Mobil Platformlarda Gizli Ağ Saldırılarının Önlenmesi ve Mobil Uygulaması

[1]S. Oyucu, [2]H. Polat, [3]İ. A. Doğru

***Özet*—Günümüzde kötü amaçlı yazılımların tespiti siber saldırılarla mücadelede önemli rol oynamaktadır. Kötü amaçlı yazılımların tespit edilmesi ise genel olarak ilk kurulum aşamasında veya uygulama pazarına yüklenirken yapılmaktadır. Fakat ilk etapta herhangi bir kötü amaca hizmet etmeyen bir uygulama, kullanıcının platformuna yerleştikten sonra kendini yenileyerek zararlı hale gelebilmektedir. Bu çalışma kapsamında ilk etapta zararlı olmayan daha sonra kendini güncelleyerek zararlı hale gelen bir saldırı çeşidi ele alınmıştır. Ayrıca bu tür saldırılar kullanıcıdan habersiz internet ağını kullanarak mobil platform üzerindeki bilgileri başka noktalara aktarmak içinde kullanılmaktadır. Bu saldırı türü bazı durumlarda gizli ağ bağlantılarıyla gerçekleştirilmektedir. Bundan dolayı çalışmada mobil platform ile kurulan gizli ağ bağlantılarının ve bu bağlantılardan yapılabilecek zararlı yazılım güncellemelerinin üzerinde durulmuştur. Çalışma sonucunda gizli ağ saldırılarını tespit ve önleme işlemlerinde kullanılacak bir mobil uygulama geliştirilmiştir.**

***Anahtar Kelimeler*—Mobil cihaz güvenliği, Ağ güvenliği, Bilgi güvenliği, Saldırı tespit sistemleri**

***Abstract*—Nowadays the detection of malicious software plays an important role in the fight against cyber attacks. In overall, detection of malware are made during the initial setup process or loading to the application market. But, even if an application does not serve any evil purpose at the first step, it can renew itself as harmful after settling on the user's platform. In this study, non-harmful in the first step then it becomes a kind of harmful attack by self-update is considered. In addition, such attacks are used to transfer information on mobile platforms to another location by using Internet networks without informing users. In some cases, these type of attacks are carried out by secret network connections. Therefore, the secret network connections established with mobile platform and harmful software updates can be done through these links are analyzed in this study. As a result of this study, a mobile application for detection and prevention of secret network attacks was developed.**

***Keywords*—Mobile device security, Network security, Information security, Intrusion detection systems**

[1] Gazi Üniversitesi, Teknoloji Fakültesi Bilgisayar Mühendisliği Bölümü 06500, Teknikokullar, Ankara- Türkiye, e-posta: saadinoyucu@gazi.edu.tr
[2] Gazi Üniversitesi, Teknoloji Fakültesi Bilgisayar Mühendisliği Bölümü 06500, Teknikokullar, Ankara- Türkiye, e-posta: polath@gazi.edu.tr
[3] Gazi Üniversitesi, Teknoloji Fakültesi Bilgisayar Mühendisliği Bölümü 06500, Teknikokullar, Ankara- Türkiye, e-posta: iadogru@gazi.edu.tr

I. GİRİŞ

MOBİL platformlar için geliştirilen uygulamalar sayesinde kullanıcıların günlük işleri kolaylaştırılmıştır. Kullanıcı, mobil platformların uygulama pazarından istediği uygulamayı rahatlıkla indirip kendi platformuna kurulabilmektedir. Uygulama pazarına erişimde ise ağ bağlantılarının farklı türleri kullanılmaktadır [1]. Erişim kolaylığı ve yüksek kullanılabilirliğe sahip mobil uygulamaların sayısı giderek artmaktadır. Bu durum mobil uygulamaları günümüz insanın vazgeçilmezi haline getirmektedir. Bununla birlikte mobil platformlar kötü niyetli yazılımlar için mükemmel bir yayılma ortamı sağlamaktadır [1]. Özellikle mobil ödeme sistemlerinin kullanımının artması saldırganları mobil platformlara saldırmak için güdülemektedir.

