılmaktadır. Bu durumda dört haneli, bulunması pekte zor olmayan şifre kullanılarak sisteme kolaylıkla girilebilir ve uygun donanımla hareketli araç içerisinden kişilerin konuşmaları da dahil her türlü ses verisi alınabilir.

3. SONUÇLAR ve ÖNERİLER (CONCLUSIONS and SUGGESTIONS)

Mobil teknolojilerin gelişim hızı ile beraber cep telefonu kullanımının yüksek seviyelere ulaştığı günümüzde, e-devlet uygulamaları ve diğer kurumsal uygulamalar mobil cihazlar üzerinden verilmeye başlanmış, mobil ortamlardan faydalanma oranı gerek bireysel gerekse kurumsal açıdan bakıldığında hızla artmaktadır. Kullanılan uygulamalar zamanla daha çok fonksiyonellik içermekte, kullanıcılara çok daha çeşitli ve kaliteli hizmet vermekte, bununla beraber, teknik açıdan bakıldığında uygulama boyutu büyümekte ve karmaşıklık artmaktadır. Bu ise pek çok güvenlik açığı ve uygulama hatasını beraberinde getirmektedir. Bu yıl yayınlanan mobil güvenlik raporuna göre, son yıllarda mobil cihaz üreticileri hiç olmadığı kadar fazla mobil kötücül yazılım saldırılarıyla karşılaşmakta ve bunları atlatmak için daha fazla zaman ve para harcamaktadır [38]. Ayrıca kurumların artık önemli ve hassas nitelikteki bilgi varlıklarını mobil ortamlarda taşıdığı göz önüne alındığında, bu alandaki

tehdit ve saldırıların önemsenecek derecede arttığı, geliştirilen kötücül ve casus yazılım çeşitlerinin ve zarar derecesinin de fazlalaştığı belirlenmiştir. Tüm bu gelişmeler ışığında, kurumların ve bireylerin mobil cihazlar ve ortamlarda meydana gelebilecek tehditlerin farkında olarak gerekli koruma tedbirlerini almaları, personel ve kullanıcılarını bu konuda eğitmeleri ve bilinçlendirmeleri gerektiği bir gerçektir.

Mobil ortamlarda yüksek seviyede bir bilgi güvenliği sağlamak için önerilerimiz aşağıda sıralanmıştır:

