Istanbul Commerce University Journal of Science
İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi, 15(30), Güz 2016
http://dergipark.gov.tr/ticaretfbd

Araştırma Makalesi

MOBİL CİHAZLARDA GÜVENLİK – TEHDİTLER ve TEMEL STRATEJİLER*

Gözde KARATAŞ[1] Akhan AKBULUT*[2] Abdül Halim ZAİM[3]

[1]*İstanbul Kültür Üniv. Fen-Edebiyat Fak. Matematik-Bilgisayar Bölümü, İstanbul, Turkey*
g.karatas@iku.edu.tr
[2]*İstanbul Kültür Üniv. Mühendislik Fak. Bilgisayar Mühendisliği Bölümü, İstanbul, Turkey*
a.akbulut@iku.edu.tr
[3]*İstanbul Ticaret Üniv. Mühendislik Fak. Bilgisayar Mühendisliği Bölümü, İstanbul, Turkey*
azaim@ticaret.edu.tr

Öz

Tüketici elektroniğinin günümüzdeki en yaygın hali mobil cihazların kullanımıdır. Bu alandaki teknolojik gelişmeler, hayatımızın her alanına etki edecek şekilde artmakta ve yaşamımıza yön vermektedir. Artık bilgisayarlarla aynı donanımsal özelliklere sahip olabilen mobil cihazların kullanımı sadece iletişim amacıyla kalmayıp, internet kullanımı, iş, hobi ve sağlık alanlarındaki uygulamaları ile zenginlemiştir. Artan kullanım oranı ile bilgi ve iletişim güvenliğine daha fazla ihtiyaç duyulmaya başlanan bu cihazlara yönelik yapılan saldırılar karşısında taşınan bilgilerin güvenliğinin sağlanması gerekliliği ortaya çıkmaktadır. Mobil cihazlardaki güvenlik açıkları ve kötücül yazılım barındıran uygulamaların son kullanıcı tarafından yüklemesi ile kişisel bilgi ve haberleşme güvenliğini tehdit eden durumlar oluşmaktadır. Bu çalışmada, mobil uygulamalarda bulunan güvenlik açıkları, saldırı ve bu sorunlara ilişkin alınan önlemler anlatılmaktadır. Sadece son kullanıcıya yönelik tavsiyeler değil, aynı zamanda uygulama geliştiriciler için de dikkat edilmesi gereken hususlar özetlenmiştir. Son kullanıcıların, mobil sistemlerin saldırı yöntemlerine dair temel bilgileri öğrenmesi ile kişisel güvenliğin arttırılabileceği değerlendirilmektedir.

Anahtar Kelimeler: Mobil güvenlik, mobil testler, Android, iOS, saldırı yöntemleri.

Research Article

SECURITY IN MOBILE DEVICES - THREATS AND BASIC STRATEGIES

Abstract

The most common form of today's consumer electronics is the use of mobile devices. The technological developments in this area are increasing in such a way as to affect all aspects of our lives and give direction to our life. The use of mobile devices, which can now have the same hardware features as computers, is not only for communication but also enriched by applications in the areas of internet use, business, hobby and health. Increased usage rate and the need for information and communication security are beginning to be needed and it is necessary to ensure the security of the information carried against the attacks against these devices. Due to security vulnerabilities in mobile devices and malicious software loaded applications by end users, there are situations that threaten personal information and communication security. This study describes security vulnerabilities, attacks in mobile applications and precautions for those problems. It summarizes not only the end-user's recommendations, but also the points to note for app developers. It is evaluated that end users can increase personal security by learning basic info for attack methods of mobile systems.

Keywords: Mobile security, mobile tests, Android, iOS, mobile attacks.

* Received / Geliş tarihi: 22/06/2016 Accepted / Kabul tarihi: 30/09/2016
*Corresponding Author/ Sorumlu Yazar : a.akbulut@iku.edu.tr

1. GİRİŞ

Mobil cihazlar son on yılda boyut olarak daha küçük ancak kullanım kapasitesinde daha güçlü bir hale gelmişlerdir. Şu anda geliştirilen uygulamalar ile çok fazla özelliği gerçekleştirebilmektedirler. Dolayısıyla, cep telefonları basit bir bilgisayarın yapacağı işleri rahatlıkla yapabildikleri için bilgisayarların küçültülmüş hali olarak değerlendirilebilmektedir (Linage vd., 2016; Ju vd. 2015). Bu geliştirmeler kapsamında cep telefonlarının çoklu işlemleri başarıyla gerçekleştirebilmeleri için Symbian, iOS, Android OS ve Windows Mobile şeklinde telefonların işletim sistemleri de geliştirilmiştir (Ahmad vd., 2013, Sağıroğlu vd., 2009).

1.1 Symbian

Symbian aynı isimli firma tarafından mobil cihazlar için geliştirilmiş bir işletim sistemidir. GPRS, Bluetooth, 3G gibi gelişen teknolojileri benimsemiştir. Sony Ericsson, Nokia, Panasonic, Motorola ve Siemens firmaları Symbian'ın önde gelen üyelerindendir. C++, Java ve Visual Basic dillerinden biri kullanılarak yazılabilir. Ayrıca Symbian işletim sistemi virüslerden kolaylıkla etkilenir (Lu vd., 2010).

1.2 Android

Linux ile yazılmış mobil bir işletim sistemidir. Bu sistem kütüphaneler, ara katman kütüphaneler ve API C dili kullanılarak geliştirilmiştir. Android işletim sistemi tabanlı telefonlarda kullanılan uygulamalar ise Google'ın açık kaynak kodu uygulaması sayesinde isteyen herkes tarafından geliştirilmektedir. Diğer işletim sistemleri ile karşılaştırıldığında Android kullanıcılarına çok sayıda ücretsiz uygulama sunmaktadır. Android cihazların erişim yetkileri "rooting" adı verilen işlem ile düzenlenebilmektedir (Masruroh vd., 2016). İşletim sisteminin kaynağına erişmek anlamına gelen bu işlem ile işletim sistemi üzerinde kapsamlı değişiklikler yapılabilmektedir (Omeleze ve Venter, 2013; Penning vd., 2014). Android açık kaynak kodlu bir işletim sistemidir. Dolayısıyla tüm geliştiriciler ücretsiz olarak Android kodlarına erişebilmektedir. Android mimarisi ise aşağıda bir şekilde açıklanmıştır;

- Linux Çekirdeği; Android mimarisinin tabanındaki katmandır. Bu katmanda; donanım bilgileri ve uygulamaların çalışabilmesi için gerekli sürücüler yer almaktadır. Linux Çekirdeği paylaşılan hafıza, güç kontrolü, süreçler arası iletişim alanlarına etki eder.
- Kütüphaneler; bu kısımda, görüntüleme kontrolü için Surface Manager, C ile yazılmış sistem kütüphaneleri, veri yapıları kontrolü ve düzenlenmesi için SQLite, internet tarayıcısı için Webkit, grafik işlemleri için OpenGL, ses ve video işlemleri için Media Framework gibi yapılar bulunur.