Mobil platformlar için geliştirilen birden fazla işletim sistemi vardır. Bunlardan en çok bilinenleri iOS, Android, BlackBerry OS ve Windows Phone'dur. Bu işletim sistemlerinden Android dünya genelinde en çok kullanılan mobil işletim sistemi olma özelliğini devam ettirmektedir [2]. Bu yüksek kullanım tercihi Android'i kötücül yazılımların/geliştiricilerin hedefi haline getirmektedir. Yapılan araştırmalara göre mobil tabanlı kötücül saldırıların %99'u Android tabanlıdır [2]. Android'in kötücül yazılımlar için hedef haline gelmesinde çeşitli faktörler vardır. Bunlardan biri Android'in resmi uygulama marketi olan Play Store'a yüklenen uygulamalara yönelik pasif koruma sergilenmesidir. Diğer önemli faktör ise Android işletim sistem sisteminin açık kaynak kodlu yapısıdır [2].

Kötü amaçlı yazılımlar mobil güvenlik için en büyük tehditlerden biridir [3]. Mobil kötü amaçlı yazılımlar üç ana kategoriye ayrılır. Bunlar virüs, truva ve casus yazılımlardır [4]. Kötü amaçlı yazılımlardaki virüs saldırılarına karşı mobil platformları koruma konusunda iki yaklaşım vardır. İlk yaklaşım cihaz üzerinde anti virüs yazılımı ile tarama yapmaktır. İkinci yaklaşımda ise tek cihaz ile güvenilir bir bilgi işlem ortamı kurmaktır. İlk yaklaşımda çevrimiçi virüs veri tabanına bağlanılarak işlem gerçekleştirmek gerekmektedir. İkinci yaklaşımda ise cihazda güvenilir ortamın kurulması ve korunması için güvenlik hizmetine ihtiyaç vardır [5].

Kötü amaçlı yazılımın bulaştığı uygulamalar kendi kendini kullanıcının haberi olmadan arka planda

güncelleyebilmektedir. Bu işlemi gerçekleştirirken paket içeriklerini gizli tutarak tehlikeli paket içeriklerini okuyabilecek uygulamaların izlemesine de engel olmaktadır. Ayrıca profesyonel kötü amaçlı yazılımların yaptığı ağ bağlantıları da gizli ağ bağlantıları olmaktadır. Kötü amaçlı yazılımlar gizli ağ bağlantıları ile kullanıcıdan habersiz kişisel bilgileri başka noktalara aktarabilmektedir. Aynı yöntemle kendi güncel kötü amaçlı yazılım dosyalarını kullanıcının platformuna indirebilmektedir. Bu durumda ise çoğu güvenlik senaryosu saf dışı bırakılmaktadır.

Literatür incelendiğinde mobil platformların güvenliğini sağlamak adına birçok çalışma yapıldığı görülmektedir. Özellikle kötü amaçlı yazılımların tespiti, mobil ağ ve mobil geçici ağların güvenliği üzerine yapılan çalışmalar oldukça fazladır.

Oberheide ve arkadaşları 2008 yılındaki çalışmalarında kötü amaçlı yazılımların tespitinde farklı bir yöntem uygulamışlardır. Kaynak tüketimi analizine göre tespit edilen kötü amaçlı yazılımlar, mobil sistemlerde sanallaştırılmış bulut hizmeti kapsamında ele alınmıştır. Çalışma sonucunda daha az CPU ve bellek tüketiminin olduğu gözlemlenmiştir [6].

Yu ve arkadaşları 2009 yılındaki çalışmalarında mobil güvenlik erişim sistemi geliştirmişlerdir. Çalışmalarında ağ üzerinden iletilen bilgilerin daha güvenli olması için SSL, VPN ve akıllı kart teknolojisini kullanmışlardır [7]. Üst düzey güvenlik gerektiren işlemler için bir öneri olarak sunulmuştur.

Ahmad ve arkadaşları 2013 yılındaki çalışmalarında Andoid ve IOS mobil işletim sistemlerini güvenlik açısından karşılaştırmışlardır. Çalışma boyunca yapılan karşılaştırmalar sonucunda güvenlik bakımından IOS işletim sisteminin Android'e göre daha avantajlı olduğu sonucuna varmışlardır [8].

