Android Adli Bilişim:

Bir Mobil Cihazdan Otomatik Veri Toplama ve Raporlama (DroidWatch)

Justin Grover a,b,*
a The MITRE Corporation, 7515 Colshire Dr., McLean, VA, United States
b Rochester Institute of Technology, 1 Lomb Memorial Dr., Rochester, NY, United States

Çeviri: Özgür Koca, ensei@tankado.com

ÖZET

Bu araştırmada, olaya müdahale eden, güvenlik denetçilerini, proaktif güvenlik izleyicilerini ve adli araştırmacıları ilgilendiren birçok veri setini sürekli olarak toplamak üzere Android akıllı telefonlar için kurumsal bir prototip izleme sistemi geliştirilmiştir. Kapsanan birçok veri seti, mevcut diğer kurumsal izleme araçlarında bulunamadı. Prototip sistemi ne kök ayrıcalıklarını ne de doğru işlem için Android mimarisinin çözümlemesini gerektirmez, böylece Android cihazları arasındaki birlikte çalışabilirliği artırır ve sistem için casus yazılım sınıflandırmasını önler. Kurcalamaya karşı savunmasız alanları belirlemek ve daha da güçlendirmek için sistemde bir anti-adli analiz yapıldı. Bu araştırmanın katkıları, türünün ilk açık kaynaklı Android kurumsal izleme çözümü, yükseltilmiş ayrıcalıklar olmadan koleksiyon amaçlı kullanılabilecek veri setlerinin kapsamlı bir rehberinin ve çeşitli Android uygulama bileşenlerini sahada uygulamak için yararlı yeni bir tasarım stratejisinin kullanıma sunulmasını içermektedir.

Sunuş

Birleşik Devletlerde (ABD), nüfusun üçte birinin 2012 yılı Ekim ayı itibarıyla akıllı telefonu olduğu görülmektedir (comScore, 2012; ABD Sayım Bürosu, 2010). Akıllı telefon pazarındaki en büyük oyuncular arasında Google, Apple, Research In Motion (RIM) ve Microsoft yer alıyordu. RIM, %7.8'lik düşüşünü sürdürürken, Google'ın Android platformu pazarın % 53.6'sına kadar önemli kazançlar gösterdi (comScore, 2012). Akıllı telefon pazarında Google'ın yaygınlığı arttıkça, kuruluşların mevcut mobil seçeneklerinden Android'e geçmeleri yönündeki baskı da artacak. Bu kuruluşlar arasında, bazıları RIM'den yeni akıllı telefon sistemlerine geçmeyi düşünen ABD hükümet ajansları bulunmaktadır (Marks, 2012; Rauf, 2012). Bazı kuruluşlar, kişisel cihazlarınızı (Android akıllı telefonlar da dahil olmak üzere) kendi cihazınızı getir (BYOD) politikaları ile (Citrix, 2011) kurumsal ağlarda kişisel cihazları kullanma kabiliyetine ulaşmaya başlamıştır. BYOD'un 2017 yılına kadar 181.39 milyar $ 'lık bir sektör oluşturması bekleniyor (MarketsandMarkets, 2012).

Hükümet ve endüstrideki mobil cihaz eğilimleri göz önüne alındığında, bir işletmede akıllı telefonu güvence altına alma sorunu ortaya çıktı. Çoğu satıcı öncelikle işletmeler için değil, telefonlarını kişisel bir cihaz olarak kullanacak olan tüketiciler için akıllı telefonlar tasarlar. RIM kurumsal müşterilerin cihaz yönetimi için bir BlackBerry Kurumsal Sunucu dağıtabilmesinden dolayı istisnadır. RIM'in aksine, Android cihaz satıcıları dahili mobil cihaz yönetimi (MDM) sistemleri ile birlikte gönderilmemektedir. Üçüncü taraf MDM, akıllı telefon endüstrisinin bıraktığı güvenlik boşluklarına hitap eden hızla gelişen bir satış sektörüdür. Önümüzdeki beş yıl içerisinde, tüm işletmelerin %65'inin bir MDM sistemi oluşturması bekleniyor (Pettey, 2012). BYOD, bir kuruluşta güvenilmeyen cihazlara izin verilmesi ile ilgili doğasında olan riskler nedeniyle MDM sistemlerine olan ihtiyacı artırır; Kuruluşlar, BYOD risklerini azaltmak için mobil cihaz güvenlik politikalarının sıkı bir şekilde uygulanmasına ihtiyaç duymaktadır.