- Android Çalışma Zamanı; Alt seviye işler için Android'in Linux Kernel'ini kullanır. Temel Java kütüphanelerini içerir. Ayrıca bu katmanda, Dalvik Sanal Makinesi ve Çekirdek Kütüphaneleri yer alır.
- Uygulama Çatısı; Android ile geliştiricilere çeşitli uygulamalar tarafından kullanılan uygulama programlama ara yüzlerine (API) erişim hakkı tanınmıştır. Bu mimari; içeriklerin yeniden kullanılması için tasarlanmıştır. Herhangi bir uygulamanın özellikleri yayınlanabilir ve bu özellikler diğer uygulamalar tarafından kullanılabilir. Bu sayede kullanıcılar uygulama içeriklerini istedikleri gibi değiştirebilir.
- Uygulamalar; Bunlar yerel ve üçüncü parti Android uygulamalarını kapsar. Yerel uygulamalar arasında Google Maps, E-posta sunucusu, telefon rehberi, SMS programı gibi temel uygulamalar yer almaktadır.

1.2.1 Android Güvenlik Programı

Android Güvenlik Programı; işletim sistemi için geliştirilen uygulamalar, aygıt yazılımı ve cihaz donanımının kısıtlarını belirler. Bu yapının ana bileşenleri:

- Tasarımı Gözden Geçirme: Her özellik teknik ekip tarafından gözden geçirilir.
- Test etme ve Kodu İnceleme: Ekipler ve danışmanlar tarafından gerçekleştirilen güvenlik incelemeleri.
- Olaylara Müdahale: Sistemde ortaya çıkan bir soruna/açıklığa karşı ekip sorunu çözmek için yazılımlar geliştirerek, güncellemeler yayınlarlar.
- Açık Kaynak ile Topluluk Gözden Geçirme: Sistemin açık kaynak kodlu olması meraklıların da testler yapmasına olanak tanır.

1.3 iOS

Geliştirici şirketi Apple olan, Unix veri tabanlı, Apple marka cihazlar için geliştirilmiş kapalı bir işletim sistemidir. Dolayısıyla oldukça güvenilir bir yapıya sahiptir. Uygulamaları geliştirmek için Mac işletim sisteminin yüklü olduğu bir bilgisayara ihtiyaç vardır ve iOS için geliştirilen uygulama marketten indirilmektedir. Uygulamanın ilk sürümleri çoklu işlemleri (multitasking) desteklemezken, iOS 4.0 sürümü ile çoklu işlemler de eklenmiştir (Tilson vd., 2011; Masruroh vd., 2016). Ayrıca kullanımı en kolay mobil işletim sistemidir. 2017 yılı itibariyle Apple'in üretimi devam eden tüm cihazları için kullanılmasını önerdiğini işletim sistemi sürümü iOS 10'dur.

1.3.1 iOS Güvenlik Mimarisi

iOS güvenlik mimarisi, işletim sisteminin çekirdeğinde gerçekleştirilmiştir;

- Güvenlik Sunucusu Programı: Arka planda çalışan güvenlik servisleri ile kullanıcı yönetimi ve diğer uygulamalar için bazı işlemler gerçekleştiren protokoller çalışmaktadır.
- iOS Güvenlik Uygulamaları: iOS Güvenlik arayüzü, çekirdek seviyesinde çalışan 4 katmandan oluşmaktadır. "Keychain, CFNetwork, Certificate, Randomization Services".
- Kimlik Doğrulama, Tanıma ve Yetkilendirme: Android işletim sisteminin sahip olduğu yapıya benzeyen bir yaklaşımı içerir. Ancak farklı olarak tüm iOS uygulamaları aynı birim içerisinde çalışır.

Mobil uygulamalar, kullanılacakları çalışma alanına göre kategorize edilirler. Bu sayede geliştiriciler istedikleri türde uygulamayı ne şekilde geliştireceklerine doğru bir şekilde karar verebilirler (Fan vd., 2016; Pooryousef vd., 2016);

- Platforma Özgü (Native) Uygulamalar; belli bir platforma özel geliştirilen uygulamalardır. Android için Java, Android Studio IDE; iOS için Objective-C, XCode IDE; Windows Phone için C# Visual Studio ortamlarında geliştirilirler. Bu dillerin dışında başka bir dil ile bu tip uygulama geliştirilemez. (Adinata ve Liem 2014). Mobil cihazların barındırdığı çekirdek kütüphanelerine erişim tam olduğundan, cihazların sunabildiği özelliklerden yararlanılabilecektir. Ancak güncelleme/dağıtım süreleri her bir platform için tekrar edildiğinden uzundur.
- Web Tabanlı Uygulamalar; Geliştirilen uygulamanın HTML5, CSS3, JavaScript, XML tarzı web programlama dilleri ile tarayıcılarda çalışacak şekilde yazılması ve sunulmasıdır. Bu tarz uygulamalar mağazalardan indirilmez ve tarayıcılar vasıtası ile erişilir (Lu vd., 2014). Kaynak çeşitliliği vardır, platformdan bağımsız geliştirilir. Ancak bu uygulamalar performansı düşürür, arayüz kütüphanesi çeşitliliği kısıtlıdır.
- Melez (Hybrid) Uygulamalar; Platforma özgü ve Web platformlarının ortak kullanımı ile hazırlanan uygulamalardır. Web uygulamalarından farkı; cihazın özelliklerini daha verimli kullanabilir ve uygulama mağazalarından indirilebilir. Bir diğer farkı ise bir kez geliştirilip tüm mobil platformlarda çalıştırılabilmesidir (Setiabudi vd., 2013; Bosnik vd., 2016).

2014 Yılı itibariyle mobil cihaz kullanım oranının, masaüstü bilgisayarların kullanım oranını geride bırakmış olması (Chaffey 2016) mobil cihazlar üzerinde çalışan uygulamaların sunduğu güvenlik imkanlarının arttırılması gerektiğinin açık bir göstergesidir. Makalenin ikinci bölümünde yazılımcıların uygulama geliştirirken yaptığı hatalardan, üçüncü bölümünde güvenlik riskleri ve yapılan ataklardan, dördüncü bölümde güvenlik adımları ve testlerinden, beşinci bölümde yapılan testlerdeki sorunlardan, altıncı bölümde güvenlik için geliştirilmiş yazılımlardan, yedinci bölümde güvenliği kırmak için kullanılan yöntemlerden bahsedilmiştir.

Ardından mobil cihazlarda güvenliğin ihlalini test etmek için bir uygulama yapılmıştır.