1. Mobil cihazlarda anti-viral (anticasus, antivirüs, antispam) yazılımlar kullanılmalı ve işletim sistemi dahil olmak üzere sürekli güncel tutulmalıdır [10].
2. Telefon üreticileri, bilgisayar üreticilerinin birçoğunun şu an yaptığı gibi, müşteriye cihazları antivirüs yazılımı kurulmuş olarak teslim etmelidir [34].
3. Telefon operatörleri, mobil kötücül yazılımlar salgın hale gelmeden, müşterilerini mobil virüslerin nasıl belirlenmesi gerektiği ve bunlardan korunulması gerektiği konusunda eğitmelidirler [34].
4. Ağ ve İnternet bağlantısı kullanan mobil cihazlarda güvenlik duvarı kurulmalı ve sürekli açık tutulmalıdır.
5. Cihazların ağ uygulamaları kapalı konuma getirilmeli ya da 'görünme durumu' seçeneği 'gizli' olarak seçilmelidir. Bu özelliklerin kullanılmasını sağlamak için satış personeli kullanıcılara bilgi vermelidir [15].
6. Mobil telefon PIN kodları ve diğer şifreleri '1234' ya da kullanıcının doğum tarihi gibi kolay tahmin edilebilecek kombinasyonlardan kaçınılarak belirlenmelidir.
7. Tüm mobil telefonlar GSM ağında kendini tanıtan 15 haneli bir uluslararası mobil cihaz kimlik numarasına (IMEI – International Mobile Equipment Identification) sahiptir. IMEI numarası, telefon tuşlarına *#06# yazılarak öğrenilebilir. Kullanıcıların çalınma ya da kaybolma riskine karşı cihazlarının IMEI numarasını kaydetmeleri gerekir [35].
8. Son zamanlarda platform güvenliğine karşı yapılan saldırıların arttığı, istenmeyen içerik ya da servisleri silmeyi veya engellemeyi kapsayan dinamik içerik güvenliği gibi tamamlayıcı güvenlik teknolojilerine ihtiyaç duyulduğu görüldüğünden bu konularda güvenlik çözümleri geliştirilmesi gerekmektedir [38].
9. Mobil cihaz içerisinde depolanmış önemli bilgiler şifrelenmiş olarak saklanmalıdır. Mümkün olduğunca da bu ortamlarda tutulmamaya çalışılmalıdır.
10. Mobil cihaza kopyalanan ve indirilen tüm dosyalar virüs taraması yapıldıktan sonra kullanılmalıdır.
11. Mobil cihazda saklanan verilerin düzenli olarak yedeğinin alınması gerekir.
12. Mobil telefonlar, kullanıcılarına görsellik ve pil seviyesi, pil tüketim oranı, veri aktarımı ve işlemci aktiviteleri gibi en kritik istatistiklerinin günlüklerini sunmalıdırlar [15].
13. Servis sağlayıcıları kullanıcının telefonunda kötü niyetli kullanımı tespit etmek için kullanıcının genel kullanım karakteristiğini çıkarmalıdır. Eğer şüpheli bir aktivite tespit ederlerse, servis sağlayıcıları kullanıcının durumdan haberi olup olmadığını anlamaya yönelik bir mesaj göndermelidir [15].
14. Birçok şirket saldırgan bir tutumla, mobil cihazlarının kullanımda olduğu GPRS ya da UTMS veri ağları üzerindeki trafiği filtrelemektedir. Wi-Fi ağlarında bu çeşit bir koruma olmadığı bilinmelidir [34].
15. Tüm mobil cihazlar, erişim için kimlik kanıtlama isteyecek şekilde ayarlanmalıdır [10]. Cihazın yapılandırmasında güvenlik ayarları da göz önünde bulundurulmalıdır.
16. Bazı operatörler kötücül ekleri olan MMS mesajlarını silmek üzere filtreleme yapmaktadır. Tüm operatörlerin bu çeşit bir filtreleme yapması gerekmektedir [34].
17. Fiziksel olarak telefonla güç bağlantısını kaldıran güç anahtarları kullanılarak, telefonun tamamen kapandığından emin olunabilir. Eğer bir telefon hoparlör moduna sahipse, fiziksel güç anahtarı, telefon mikrofonunun kullanıcının bulunduğu ortamdaki sesleri alacak şekilde kötü amaçlı kullanımını engeller [15].
18. Mobil ortamlarda işlenen suçların kapsamı belirlenmeli ve bu konuda yasal düzenleme yapılmalıdır.
19. Kullanıcılar, mobil ortamlardaki güvensizliğin farkında olarak hareket etmeli, önceki maddelerde belirtilen hususları uygulamaya çalışmalı ve mobil ortam güvenliğinden kendilerinin de sorumlu olduklarını hatırlarında tutmalıdırlar.

Daha spesifik olarak değerlendirildiğinde ise; casus ve kötücül yazılımlara karşı koruma işi birçok ayrı kısımdan oluşmaktadır. Antiviral yazılımı kurup kullanmaya ek olarak, cihaz yapılandırması güvenliği sağlayacak şekilde ayarlanmalı, sıfır-gün-korumayı sağlayacak antivirüs programları, anticasus ve benzeri programlarla koruma desteklenmeli ve güçlendirilmelidir.