Birkaç lider MDM ürünü üzerine yapılan araştırma, kurumsal düzeyde Android cihazlardan otomatik olarak adli veri koleksiyonları elde etmede genel bir özellik eksikliği ortaya çıkardı. Bu verilerin bulunması, olayların yanıtı, güvenlik denetimi, proaktif güvenlik izleme ve adli soruşturmalar da dahil olmak üzere kuruluşlar arasında bulunan ortak güvenlik uygulamalarına yardımcı olacaktır. 2010/2011 Bilgisayar Güvenlik Enstitüsü Bilgisayar Suçları ve Güvenliği Anketi'ne göre, çeşitli şirketlerden gelenlerin %61.5'i iç denetimlerin bir güvenlik mekanizması olarak kuruluşlarında yapıldığını bildirdi. Buna ek olarak,%44 veri-kayıp önleme ve kullanıcı içerikli izleme programlarının bulunduğunu bildirmiştir (Richardson, 2010). Bu istatistikler, birçok organizasyonun içeriden öğrenebilecekleri tehditlerle ilgili kurumsal risklerin farkında olduğunu ve bunları hafifletmek için gerekli önlemleri aldıklarını göstermektedir; Ancak, Android akıllı telefonu izlemek için teknoloji eksikliği göz önüne alındığında, bu cihazlarda gerçekleştirilen birçok işlem denetlenmemektedir. İzleme seçeneklerinin olmaması, bu verilerin iç soruşturmalarda yaratacağı önemli etkiyle birlikte, bu makalenin konusu olan DroidWatch adlı bir prototip çözüm önerisi ve geliştirilmesine yol açtı.

Bu makale, politika ihlalleri, fikri mülkiyet hırsızlığı, yanlış kullanım, zimmete para geçirme, sabotaj ve casusluk da dahil olmak üzere iç soruşturmalar için kullanışlı verilerin toplanmasını otomatikleştiren bir Android uygulamasının ("uygulaması") tasarlanması ve uygulanması üzerine odaklanmaktadır. Veriler, Gingerbread 2.3.6 çalıştıran bir Samsung Galaxy S II Epic 4G Dokunmatik Android akıllı telefonundan toplandı. Ardından PHP, MySQL, Apache ve Splunk çalıştıran uzak bir Ubuntu sunucusuna gönderildi. Anti-virüs, kök algılama ve uygulamanın sonlandırılmasına veya kaldırılmasına karşı

korunma gibi özellikler, sistem ve kurumsal güvenlik için gereklidir, ancak bu araştırmanın kapsamı dışındadır. Uygulanan çalışma ile toplanan tüm veriler, kurumsal veya resmi ağlarda yaygın olanlara benzer bir kullanıcı onayı vasıtasıyla gerçekleşir. Veriler, köklü ayrıcalıklar veya Android mimarisinin kullanılmasıyla elde edilemez.

Bu yazının geri kalan kısmı aşağıdaki şekilde düzenlenmiştir. Bölüm 2, Android'in geliştirilmesi, güvenliği ve gizliliği ile ilgili arka plan konularını anlatıyor. İlgili çalışma Bölüm 3'te, ardından Bölüm 4'te DroidWatch'ın tasarım ve uygulama ayrıntıları bulunur. Gelecekteki çalışma ve sonuç sırasıyla Bölüm 5 ve 6'da sunulmuştur.

2. Ön Çalışma

Aşağıdaki alt bölümlerde temel uygulama geliştirme terminolojisi (Kısım 2.1), Android uygulama güvenlik modeli (Kısım 2.2), bir cihazın köklendirilmesi (Kısım 2.3), güncel araştırmalarda mobil cihazların kullanımı (Kısım 2.4) ve gizlilik kaygısı ele alınmıştır. (Kısım 2.5).