2. UYGULAMA GELİŞTİRİRKEN YAPILAN HATALAR

Güvenlik, tüm alanlarda birincil derecede önem verilmesi gereken bir konuyken genellikle bazı şartlar (zaman sınırı, kişinin yeterli derecede bilgili olmaması, kaynak kısıtı vb.) nedeniyle göz ardı edilmektedir. Ancak unutulmamalıdır ki hiçbir uygulama %100 güvenli değildir (Küçüksille vd., 2013). Aşağıda genel hatlarıyla geliştiricilerin göz ardı ettiği durumlar listelenmiştir;

i. Kırılmış şifreleme algoritmaları kullanmak: birçok uygulama geliştiricinin yaptığı yanlışlardan biridir. Kırılmamış veya kırılması çok güç algoritmalar kullanmak sistemin güvenliğini arttırır. Gelişmiş Şifreleme Standardı (AES-Advanced Encryption Standard), Veri Şifreleme Standardı (DES-Data Encryption Standart) kırılmış şifreleme algoritmalarına örnek olabilir.

ii. Verilerin saklanması: Uygulamalar, bazen ihtiyacı olmayan verilere ve ortamlara (fotoğraflar, rehber vb.) da erişmek isterler. Özellikle önemli verilerin erişilebilmesi durumunda saldırgan uygulama üzerinden tüm bilgilere ulaşabilir. Bunun önüne geçmek için verinin çalışma anında işlenip, uygulama kapatıldığında yok edilmesi gerekmektedir.

iii. Sunucu tabanlı kontrollerin yapılmaması: Uygulama geliştirilirken en çok özenilen ve üzerinde emek harcanan kısımlar kullanıcı arayüzleridir. Son kullanıcıların çoğu uygulamayı kullanılabilirliği ve görselliği ile değerlendirdiği bilinmektedir. Kısıtlı depolama kapasitesi ve işlem kabiliyeti sebebiyle, uzun sürün ve kapsamlı işlemleri mobil cihaz yerine sunucuların tercihen bulut ortamlarının üzerine aktarılarak gerçekleştirilmesi yöntemi, sunucu tarafında da güvenlik önlemlerinin alınmasını ve kontrollerin yapılmasını mecbur kılmaktadır.

iv. Güvenlikten sorumlu bir birim/kişi olmayışı: Uygulama geliştirildikten sonra test aşamasında uygulamanın çalışabilirliği ile beraber güvenliğini de ayrıca test edecek bir birim olmalıdır. Uygulama testlerinde otomatik test araçlarından faydalanılarak farklı işletim sistemi sürümlerinde ve farklı donanımdaki mobil cihazlarda kontrollerin daha süratli bir şekilde yapılması önerilmektedir.

v. Girdi kontrollerinin yapılmaması: Mobil uygulamaların arayüzlerindeki girdi alanlarının kontrol edilmemesi güvenlik zafiyetlerinin oluşmasına neden olmaktadır. Bu yüzden girilen değerlerin doğruluğunu kontrol eden mekanizmaların eklenmesi gerekir. Örneğin sayısal bir değer girilmesi gereken alanların kontrol edilmemesi, özellikle sorgulara alınacak giriş değerlerinin tiplerinin kontrol edilmemesi vb.

vi. Açıklama satırlarında detaylı bilgiler vermek: Geliştiricilerin uygulamanın kod tarafına yazmış olduğu açıklama satırları, bu satıların içerisine aldıkları şifreler/kullanıcı isimleri sonradan görülebilmektedir. Bu da çok sık yapılan bir hatadır.

vii. Gereksiz yetkilendirme: Uygulamanın yetki tabloları düzenlenirken sadece ihtiyaç olanlar değerlendirilmelidir. Özel bilgilerin olacağı tablolara erişim kısıtı getirilmelidir.

viii. Açık şifreleme anahtarları: Şifreleme işleminde kullanılan anahtar, sunucu tarafında güvenli bölgede şifreli bir şekilde tutulmalıdır.

ix. Uygulama bütünlüğünün korunmaması: Uygulamanın sunucu üzerinden bilgilerinin kontrol edilmesi ve güncel kalması saldırganların sistemde değişiklik yapıp yapmadığını anlayabilmek için faydalı olabilir.

3. MOBİL UYGULAMALARDA GÜVENLİK RİSKLERİ VE ATAKLAR

Güncel mobil cihazlar aşağıda listelenen özelliklere sahiptir;

x. Artık her akıllı telefonda bir işletim sistemi bulunmaktadır (iOS, Android, Windows Phone).

xi. 3G/4G, Wireless, Bluetooth ağları.

xii. İnternete rahatlıkla erişebilirlik.

xiii. Uygulama Marketinden indirilen başkalarının geliştirdiği uygulamaları çalıştırabilirler.

xiv. MMS ve SMS gönderirler.

xv. Sensör bulundururlar.

Bu özelliklerin mevcudiyeti aynı zamanda saldırıya açık olma durumunu beraberinde getirir. Olası saldırıları önlemek ve mobil cihazlarda güvenliği sağlamak için aşağıdaki adımlar izlenmelidir.

- Hazırlık,
- Bilgi Toplama,
- İş Parçacığı Modelleme,
- Zafiyet Analizi,
- Saldırıları/Zararlı Yazılımı belirleme,
- Güçlü Şifreleme Yöntemleri Kullanma,
- Saldırıları önleme,
- Sistem açıklarını düzenli olarak kontrol etme.

Bu adımlar izlenerek mobil cihazlar için test geliştirilebilir. Aşağıda Mobil cihazlar için saldırı çeşitlerinden bahsedilmiş, bir saldırı anında cihazdaki işlemler anlatılmıştır (Sun vd., 2011; Wang ve Alshboul, 2015).

3.1 Saldırı Çeşitleri

Mobil cihazlar saldırılara oldukça açıktır. Bunlar genellikle kendini normal yazılım olarak gösteren yazılımların içinde gelirler (Bere, 2013; Wang vd., 2015, Wang vd., 2014, Kikuchi vd., 2016, Mohamed vd., 2016). Mobil cihazlara yapılan ataklar şu şekilde listelenmektedir.

- *İzinsiz Dinlemek (Sniffing):* Her türlü veri aktarımının izinsiz üçüncül bir kişi/sistem tarafından dinlenmesi ve/veya elde edilmesidir. Amacı; şifreleri, E-posta metnini, transfer edilen dosyaları yakalamaktır.
- *Toplu Gönderim (Spamming):* Kullanıcının isteği dışında, kullanıcıya ait olan bir cihaza veya adrese gönderilen sahte iletiler ile bilgilere ulaşmayı hedefler. Örneğin istenmeyen E-posta, istenmeyen MMS mesajı gibi
- *Yanıltma (Spoofing):* DNS zehirlenmesi olarak da adlandırılır. DNS sunucusunun ön bellek bilgilerine yeni bir veri eklenerek veya aradaki verileri değiştirerek sunucunun isminin yanlış IP adresleri göndermesine ve trafiğin başka bir bilgisayara yönlendirilmesine neden olan bir saldırıdır. Genel olarak saldırganın ağ üzerindeki bir sağlayıcıya erişip onun üzerinden bir başka kurbana saldırmasıdır.
- *Oltalama (Phishing):* Bankalar veya finans şirketleri tarafından gönderilmiş gibi görünen ve acil konular, önemli bilgiler içeriyormuş gibi duran sahte postalardır. E-posta ve web site oltalama işleminin birleşimidir.
- *Yönlendirme (Pharming):* Erişilmeye çalışılandan farklı bir illegal web sayfasına yönlendirmekle gerçekleştirilen bilişim suçudur.
- *Veri Sızıntısı (Data Leakage):* Uygulamalardan kısmi veri alınarak yapılan saldırıdır.
- *Hizmet Engelleme (DoS) Atakları:* Saldırganın daha önceden tasarlanmış olduğu makine üzerinden hedefe saldırı yaparak, karşı tarafın sisteminin kimseye hizmet veremez hale gelmesini sağlamayı amaçlayan bir saldırı çeşididir. Örneğin, bataryaya aşırı yüklenme (exhausting), radyo frekansına karıştırma (jamming) gibi.