Sun ve arkadaşları 2014 yılındaki çalışmalarında beş açıdan Android güvenliğini ele almış ve bir mobil güvenlik uygulama denetlemesi önermişlerdir. Bu çalışmalarındaki teoriyi desteklemek için üç tekniği prototip olarak tasarlanmışlardır [9].

Penning ve arkadaşları 2014 yılındaki çalışmalarında kötü amaçlı mobil yazılım tehditleri ve saldırıları, kötü amaçlı yazılıma yönelik siber suçlu motivasyonları, mevcut korunma yöntemleri ve bunların sınırlılıklarını özetlemektedirler. Ayrıca çalışmalarında kötü amaçlı mobil yazılım tespiti için bulut tabanlı bir çerçeve önermektedirler [10].

Wang ve Alshboul 2015 yılındaki çalışmalarında mobil güvenlik testleri üzerine odaklanmış ve mobil güvenlik için dört test yaklaşımını incelenmişlerdir. Bunlar adli mobil yaklaşım araçları, sızma testi, statik ve dinamik analizlerdir [4].

Önceki çalışmaların genellikle güvenlik senaryoları ve kötücül yazılımların tespiti üzerine yapılan çalışmalar olduğu görülmektedir. Fakat bazı çalışmalar ağ güvenliği üzerine yoğunlaşmıştır. You ve arkadaşlarının 2013 yılındaki çalışmalarında yaptıkları TCP ve SSL karşılaştırması [11], Rashwan ve arkadaşlarının 2014 yılındaki çalışmalarında oluşturdukları mobil sistemler için güvenlik senaryosu ve bu senaryo içerisinde sürekli iletişim performansı analizinin yapılması [12] daha önce yapılan önemli çalışmalardandır. Fakat bu çalışmada ele alınan konu daha önce yapılan çalışmalardan farklı bir konuya dikkat çekmektedir.

Bu çalışmada ilk etapta hiçbir kötücül unsur içermeyen bir uygulamanın, gizli bağlantılar ile kendini güncelleyip kötücül hale gelmesinin tespiti yapılmıştır. Ayrıca uygulamanın ağ davranış biçimi incelenerek kullanıcıya uyarı verilmesi amaçlanmıştır. Kullanıcı bu uyarılara göre karar verip çalışan uygulamaları kapatabilecektir. Böylelikle kötücül yazılımın neden olduğu kötü amaçlı saldırılardan mobil platformun ve mobil kullanıcının korunması amaçlanmıştır. Bu doğrultuda Android işletim sistemi için bir mobil uygulama geliştirilmiştir.

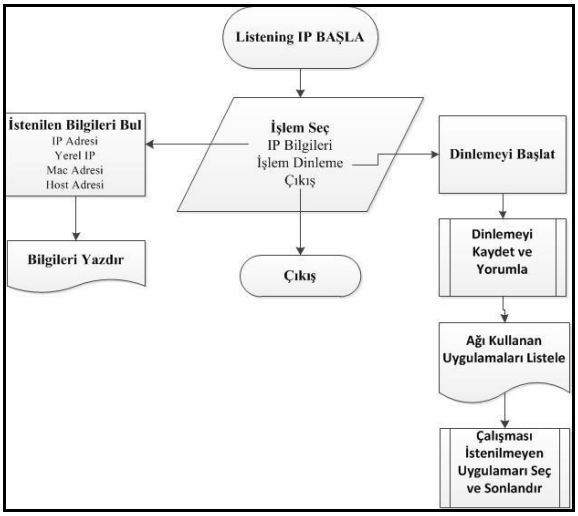
II. MATERYAL VE METOD

Akıllı mobil sistemlerden önce saldırıların yayılması için en etkili yollardan birinin bluetooth olduğu söylenebilir [13]. Fakat bluetooth bağlantısı olabilmesi için aradaki mesafenin kısa olması ve bluetooth sisteminin açık olması gerekmektedir. Günümüzde internet ağı yaygın olarak kullanılmakta ve hemen her mekânda mobil cihazların kullanabileceği kablosuz bir internet ağı bulunmaktadır. Bu durum kötü niyetli insanların internet ağını kullanarak zarar verme olasılığını giderek arttırmıştır. Bu nedenle bu çalışmada gerçekleştirilen uygulama da örnek teşkil etmesi açısından kablosuz internet ağı kullanılmıştır.