Veri-iletişiminin dinlenmesini engellemek için alınan ve gönderilen verilerin şifrelenmiş olarak iletilmesi gerekir. Bluetooth ve benzeri teknolojileri kullanırken cihazların normalden çok daha korunmasız olduğunun farkında olunması ve buna göre tedbir alınması gerekir. Kullanılmadığı zamanlarda ağ bağlantı arayüzlerinin iptal edilmesi gerekir. Son olarak, mobil cihaz içerisine farklı yazılımların eklenilmediğinden emin olunması gerekmektedir.

Bugünün mobil güvenlik sistemleri, anti-virüs yazılımı, güvenlik duvarı gibi geleneksel ölçütlere ek olarak bazı mobil kötücül yazılım türlerini engellemek için, gelişmiş uygulama imzalama ve diğer yaklaşımları kullanmaktadır [36]. Uygulamaların telefon rehberi dizinine ve diğer belirli özelliklere erişimini engelleme gibi yaklaşımlar, kullanıcı ve saldırganlar için kötücül yazılım içeren, onaylanmamış uygulamaları kurmayı daha zor hale getirmektedir. Mobil kullanıcılar artık, geleneksel güvenlik ölçütlerini uygulamanın yanı sıra bu tür yeni yöntemleri takip edip, güvenlik bilinç düzeylerini yükseltmeli ve cihazlarını güncellemeleri gerekmektedir.

TEŞEKKÜR (ACKNOWLEGEMENT)

Bu çalışma Gazi Üniversitesi BAP tarafından desteklenen **"Mobil Ortamlarda Kötücül Yazılımlar ve Karşı Tedbirler Üzerine Uygulama Geliştirme"** 06/2008-49 no'lu Gazi Üniversitesi Bilimsel Araştırma Projesi kapsamında yapılmıştır. Yazarlar, Gazi Üniversitesi BAP Başkanlığı'na teşekkür eder.

KAYNAKLAR (REFERENCES)