Mobil cihazlarda gerçekleşen saldırı tipleri ise aşağıdaki şekildedir;

- *Kötücül Yazılımlar: Virüs, solucan, Truva atı ve casus yazılımlardır. Ünlü kötücül yazılımlara örnek olarak Sub7, Poison Ivy, Netbus, OptixPro, Subseven verilebilir. Bu yazılımlar bilgisayarlardaki gibi mobil cihazlarda da cihazdan cihaza bulaşabilir. Zararlı yazılımlar internetten, MMS mesajları ile depolama birimleri arasında ve mobil cihazlar arasındaki veri aktarımı ile yayılabilirler. Kötücül yazılımlar, bulaştıkları cihazlarda sertifikaları ele geçirme, veri toplama, kısa mesaj atma, klavye girişlerini*

kaydetme, ortam dinleme, çağrı kayıtlarına günlük oluşturma, yasadışı yazılım yükleme, GPS konum bilgisini kaydetme gibi faaliyetleri gerçekleştirerek kullanıcı bilgilerini ele geçirir ve kullanıcıya zarar verirler (Bere, 2013; Zhou, 2012).

- *Doğrudan Saldırı: Bu saldırılarda, saldırgan uygulamadaki bir açıklığı ya da işletim sistemindeki açıklığı kullanarak, yetkisiz erişim ile bilgileri elde etmeyi hedefler. Bu saldırıda cihaza herhangi bir yazılım yüklenmez dolayısıyla bu özelliği ile kötücül yazılımdan ayrılır (Penning vd., 2014; Guerid vd., 2011).*
- *Araya Girme: Bu yöntemde, ağ üzerindeki paketler toplanır ve analiz edilir ardından protokollerine göre ayrıştırılır ve eğer gerekli ise şifreli trafik çözülerek gönderilen veri ele geçirilir. Kablolu Ağlarda, Wireshark isimli uygulama bu yöntem için yaygın olarak kullanılır. Kablosuz Ağlarda, Cain&Abel gibi uygulamalarla bilgi elde edilir.*
- *Açıklık Yakalama: Mobil cihazlardan bilgi sızdırmada yapılan açıklık yakalama yöntemleri de kullanılmaktadır. Örneğin, bilinmeyen bir numaradan gelen kısa mesaj ile oltalama saldırısına maruz kalınabilir. Bu teknikle saldırgan sizden gizli bilgilerinizi toplayabilir.*

3.2 İş Parçacığı (Thread) Modeli

3 katmana ayrılır. Uygulama Katmanı, Haberleşme Katmanı, Kaynak Katmanı.

- *Uygulama Katmanı; Akıllı telefon ve tabletlerdeki tüm uygulamaları kapsar. Kötücül yazılım normal bir uygulama gibi davranır ve kullanıcının uygulama olarak indirmesini sağlar.*
- *Haberleşme Katmanı; Kötücül yazılım mobil cihaza bağlantı kanalları vasıtasıyla girer.*
- *Kaynak Katmanı; Mobil cihazın en önemli katmanıdır. Önemli bilgiler burada saklanır. Kötücül yazılım buradaki bilgileri kontrol ederek cihazı manipüle eder.*

4. GÜVENLİK ADIMLARI VE TESTLERİ

Mobil güvenlik testleri kötücül yazılımları bulmayı hedefler. Aşağıdaki durumlara odaklanır;

- Mobil uygulamanın güvenlik perspektifi
- Güvenlik riskleri
- Kötücül yazılımlar

Bu kısımda 7 tane önemli Mobil Güvenlik Testinden ve bir sistemi test etmeden önce yapılması gereken işlemlerden bahsedilmiştir.

4.1 Bilgi Toplama

3. kısımda bahsedilen adımlardan biridir. Bilgi toplamada, zararlı uygulamanın içeriği incelenir. Bu işlem iki aşamada gerçekleşir, Çevre Analizi, Mimari Analiz.

4.2 Çevre Analizi

- Uygulamayı geliştiren firma ve onun hakkındaki bilgiler tespit edilir.
- Uygulamanın işleyişi ve yapısı incelenir.
- Mimari Analiz.
- Uygulamanın kullandığı veri, "jailbreak/rooting" belirleme, arayüzlerle ilişkisi incelenir.
- Çalışma ortamı analizi yapılır.
- Veritabanı, güvenlik duvarı (firewall), uygulama servisleri incelenir.

4.3 Zafiyet Analizi

4.3.1 Adli Bilişim (Mobile Forensic)

Mobil cihazdaki veriyi inceleyerek değerlendirmeleri için kullanıcıya birçok imkan sunar. Kullandığı 2 araç vardır; "Micro Systemation's XRY" ve "Cellecrite UFED Touch Ultimate". Bu araçlar veri silinmiş olsa bile veriden mantıksal ve fiziksel çıkarımlar yaparlar. Mobil cihaz tam taramaya/incelemeye açıkken, veri ile ilgili sınırsız çıkarım yapılabilir. SMS/MMS, e-postalar, arama geçmişi gibi bilgiler çıkarım yapılabilir (Huang vd., 2015; Wang vd., 2015).

4.3.2 Statik Analiz

Uygulamayı çalıştırmadan uygulamanın analiz edilmesidir. Statik analiz uygulamanın kodunda bulunan zararlı yazılımları bulmak için kodu inceler. Uygulamak için kullanılabilecek araçlar, "Android Reverse Tools", "Static Android Analysis Framework". Ayrıca statik analiz geri derleme yaparak kodu analiz eder (Huang vd., 2015; Wang vd., 2015).

4.3.3 Dinamik Analiz

Uygulamayı çalıştırarak uygulamanın analiz edilmesidir. Ağ trafiğini göstererek kötü niyetli aktiviteleri ortaya çıkarmayı amaçlar. Dinamik Analiz programın işleyişine dayalı olduğundan geri derleme yapmaya gerek yoktur. Kötü niyetli yazılımlar gizlenemediği için statik analize göre daha iyi çalışır (Huang vd., 2015; Wang vd., 2015).