Çalışmada, mobil işletim sistemi olarak Android tercih edilmiştir. Bu tercihin sebebi Android işletim sisteminin açık kaynak kodlu olması, kullanılan cihaz sayısının fazla ve saldırı oranlarının yüksek olmasıdır. Android çoğu zaman işletim sisteminin tüm detaylarına ve gizlenmiş özelliklerine erişim vermemektedir. Çünkü neredeyse hiçbir mobil platform üreticisi Android tabanlı sistemlerde kullanıcılara "root" yetkisi sunmamaktadır. İşletim sisteminin tüm yeteneklerini kullanabilmek için root yetkisine ihtiyaç vardır. Bu nedenle çalışma kapsamındaki test işlemlerinde kullanılacak mobil platformun root yetkisine sahip olması gerekmektedir. Geliştiriciler için oldukça önemli avantajlar sağlayan root yetkisini kullanırken dikkat edilmelidir. Sistemi sürekli root yetkisinde kullanmak başka güvenlik sorunlarına neden olabilmektedir.

Çalışma kapsamında geliştirilen uygulama iki şekilde çalışmaktadır. Birincisi ev ve iş yerlerindeki modemler üzerinde bulunan güvenlik duvarı özelliğini kullanarak mobil platformları korumaya çalışırken gerekli olan dış İnternet Protokolü (IP: Internet Protocol) adresini tespit etmektir. Geliştirilen uygulama sayesinde dış bağlantılarda kullanılan IP adresi bilgisi rahatlıkla tespit edilebilmektedir. Bu bilgi ile kullanıcıların modem üzerinde yapacağı gerekli düzenlemeler sayesinde ev ve iş yerlerindeki bağlantılarını zararlı erişimlerden koruması planlanmaktadır. Diğer kullanım şeklinde ise kablosuz internet ağından gelen sinyaller ve erişimler sürekli kontrol edilecektir. Bu kontroller sonucunda

hangi uygulamaya erişildiği ve arka planda kullanıcıdan habersiz hangi uygulamaların çalıştığı liste halinde kullanıcıya sunulmuştur. Kullanıcı, çalışmasını istemediği uygulamaları kolaylıkla kapatabilmektedir. Böylelikle zararlı ağ erişiminin engellenmesi planlanmaktadır. Uygulamanın çalışma mantığı şekil 1.'de gösterilmiştir.



Şekil 1. Geliştirilen uygulamanın işleyiş biçimi

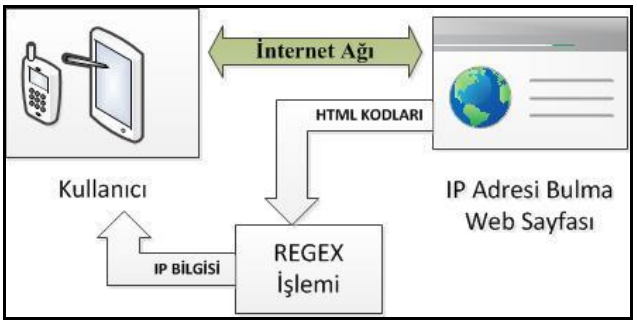
Şekil 1.'de görüldüğü gibi geliştirilen uygulama sayesinde IP bilgileri ile birlikte yerel IP adresi, MAC adresi ve Host adresi de kullanıcıya sunulmaktadır. Burada belirtilen IP adresi dış IP adresini temsil etmektedir. Gizli ağ bağlantılarını görebilmek için ise kullanıcı ağı dinlemeyi başlatmalıdır. Ağ üzerinde yapılan dinlemeler kaydedilir, yorumlanır ve ağı kullanan uygulamalar bu işlemler sonucunda kullanıcıya listelenir. Kullanıcı listeden istediği uygulamayı seçip kapatabilecektir.