1. http://www.internetworldstats.com/stats.htm
2. **1Q08 Mobile Forecast: Turkey, 2007–2010**, http://www.researchandmarkets.com/reports/579867/1q08_mobile_forecast_turkey_2007_2010
3. **Sabit ve mobil telefon kullanıcılarının profili ve eğilimlerinin belirlenmesi araştırması,** Telekomünikasyon Kurumu, Son erişim tarihi: Ağustos-2008, http://www.tk.gov.tr/anket/telkullaniciprofil.htm
4. Soitinaho J., "Security Threats of Mobile Service User", **TKK T-110.5290 Seminar on Network Security**, Helsinki University of Technology, 2007.
5. Jamaluddin J., Zotou N., Coulton P., "Mobile phone vulnerabilities: a new generation of malware", **IEEE International Symposium on Consumer Electronics**, 2004, 199-202.
6. Sun J, Howie D, Koivisto A & Sauvola J "A hierarchical framework model of mobile security." **Proc. 12th IEEE International Symposium on Personal, Indoor and Mobile Radio Communication,** San Diego, CA, 2001.
7. Canbek G., Sağıroğlu Ş., "Kötücül yazılımlar, türleri, sınıflandırılması ve güncel yazılımlar", **Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri**, Grafiker Yayıncılık, 213-253, 2006.
8. Calder A., Watkins S., **It Governance: A Manager's Guide to Data Security & BS 7799/ISO 17799**, Kogan Page, pp.14, 163, September 1, 2003.
9. Grimes R. A., **Malicious Mobile Code**, O'Reilly, pp.3, 201-203, 226-228, 238-244, 467-468, August 1, 2001.
10. Hoffman D.V., "Understanding the threats", **Blackjacking**, ch.1, Wiley Publishing Inc., Indianapolis, 3-22, 2007.
11. **"Mobile Malware Evolution: An Overview, Part1"**http://www.viruslist.com/en/analysis?pubid=200119916
12. **"McAfee Delivers on Triple Play Promise With Mobile Security Offering"**, http://newsroom.mcafee.com/article_display.cfm?article_id=2693
13. F-Secure, "Mobile Threat Summary for 2007", **CeBIT 2008**, Hanover, Germany, March 2008.
14. Coursen S., "The future of mobile malware", **Network Security** Volume 2007, Issue 8, August 2007, p. 7-11.
15. Dagon D., Martin T., Starner T., "Mobile phones as computing devices: the viruses are coming!", **IEEE Pervasive Computing**, v.3 n.4, p.11-15, October 2004.
16. Lin Y.B., Tsai M.H., "Eavesdropping Through Mobile Phone", **IEEE Transactions On Vehicular Technology,** vol. 56, no. 6, pp. 3596-3600, November, 2007.
17. http://guvenlikprogram.com/index.php?pg=item&det=382
18. http://www.flexispy.com/spyphone-call-interceptor-gps-tracker-symbian.htm
19. **"Collecting Mobile Numbers for an SMS DOS attack",** http://www.kenneyjacob.com/2007/08/23/collecting-mobile-numbers-for-an-sms-dos-attack/
20. **"SMS DOS attack on cellular networks",**http://www.kenneyjacob.com/2007/08/23/sms-dos-attack-on-cellular-networks/
21. **Mobile spam worries wireless industry analysts,** http://telecomnews2008.wordpress.com/2008/01/22/mobile-spam-worries-wireless-industry-analysts/
22. Racic R., Ma D., Chen H., "Exploiting MMS vulnerabilities to stealthily exhaust mobile phone's battery", **15th Annual USENIX Security Symposium Vancouver**, BC, 2006.
23. Martin T., Hsiao M., Ha D., Krishnaswami J., "Denial-of-service attacks on battery-powered mobile computers", **Proc. 2nd IEEE Int'l Conf. Pervasive Computing and Communications**, IEEE CS Press, 2004.
24. Nash D. C., Martin T. L., Ha D. S., Hsiao M. S., "Towards an Intrusion Detection System for Battery Exhaustion Attacks on Mobile Computing Devices"**, Proc. 2nd Int'l Workshop Pervasive Computing and Comm. Security (PerSec 05)**, pp. 141–145, IEEE CS Press, 2005.
25. **"Bluejacking Code of Ethics"**, http://www.bluejackq.com/code-of-ethics.shtml
26. **"Bluesnarfing"**, http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci952393,00.html

27. **"The Bluetooth Spam FAQ"**, http://www.mulliner.org/bluetooth/bluespamfaq.php
28. **"Hayes command set"** http://en.wikipedia.org/wiki/Hayes_command_set
29. **"Bluebug"**, http://trifinite.org/trifinite_stuff_bluebug.html
30. McAfee, **"McAfee Mobile Security Report 2008:Mobile Users Express Growing Concern Over Security"**, http://www.mcafee.com/us/research/mobile_security_report_2008.html
31. Iredale W., Gadher D., **"Airwave hackers spark computer alert"**, Sunday Times, http://www.timesonline.co.uk/tol/news/uk/article404220.ece
32. **WPA2 (Wi-Fi Protected Access 2)** http://www.wi-fi.org/knowledge_center/wpa2/
33. **"Car Whisperer"** http://trifinite.org/trifinite_stuff_carwhisperer.html
34. Hypponen M, "Malware Goes Mobile", **Scientific American**, 70-77, Nov. 2007.
35. **"Mobile phone security fact sheet"**, http://www.acma.gov.au/WEB/STANDARD/1001/pc=PC_1718
36. Lawton G., "Is It Finally Time to Worry about Mobile Malware?", **Computer -IEEE Computer Society**, vol. 41, no. 5, pp. 12-14, May, 2008.
37. **"How Many Wi-Fi Hotspots Exist Worldwide?"**, http://compnetworking.about.com/b/2008/03/04/how-many-wi-fi-hotspots-exist-worldwide.htm
38. McAfee, **"McAfee Mobile Security Report 2009"**, http://www.mcafee.com/us/local_content/reports/mobile_security_report_2009.pdf