4.4 Fonksiyonel Testler

Geliştirilen uygulamanın kullanıcı ihtiyaçlarını ne derecede karşıladığı ölçülür. Arayüz ve uygulamanın genel durumundan yola çıkılarak kullanıcılar için kullanışlı olup olmadığını belirlemeye yardımcı testlerdir.

4.4.1 Birim Testi

Özel fonksiyonlar veya kod bileşenleri test edilir. Bu testin yapılabilmesi için program kodunun mimarisinin ayrıntılı bir şekilde bilinmesi gerekir

4.4.2 Regresyon Testi

Sistemde gerekli ve son değişiklikler yapıldıktan sonra gerçekleştirilen testlerdir. Bu sayede, daha önceki testlerde ortaya çıkan sorunların giderildiğinden ve yeni hatalar yapılmadığından emin olunur.

4.4.3 Sızma Testi

Sızma Testi "Penetrasyon Test" olarak da bilinir. Firmaların bilgi işlem sistemlerini oluşturan altyapıya ve uygulamalara bir saldırganın kullanacağı yöntemler kullanılarak saldırılır ardından müdahaleler sonucunda güvenlik açıkları tespit edilir, bu açıklar ile sistemlere sızılmaya çalışılır, bu açıkların nelere sebep olabileceği incelenir. İşlem bittiğinde sonuçları raporlanır. Mobil sızma testleri cihazın içeriğini düzgünce test etmek için çeşitli ayarlar bulundurur, test sonuçlarını inceler (Jadhav vd., 2015; Wang vd., 2015).

4.4.4 Laboratuvar Testi

Geliştirilen uygulamaların farklı operatörlerde ve farklı ağ bağlantılarında düzgün çalışıp çalışmadığı kontrol edilir. Genellikle ağ üzerinden yürütülürler ve ağın benzetimi yürütülür. Mobil uygulamaların; her koşulunda aynı tutarlılıkta ve hızda çalışması önemlidir (Eizmendi vd., 2010).

4.4.5 Performans Testi

Belirli koşullar altında uygulamanın cihazın performansına etkisini ve nasıl çalıştığını kontrol etmek için yapılan testtir. Bunlar düşük çekim gücü, düşük batarya, kısıtlı hafıza gibi. Hem kullanıcı, hem de geliştirici tarafından incelenerek değerlendirme yapılır (Kim vd., 2009).

4.4.6 Kesme Testi

Kullanılan mobil cihazın temel işlevlerinin baz alındığı ve uygulamanın çalışmaya ara verdiği süreç incelenir. Uygulama yeniden çalıştırıldığında uygulamanın işlevini yerine getirip getirmediği test edilir.

4.4.7 Kullanılabilirlik Testi

Geliştirilen uygulamanın amacına uygun olup olmadığını, kullanıcılar tarafından ne kadar tercih edildiğini belirlemek için yapılır. Aynı zamanda, uygulamanın ticari başarısının ölçülmesinde de önemli rol oynar. Sezgisel (Heuristic), değerlendirici (evaluation), bilişsel gözden geçirme (cognitive walkthrough) ve sesli-düşünme (thinking-aloud study) araştırmacıların kullandıkları bazı yöntemlerdir (Borys, 2015).

5. MOBİL UYGULAMA TESTLERİNDEKİ SORUNLAR

Akıllı telefonların güvenliğini sağlamak oldukça güçtür. Bazı durumlarda uygulamaları test etmek oldukça zordur, geliştirilmiş testlerin yetersiz olduğu durumlar da bulunmaktadır (Wang vd., 2015);

- İmza tabanlı kötücül yazılımlar kolaylıkla sistemi yanıltabilir.
- Adli Bilişim araçları güvenlik erişimi etkin olduğu zaman yeterli değildir.
- Sızma Test, araçları mobil cihazlar için daha çok geliştirilmelidir.
- Statik Analiz koda ulaşamadığı için yeterince verimli çalışmaz ayrıca birçok manuel işlem gerektirir.
- Dinamik Analiz cihazın tüm kaynaklarında işlem gerçekleştirir ve bu durum zaman kaybına sebep olur.
- İndirilen uygulama kötücül yazılımı gizliyor olabilir.

6. GÜVENLİK İÇİN GELİŞTİRİLMİŞ YAZILIMLAR

6.1 Open Web Application Security Project-OWASP

OWASP, Açık web uygulama güvenliği projesi anlamındadır. Güvensiz yazılımların oluşturduğu problemleri gidermek için kurulmuş bir topluluktur. Tüm araçları, listeleri, dokümanları ve bölümleri ücretsizdir.

6.2 Odin

Android telefonlar için geliştirilmiş bir uygulamadır. İşletim sisteminin cep telefonlarına indirilmesini sağlar. Android için inceleme kısmında detaylarından bahsedilmiştir.

6.3 ITUNES

Itunes, Apple'ın geliştirdiği bir uygulamadır. Program hem Mac hem de Windows işletim sistemlerinde kullanılabilir. Bunun dışında iOS jailbreaking için de kullanılır. Çünkü Jailbreak yazılımı Itunes ile birlikte çalışır.

6.4 Jailbreak Araçları

iOS işletim sistemlerinde kullanılan başlıca Jailbreak araçları evasi0n, redsn0w, Pangu, Absinthe, greenpois0n, PwnageTool, sn0wbreeze vb. olarak bilinmektedir. Bununla ilgili detaylı bilgi 7. bölümde verilmiş olup resmi işletim sistemlerinin kullanılmaması büyük güvenlik zafiyetleri doğurmaktadır.

6.5 Burp Suit

Sızma testlerinde sıklıkla kullanılan bir vekil (proxy) uygulamasıdır. Varsayılan olarak gelen eklentileri ve harici eklentileri yardımı ile web uygulama güvenliği alanında çok kullanılan bir araç haline gelmiştir.