Uygulamada gizli ağ bağlantılarını tespit etmek için paket koklama tekniği kullanılmaktadır. Paket koklama işlemi için Tcpdump paket analizcisi tercih edilmiştir. Tcpdump, ağ arabiriminden geçen paketleri kaydedip, pcap (packet capture) destekli herhangi bir araç kullanarak kaydedilmiş paketleri okuma işinde kullanılır [14]. Tcpdump yoğun ağ trafiğinde bile sorunsuz çalışabilmektedir. Bu nedenden dolayı ağı dinlerken Tcpdump tercih edilmiştir. Çalışma kapsamındaki mobil uygulama, Android uygulama geliştirme aracı olan Eclipse üzerinde geliştirilmiştir. Programlama dili olarak ise Java seçilmiştir.

III. UYGULAMA GELİŞTİRME

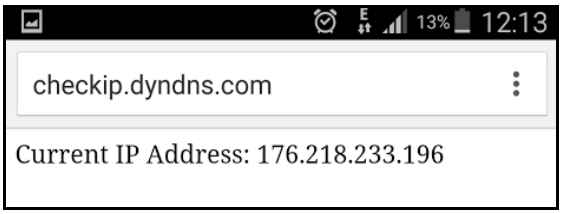
Mobil uygulama geliştirilirken ilk etapta bir emülatör tanımlamak gerekmektedir. Emülatör, mobil bir platformun donanım ve yazılım özelliklerini içeren sanal bir cihazdır [15]. Bir uygulamanın test ve modellemesinin rahat yapılabilmesi için Android Sanal Aygıt yapılandırılmasının yapılması gerekmektedir [15].

Geliştirilen uygulamanın ilk çalışma şekli olan dış IP adresini bulmak için metin içerisinde kural tabanlı anlamlı ifadeler elde etme tekniği Regex (Regular Expression: Düzenli İfade) kullanılmıştır. Regex belirli bir ifadeyi belli bir kalıba göre bulmayı, değiştirmeyi veya parçalamayı sağlayan yazılım algoritmasıdır [16]. Regex bu çalışmada dış IP bilgisini alma işlemin için kullanılmıştır. Şekil 2.'de Regex işleminin uygulamada yaptığı görev açıklanmıştır.



Şekil 2. Regex işlemi

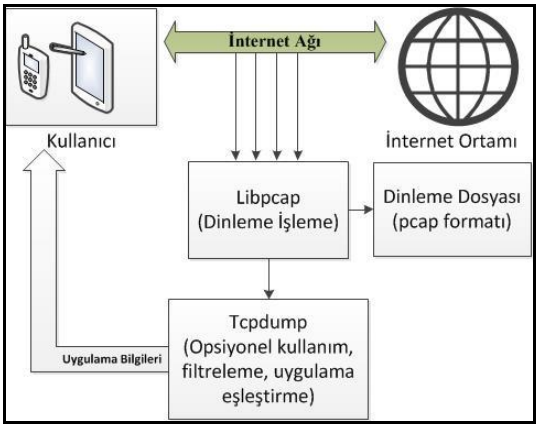
Kullanıcı mobil platformlardan uygulamayı açarak IP bilgilerini bulma işlemini başlatır. Ardından şekil 2.'de görüldüğü gibi mobil platform internet ağı yardımıyla dış IP adresini tespit etme hizmeti sunan bir web sayfasına bağlanır. Bu web sayfasının adresi http://checkip.dyndns.com/ adresidir. Android bir platform ile web sayfasına bağlantı yapıldığında alınan bilgi resim 1.'de gösterilmiştir.



Resim 1. IP adresini bulmak için kullanılan web sayfa bağlantısı

Resim 1.'de görülen web sayfasının Hiper Metin İşaretleme Dili (HTML: Hypertext Markup Language) kodları içerisinden gerekli bilgiler alınmakta ve Regex işlemine tabi tutulmaktadır. Bu işlem sonucu elde edilen dış IP bilgisi kullanıcıya sunulmuştur. Mobil uygulamada kullanıcıya gösterilmek istenilen yazı, metin ve resimler için ise ayrı ayrı hazırlanan TextView'ler oluşturulmuştur.

Gerçekleştirilen uygulamanın ikinci çalışma şekli gizli ağ bağlantılarını kullanıcıya göstermek ve engellemektir. Bunun için hazırlanan uygulamanın açılması ve kullanıcının ağı dinlemeyi başlatması gerekmektedir. Böylelikle ağ analiz verileri kaydedilebilecektir.