7. MOBİL İŞLETİM SİSTEMLERİNDE GÜVENLİĞİ KIRMA

7.1 iOS - Jailbreak

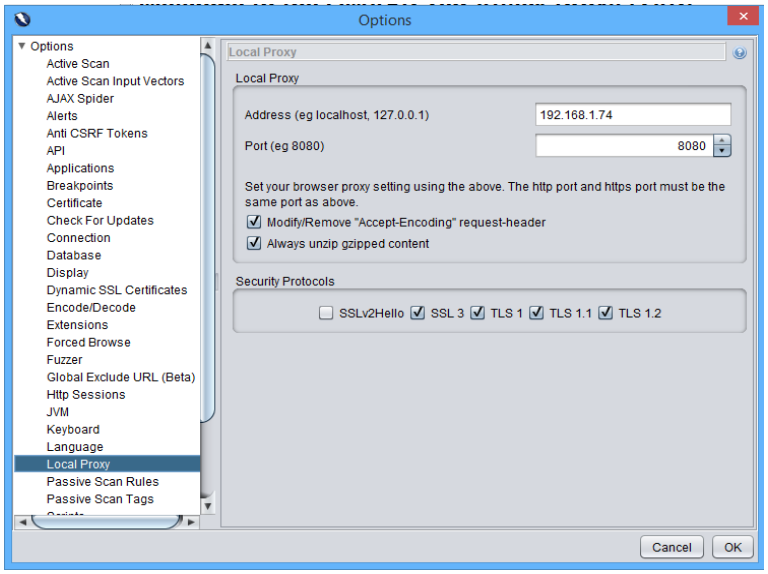
Apple bir cihazınızın resmi güvenlik mekanizmalarını devre dışı bırakmak olarak açıklanabilir. Jailbreak yaparak cihazın sistem dosyalarına sızan saldırganlar, telefona istediği müdahaleyi yapabilme imkanına erişir. Örneğin uygulama mağazasında bulunmayan, içeriği kötü amaçla değiştirilmiş uygulamaların mobil cihazlara kurulumlarının yapılması en bilinen yöntemlerdendir. Bunların yanı sıra, Jailbreak işlemi ile ücretli uygulamalar cihaza ücretsiz olarak yüklenebildiği için lisans bedellerinin ücretlendirilememesi yolu ile suç işlenmektedir. Geliştiriciler tarafından desteklenmediği için Apple Jailbreak yapılmış cihazlarda güvenlik açığı bulunduğunu belirtmiştir. Ayrıca Cydia gibi yerlerden indirilen uygulamalar telefona zarar verebilir. Güvenliği garanti edilmemiş uygulamalar, batarya ömrü gibi önemli parçaları etkileyebilir (Ma vd., 2014).

7.2 Android – Rooting

Android cihazlarda, kullanıcılar cihaz üzerinde tüm yetkiye sahip değillerdir. "Fabrika Ayarları" kısmında bazı özellikler kapatılmıştır. Root erişimi sayesinde kullanıcı cihaz üzerinde tam yetkiye sahip olur. Root sayesinde kullanıcı telefon üzerinde; tam yedekleme yapabilir, reklamları engelleyebilir, işletim sistemini düzenleyebilir. Root yapılmış telefon garanti kapsamından çıkar. Ayrıca telefonun bazı fonksiyonel özelliklerini kaybetmesine sebep olabilir. Bir diğer risk ise güvenlik ile ilgili riskler oldukça artar. SuperOneClick, Unlock Root, Z4Root ve UniversalAndRoot Root için geliştirilmiş araçlardır (Ma vd., 2014).

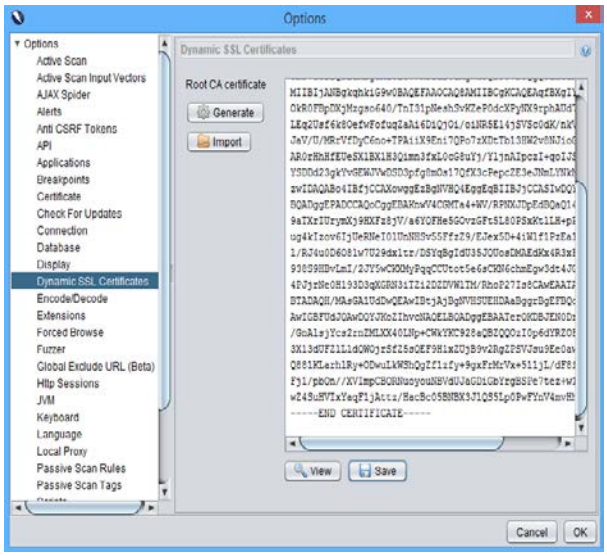
8. UYGULAMA

Uygulama için "Owasp Penetration Test" programı kullanılmıştır. Uygulamanın adım adım gerçeklenmesi aşağıda gösterilmektedir.



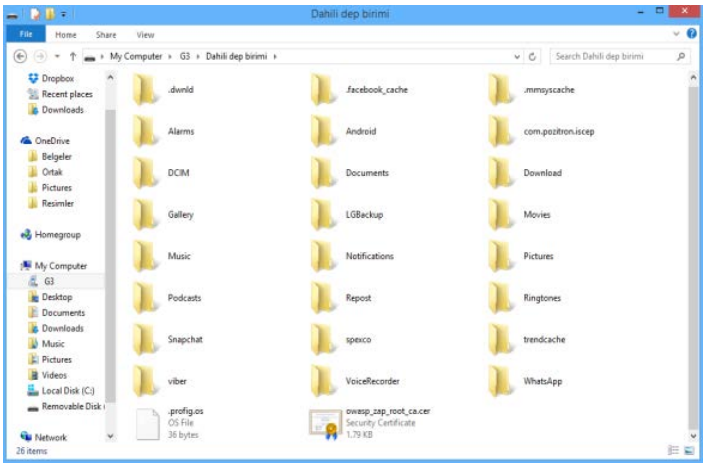
Şekil 1. Owasp Local Proxy

Şekil1'de görüldüğü gibi öncelikle programın "Local Proxy" ayarı yapılmıştır. Bunun sebebi saldırılacak olan cihaz ile aynı ağda olabilmektir.



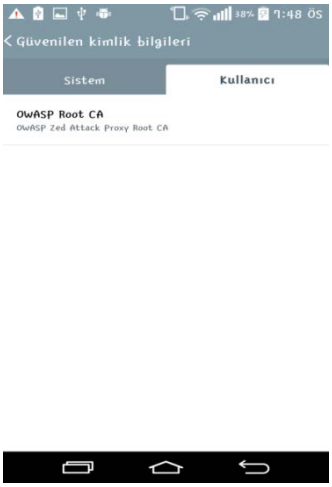
Şekil 2. SSL Sertifikası

Ardından cihaza konulmak üzere Şekil2'deki gibi SSL sertifikası oluşturulmuştur. Bir sonraki adım olarak bu sertifika cihazın içine Şekil3'deki gibi yerleştirilmiştir.

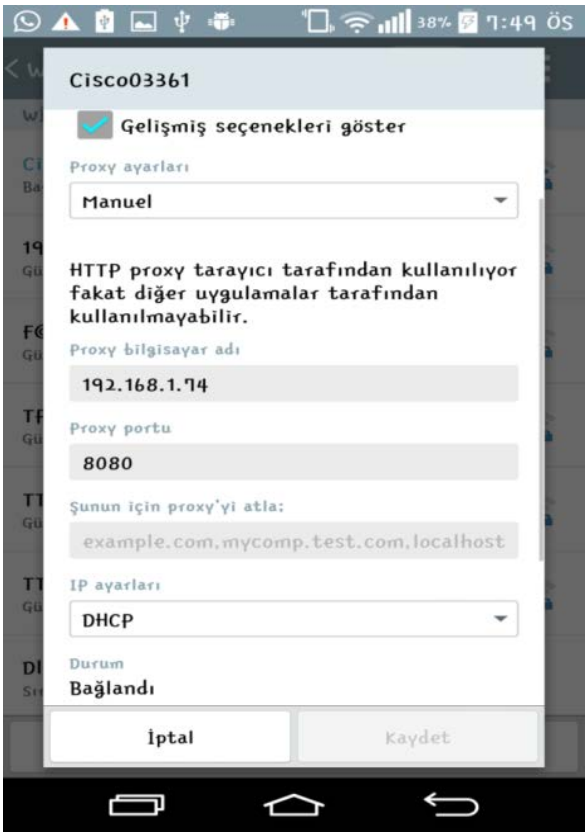


Şekil 3. Sertifika Yerleştirme

Sertifika cihaza konulduktan sonra gerçekten cihazın tanıyıp tanımadığı Şekil4'deki gibi kontrol edilmiştir. Sertifikanın cihazda olduğu kesinleştikten sonra ise cihazın "Proxy-Ağ Ayarları" Şekil5'deki gibi gerçekleştirilmiştir.

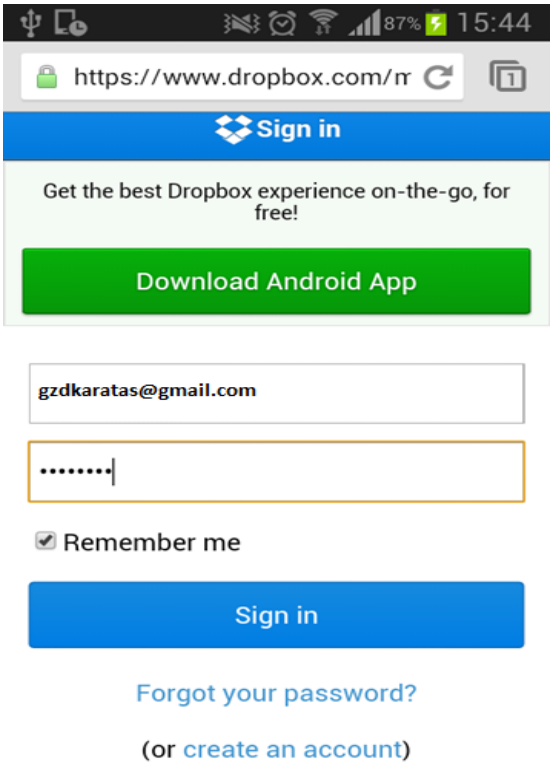


Şekil 4. Sertifika

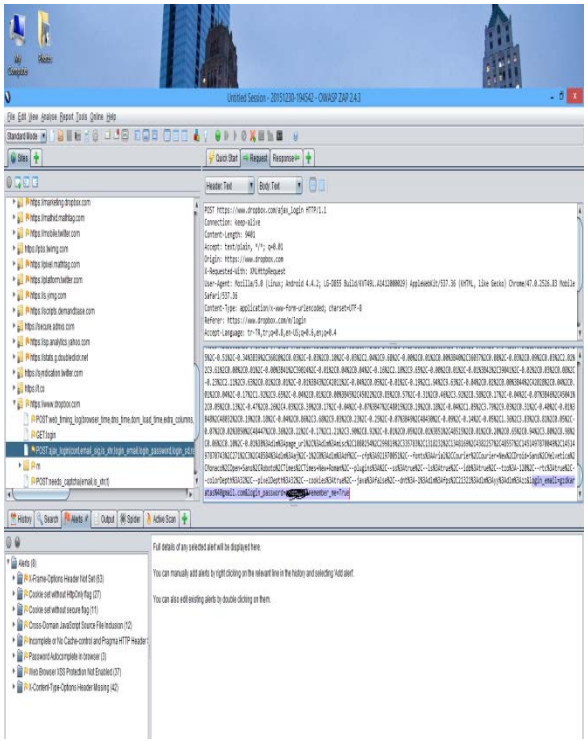


Şekil 5. Proxy Ayarı

Son adım olarak kullanıcının "kullanıcı adı" ve "şifresi" bir site için ele geçirilmeye Şekil 6'daki gibi çalışılmıştır ve Şekil 7'de gösterilen şekilde bu bilgilere ulaşılmıştır.



Şekil 6. DropBox Uygulama



Şekil 7. Bilgilere Ulaşma

9. SONUÇ

Mobil cihazlardaki gelişmeler ve bu cihazların kullanımının gittikçe yaygınlaşması, kullanıcıların yapacağı işleri mobil ortamlara yönlendirmektedir. Mobil ortamlarda bilgi güvenliğini sağlayabilmek için her gün yeni yöntemler ve yeni yaklaşımlar geliştirilmektedir. Bu doğrultuda birçok kurumda sadece mobil cihazların güvenliğine yönelik çalışmalar yapacak birimler istihdam edilmektedir. Bu gelişmeler ile birlikte özellikle kurumların mobil cihazlarda meydana gelecek tehditlerin farkında olarak gerekli önlemleri almaları, kullanıcılarını da bu konuda bilgilendirmeleri gerekmektedir. "Mobil Cihazlarda Güvenlik Raporu" incelendiğinde son yıllarda mobil cihaz üreticileri giderek artan ve özellikle kötücül yazılımlar ile yapılan saldırılarla karşılaşmakta ve bu saldırılardan kurtulabilmek için daha fazla para harcamaktadırlar (Sağıroğlu vd., 2009).

Bu çalışmada Mobil Cihazlarda güvenlik üzerine araştırmalar derlenmiştir. Mobil cihazlarda kullanılan işletim sistemleri, geliştirilen uygulama türleri hakkında bilgi verilerek çalışmasının asıl amacı olan güvenlik hakkında detaylı bilgi verilmesi amaçlanmıştır. Bu doğrultuda mobil cihazlara yapılan saldırılar özetlenmiş, geliştirme esnasında yapılan hatalar vurgulanmış ve alınabilecek güvenlik önlemlerinden bahsedilmiştir. Sonra olarak günümüzde yaygın olarak kullanılan ve mobil cihazların güvenliğini test etmek için kullanılan yazılımlar ve örnek bir uygulama yapılmıştır.

Mobil cihazlarda düzenli olarak sistem günlükleri tutulmalı ve üretici firmaya aksama durumlarına karşı bilgi iletilmesi sağlanmalıdır. Mobil cihazlar hazır antivirüs programlı üretilmeli (işletim sistemine gömülü olarak) ve bu programların güncel tutulması sağlanmalıdır. Ayrıca cihazlar güvenlik duvarı barındırmalı ve bu duvar sürekli etkin tutulmalıdır.

Cihaza indirilen tüm uygulamalar önce antivirüs programından geçirilmeli ardından uygun ise kullanımına izin verilmelidir. Mobil cihazlar için yüksek önem teşkil eden şifreler kolay tahmin edilebilir ve herkes tarafından tercih edilen şifrelerden olmamalıdır. Cihazların içerisinde önemli bilgiler muhafaza edilmemelidir. Eğer saklanacak ise şifrelenmiş olarak tutulmalıdır.