Şekil 3. Gizli ağ bağlantılarını dinleme işlemi

Şekil 3.'te görüldüğü gibi kullanıcı mobil platformlardan geliştirilen uygulamayı kullanarak ağı dinlemeyi başlatır. Bu adımdan sonra ağdaki tüm hareketler ve dalgalanmalar libpcap kütüphanesi yardımıyla pcap formatında kaydedilmektedir. Kaydedilen bu bilgiler tcpdump ile işlenerek çalışan uygulamalarla eşleştirilmiştir. Çalışan uygulamalar kullanıcıya liste halinde sunulmuş ve kullanıcının tüm ağ bağlantısı hakkında bilgi sahibi olması sağlanmıştır. Ayrıca kullanıcının, listelenen uygulamalardan istediğini kapatabilmesine olanak verilmiştir.

Uygulama gelişilirken bazı noktalarda Linux komutlarından faydalanılmıştır. Android işletim sistemi üzerinde geliştirilen uygulamanın root yetkisine sahip olması gerekmektedir. Kullanıcı değiştirme işlemi ve pcap uzantılı dosyanın oluşturulması işleminde Linux konutlarından yararlanılmıştır.

Ağı dinleme sonucu alınan çalışan uygulamaların listesi daha önce hazırlanan ve kullanıcıya liste yapısını sunmakta yararlanılan "MyCustomBaseAdapter" ile kullanıcıya sunulmaktadır. Böylelikle ağı kullanan uygulamalar ekranda listelenip kullanıcıya bildirilmektedir. Bu işlemler sonucunda kullanıcıdan habersiz çalışan tüm uygulamaların kontrol altına alınması sağlanmıştır. Kullanıcı liste ekranından istediği uygulamayı seçip kapatabilmektedir.

IV. ANALİZ VE TEST

Sistem geliştirilirken kullanılan emülatör sayesinde gerekli test işlemleri uygulama geliştirmenin her aşamasında yapılmıştır. Görünüm dosyalarının oluşturulması vb. işlemlerde başarılı bir şekilde çalışan emülatör ağ dinleme işlemlerinde tıkanmalara neden olmuştur. Bunun nedeni ise geliştirilen uygulamada kullanılmak istenen kablosuz ağın emülatörde çalışmamasıdır. Bu nedenle gerekli test işlemleri root yetkisine sahip ve kablosuz internet iletişimini destekleyen Android işletim sistemi yüklü bir cihazda gerçekleştirilmiştir. Resim 2.'de geliştirilen uygulamanın kullanıcıyı karşılama ara yüzü gösterilmektedir.

Resim 2. Kullanıcı karşılama ara yüzü

Geliştirilen uygulamadan faydalanarak yapılabilecek işlemler Resim 2.'de gösterilmektedir. IP bilgilerini bulmak için "Ip Bilgileri", gizli ağ bağlantılarını görmek ve ağ dinlemeyi başlatmak için "İşlem Dinleme" ve uygulamayı kapatmak için "Çıkış" butonuna basmak yeterlidir.

Resim 3.'te yer alan ekran görüntüsünde ise geliştirilen uygulamada ağ dinleme sonucu çalıştığı tespit edilen uygulamaların listesi gösterilmektedir.

Resim 3. Ağ dinleme sonucu çalışan uygulamaların listesi

Resim 3.'te görüldüğü gibi ağı dinleme sonucu ağı kullanan uygulamaların listesi kullanıcıya sunulmuştur. Geliştirilen uygulama sayesinde kullanıcı, çalışan uygulamalardan istediğini seçebilmekte ve uygulananın çalışmasına son verebilmektedir. Bu işlem için ekranda listelenen uygulamalardan birini seçip "Durdur" butonuna basması yeterlidir. Yapılan testler sonucu uygulamanın dış IP adresini öğrenme fonksiyonundan, ağı dinleme ve çalışan uygulamaları sonlandırma gibi bütün fonksiyonlarının çalıştığı net olarak görülmüştür. Ayrıca kullanıcının kullanmadığı fakat arka planda ağı kullanan uygulamaların olduğu gözlemlenmiştir.