Mobil cihazlarda bulunan ağ trafiği filtrelenmelidir. Veriler belirli aralıklarla yedeklenmelidir. Kullanıcının genel kullanımının aksine cihazda şüpheli bir kullanım olup olmadığı belirlenebilmeli, tehlikeli bir durum sezildiğinde kullanıcı bilgilendirilmelidir. Kötü niyetli SMS/MMS mesajları filtrelenecek şekilde geliştirme yapılmalı ve ilgili yazılımlar kullanılmalıdır. Kullanıcılar cihaz koruması konusunda bilgilendirilmesi gerekiyorsa bu konuda eğitim almaya yönlendirilmelidir. Alınan ve gönderilen veriler şifreli olarak iletilmesi yavaşlamaya sebep olmakla birlikte, kişisel güvenliği önemli ölçüde arttıracaktır.

KAYNAKLAR

Adinata, M., Liem, I., (2014). "A/B test tools of native mobile application," Proc. 2014 Int. Conf. Data Softw. Eng. ICODSE 2014.

Ahmad, M. S., Musa, N. E., Nadarajah, R., Hassan, R., & Othman, N. E. (2013). 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.

Bere, A., (2013) "Toward assessing the impact of mobile security issues in pedagogical delivery: A mobile learning case study," Sci. Inf. Conf. (SAI), 2013, pp. 363–368.

Borys, M., (2015). "Mobile Application Usability Testing in Quasi-Real Conditions," pp. 381–387.

Bosnic, S., Papp, I., & Novak, S. (2016). The development of hybrid mobile applications with Apache Cordova. In Telecommunications Forum (TELFOR), 2016 24th (pp. 1-4). IEEE.

Chaffey, D. (2016) "Mobile Marketing Statistics Compilation" Erişim Tarihi: 24.06.2016
Kaynak: http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/

Eizmendi, I., Velez, M., Prieto, G., Correia, S., Arrinda, A., Angueira, P., (2010) "Laboratory Tests for testing DVB-T2 mobile performance," Evaluation, pp. 1–5.

Fan, X., & Wong, K. (2016). Migrating user interfaces in native mobile applications: android to iOS. In Proceedings of the International Workshop on Mobile Software Engineering and Systems (pp. 210-213). ACM.

Guerid, H., Serhrouchni, A., Achemlal, M., Mittig, K., (2011). "A Novel Traceback Approach for Direct and Reflected ICMP Attacks," 2011 Conf. Netw. Inf. Syst. Secur., pp. 1–5.

Huang, K., Zhang, J., Tan, W., Feng, Z., (2015). "An Empirical Analysis of Contemporary Android Mobile Vulnerability Market," 2015 IEEE Int. Conf. Mob. Serv., pp. 182–189.

Jadhav, S., Oh, T., Kim, Y.H., Kim, J.N., (2015). "Mobile device penetration testing framework and platform for the mobile device security course," 2015 17th Int. Conf. Adv. Commun. Technol., pp. 675–680.

Ju, H., Kim, Y., Jeon, Y., & Kim, J. (2015). Implementation of a hardware security chip for mobile devices. IEEE Transactions on Consumer Electronics, 61(4), 500-506.

Kikuchi, H., Sasa, K., & Shimizu, Y. (2016). Interactive History Sniffing Attack with Amida Lottery. In Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2016 10th International Conference on (pp. 599-602). IEEE.

Kim, H., Choi, B., Wong, W.E., (2009). "Performance testing of mobile applications at the unit test level," SSIRI 2009 - 3rd IEEE Int. Conf. Secur. Softw. Integr. Reliab. Improv., pp. 171–180.

Küçüksille, E., Özger, F., & Genç, S. (2013). Mobil bulut bilişim ve geleceği. Akademik Bilişim Konferansı Bildirileri, 23-25.

Liyanage, M., Abro, A. B., Ylianttila, M., & Gurtov, A. (2016). Opportunities and challenges of software-defined mobile networks in network security. IEEE Security & Privacy, 14(4), 34-44.

Lu, X., Luo, Y., Liu, X., (2014). "A Graph-Based Approach to Assisting Creation of Mobile Web Applications," 2014 IEEE Int. Conf. Web Serv., pp. 728–729, 2014.

Lu, H. L. H., Gheitanchi, S., Young, R., Chatwin, C., (2010). "A symbian based mobile user authorization system using mobile networks," Wirel. Adv. (WiAD), 2010 6th Conf.

Ma, H.J., Li, M., Wang, K., Dou, Z., Jiang, H., (2014). "NTP network timing technique research for Android and iOS mobile platform," 2014 IEEE Int. Freq. Control Symp., vol. 3, pp. 1–4.

Masruroh, S. U., & Saputra, I. (2016, April). Performance evaluation of instant messenger in Android operating system and iPhone operating system. In Cyber and IT Service Management, International Conference on (pp. 1-6). IEEE.

Mohamed, M., Shrestha, B., & Saxena, N. (2016). SMASheD: Sniffing and Manipulating Android Sensor Data for Offensive Purposes. IEEE Transactions on Information Forensics and Security.

Omeleze, S., Venter, H. S., (2013). "Testing the harmonised digital forensic investigation process model-using an Android mobile phone," 2013 Inf. Secur. South Africa - Proc. ISSA 2013 Conf.

Penning, N., Hoffman, M., Nikolai, J., Wang, Y., (2014). "Mobile Malware Security Challenges and Cloud-Based Detection," 2014 Int. Conf. Collab. Technolgies Syst., pp. 181–188.

Pooryousef, S., & Amini, M. (2016). Fine-grained access control for hybrid mobile applications in Android using restricted paths. In Information Security and Cryptology (ISCISC), 2016 13th International Iranian Society of Cryptology Conference on (pp. 85-90). IEEE.

Sağıroğlu, Ş., Bulut, H. (2009). Mobil ortamlarda bilgi ve haberleşme güvenliği üzerine bir inceleme. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 24(3).

Setiabudi, D. H., Tjahyana, L. J., (2013). "Mobile learning application based on hybrid mobile application technology running on Android smartphone and Blackberry," Int. Conf. ICT Smart Soc., pp. 1–5.

Sun, J.Z, Howie, D., Koivisto, A., Sauvola, J., (2001). "A hierarchical framework model of mobile security," 12th IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. PIMRC 2001. Proc. (Cat. No.01TH8598), vol. 1, pp. 56–60, 2001.

Tilson, D., Sorensen, C., Lyytinen, K., (2011). "Change and control paradoxes in mobile infrastructure innovation: The Android and iOS mobile operating systems cases," Proc. Annu. Hawaii Int. Conf. Syst. Sci., pp. 1324–1333.

Wang, Y., Alshboul, Y., (2015). "Mobile security testing approaches and challenges," 2015 First Conf. Mob. Secur. Serv., pp. 1–5.

Wang, Y., Wei, J., Vangury, K., (2014). "Bring your own device security issues and challenges," 2014 IEEE 11th Consum. Commun. Netw. Conf., pp. 80–85.

Zhou, Y., Jiang, X., (2012). "Dissecting Android Malware: Characterization and Evolution," 2012 IEEE Symp. Secur. Priv., no. 4, pp. 95–109.