V. SONUÇ VE ÖNERİLER

Bu çalışmada, ilk etapta hiçbir kötücül yazılım içermeyen daha sonra zararlı hale gelen bir saldırı türü ele alınmıştır. Çalışma kapsamında zaman içerisinde kendine ait kötü amaçlı yazılımı güncelleyen ve bu işlemi gizli ağ bağlantılarıyla gerçekleştiren bir saldırı çeşidi incelenmiştir. Bu tür gizli ağ saldırılarını engellemek için çalışma kapsamında bir mobil uygulama geliştirilmiştir. Uygulama sayesinde farklı durumlarda oluşan ağ trafiği kontrol edilerek kullanıcıdan habersiz çalışan uygulamalar kullanıcıya bildirilmiştir. Yapılan test ve incelemeler sonucu ağ üzerinden yapılan saldırılarda zararlı yazılım bulaşan uygulamaların ağ davranışları ve trafik desenlerinin zararlı yazılım tespitinde oldukça önemli rol oynadığı görülmüştür. Gizli ağ saldırılarında ağ trafiğini inceleyip bu incelemeye göre saldırı önlemi almanın diğer yöntemlere göre daha başarılı olduğu görülmüştür. Ağı kullanan her uygulamanın zararlı olmayacağı için ileriki çalışmalarda bu konu üzerine farklı çalışmalar yapılabilir. Çalışma kapsamında geliştirilen uygulamanın kendi güvenliğinin sağlanması ise farklı bir çalışma olarak ele alınabilecektir.

KAYNAKLAR

[1] Gelenbe, E., Gorbil, G., Tzovaras, D., Liebergeld, S., Garcia, D., Baltatu, M., & Lyberopoulos, G. (2013, June). Security for smart mobile networks: The NEMESYS approach. In *Privacy and Security in Mobile Systems (PRISMS), 2013 International Conference on* (pp. 1-8). IEEE.

[2] Kabakuş, A. T., Doğru, İ. A., & Çetin, A. Android kötücül yazılım tespit ve koruma sistemleri. *Erciyes Üniversitesi Fen Bilimleri Dergisi*, (31), 9-16.

[3] Wang, Y., Streff, K., & Raman, S. (2012). Smartphone security challenges.*Computer*, (12), 52-58.

[4] Wang, Y., & Alshboul, Y. (2015, February). Mobile security testing approaches and challenges. In *Mobile and Secure Services (MOBISECSERV), 2015 First Conference on* (pp. 1-5). IEEE.

[5] Sudin, S., Tretiakov, A., Ali, R. H. R. M., & Rusli, M. E. (2008, December). Attacks on mobile networks: An overview of new security challenge. In *2008 International Conference on Electronic Design*.

[6] Oberheide, J., Veeraraghavan, K., Cooke, E., Flinn, J., & Jahanian, F. (2008, June). Virtualized in-cloud security services for mobile devices. In *Proceedings of the First Workshop on Virtualization in Mobile Computing* (pp. 31-35). ACM.

[7] Yu, D., Chen, N., & Tan, C. (2009, March). Design and implementation of mobile security access system (MSAS) based on SSL VPN. In *Education Technology and Computer Science, 2009. ETCS'09. First International Workshop on* (Vol. 3, pp. 152-155). IEEE.

[8] Ahmad, M. S., Musa, N. E., Nadarajah, R., Hassan, R., & Othman, N. E. (2013, July). Comparison between android and iOS Operating System in terms of security. In *Information Technology in Asia (CITA), 2013 8th International Conference on* (pp. 1-4). IEEE.

[9] Sun, Y., Wang, Y., & Wang, X. (2014, November). Mobile Security Apps: Loyal Gaurds or Hypocritical Thieves?. In *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference on* (pp. 568-572). IEEE.

[10] Penning, N., Hoffman, M., Nikolai, J., & Wang, Y. (2014, May). Mobile malware security challeges and cloud-based detection. In *Collaboration Technologies and Systems (CTS), 2014 International Conference on* (pp. 181-188). IEEE.

[11] You, W., Xu, L., & Rao, J. (2013, May). A comparison of TCP and SSL for mobile security. In *Sensor Network Security Technology and Privacy Communication System (SNS & PCS), 2013 International Conference on* (pp. 206-209). IEEE.

[12] Rashwan, A. M., Taha, A. E. M., & Hassanein, H. S. (2014). Characterizing the Performance of Security Functions in Mobile Computing Systems. *Internet of Things Journal, IEEE*, *1*(5), 399-413.

[13] Willems, E. (2013). Android under attack. *Computer Fraud & Security*,*2013*(11), 13-15.

[14] Fuentes, F., & Kar, D. C. (2005). Ethereal vs. Tcpdump: a comparative study on packet sniffing tools for educational purpose. *Journal of Computing Sciences in Colleges*, *20*(4), 169-176.

[15] Bläsing, T., Batyuk, L., Schmidt, A. D., Camtepe, S. A., & Albayrak, S. (2010, October). An android application sandbox system for suspicious software detection. In *Malicious and unwanted software (MALWARE), 2010 5th international conference on* (pp. 55-62). IEEE.

[16] Thompson, K. (1968). Programming techniques: Regular expression search algorithm. *Communications of the ACM*, *11*(6), 419-422.

Saadin Oyucu, 2012 yılında Gazi Üniversitesi Teknik Eğitim Fakültesi, Bilgisayar Sistemleri Eğitimi Bölümünden mezun oldu. Lisans eğitimi boyunca çeşitli kurslarda eğitici olarak görev yaptı. Lisans eğitimini bitirdikten sonra 2 yıl özel sektörde web yazılım ve arayüz geliştiricisi olarak çalıştı. Bu dönemde birçok önemli kuruluştaki projelerde görev aldı. 2014 yılında ÖYP kapsamında Adıyaman Üniversitesi, Bilgisayar Mühendisliği Ana bilim Dalına Araştırma Görevlisi olarak atandı. Aynı yıl Gazi Üniversitesi Fen Bilimleri Enstitüsüne görevlendirilme ile geldi. 2015 haziran ayında yüksek lisansını tamamladı. Halen görevlendirme ile geldiği, Gazi Üniversitesi Teknoloji Fakültesi Bilgisayar Mühendisliği bölümünde Araştırma Görevlisi olarak çalışmaktadır. Çalışma ve ilgi alanları; M2M, IoT, Robotik, Web Servisler, Yazılım, NoSQL Veritabanları, Mobil sistem Güvenliği, Web uygulama geliştirme, Web arayüz geliştirme.

Hüseyin Polat, 1993 yılında Karadeniz Teknik Üniversitesi, Mühendislik Mimarlık Fakültesi Elektrik Elektronik Mühendisliği Bölümünden mezun oldu. 1995 yılında Gazi Üniversitesi Teknik Eğitim Fakültesi Elektronik Bilgisayar Eğitimi Bölümüne Uzman olarak göreve başladı. Gazi Üniversitesi Fen Bilimleri Enstitüsünde 1998 yılında yüksek lisans ve 2006 yılında doktorasını tamamladı. 2010 yılında Gazi Üniversitesi Teknik Eğitim Fakültesi Elektronik Bilgisayar Eğitimi Bölümüne Yardımcı Doçent olarak atandı. 2011 yılında da Gazi Üniversitesi Teknoloji Fakültesi Bilgisayar Mühendisliği Bölümüne Yardımcı Doçent olarak atandı. Halen burada görevine devam etmektedir. Çalışma ve ilgi alanları; Bilgisayar ağları, Bilgisayar donanımı, Endüstriyel otomasyon, Makinalar arası iletişim(M2M) Biomedikal sinyal işleme, Yapay sinir ağları

İ. Alper Doğru, 2004 yılında Atılım Üniversitesi Bilgisayar Mühendisliği Bölümünden mezun oldu. 2007 yılında Gazi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümünde yüksek lisansını 2012 yılında Elektronik-Bilgisayar eğitimi anabilim dalında doktorasını tamamladı. Halen Gazi Üniversitesi Teknoloji Fakültesi Bilgisayar Mühendisliği Bölümünde Yrd. Doçent olarak görev yapmaktadır. Çalışma ve ilgi alanları, Mobil şebeke teknolojileri, Mobil tasarsız ağlar, Mobil güvenlik, Network forensics, Mobil forensics, Mobil kötücül yazılım tespiti ve Bulut bilişim sistemleridir.