2.1. Android Uygulama Geliştirme Terminolojisi

Android uygulama bileşenleri, bir uygulamanın davranışını tanımlamaya yardımcı olan Android çerçeve bloklarından oluşur (framework blocks) (Google. (N.d.). Uygulama temelleri). DroidWatch içinde şu uygulama bileşenleri kullanılmaktadır: etkinlikler, hizmetler, içerik sağlayıcıları, yayın alıcıları, içerik gözlemcileri ve alarmlar. Aşağıda açıklanan her bileşen, farklı ve kullanışlı bir amaca hizmet eder.

Etkinlikler (Activities), bir kullanıcı arabirimini uygulayan bağımsız ekranlardır. Bilgi görüntüler, kullanıcı etkileşimini ister ve diğer etkinlikleri başlatırlar (Google. (N.d.). Uygulama temelleri). DroidWatch'da etkinlikler nadiren kullanılır; Genel kullanıcı deneyimini etkilememek için, çalışmaların çoğu arka planda gerçekleşir.

Hizmetler (Service), kullanıcı etkileşimi gerektirmeyen uzun süre devam eden işlemlerdir. Etkinlikler gibi diğer uygulama bileşenleri, diğer uygulamalar ve hizmetler çalışırken bile hizmet başlatabilir ve devam ettirebilir (Google. (N.d.) Uygulama temel bilgileri). DroidWatch, veri koleksiyonlarını ve aktarımları gerçekleştirmek için sürekli olarak bir servis kullanır..

İçerik sağlayıcıları (Content Providers), uygulama verisinin erişimini ve paylaşımını yöneten uygulama bileşenidir. Ön tanımlı tekil kaynak tanımlayıcıları (URI) aracılığıyla içerik sağlayıcılarıyla arabirimlenerek kullanılır (Google. (N.d.). Uygulama temelleri). DroidWatch içerik sağlayıcıları iki şekilde kullanır:

1. Diğer uygulamalar içinde saklanan verileri okurken
2. DroidWatch uygulaması içinde depolanan verileri okuyup yazar iken

Yayın alıcıları (Broadcast Receiver), bir Android cihazdaki yayın sistemi olaylarını işleyen ve bunlara yanıt veren uygulama bileşenleri (Google. (N.d.). Uygulama temelleri) 'dir. Gelen Kısa Mesaj Servisi (SMS) mesajları ve uygulama yüklemesi gibi olayları tespit etmek için DroidWatch da kullanılırlar.

İçerik gözlemcileri (Content Observers), içerik sağlayıcılarla ilişkili olduğunda, hedeflenen bir veritabanı altında yatan veri kümesinin içeriği değiştiğinde bildirim alırlar (Google. (N.d.) ContentObserver). DroidWatch bunu verilerin gerçek zamanlı değişikliklerini algılamak için kullanır.

Alarmlar (Alarms), periyodik olarak içerik sağlayıcıları sorgulamak ve yeni veriler çekmek için DroidWatch'ta yapılandırılan, cron işlerine (cronjobs) benzer şekilde zamanlanmış işlemlerdir. Güvenilirdir ve yalnızca belirlenen zamanlarda çalışırlar.

2.2. Android Uygulama Güvenliği

Google'ın Android uygulamaları güvenlik modeli, bir uygulamanın AndroidManifest.xml dosyasında (daha sonra "AndroidManifest" olarak anılacaktır) izin beyanını içerir. Varsayılan olarak, istenen izinlere sahip olmayan bir uygulama, "diğer uygulamaları, işletim sistemini veya kullanıcıyı olumsuz yönde etkileyecek her hangi bir işlemi gerçekleştiremez" (Google. (N.d.) İzinler). Bu, bir uygulamanın diğer uygulamaların özel verilerine erişememesi, şebeke servislerini kullanamaması, dahili / harici hafızaya yazamaması veya diğer temel işlevleri yerine getirememesi anlamına gelir. Yeni indirilen bir uygulama, yüklenmeden önce kabul edilmiş olması için kullanıcıya bildirilen izinlerini sunmalıdır. Bu durum Android 5 ile değişmiştir. Yeni güvenlik modeline göre önemli (tehlikeli kategorideki) izinlerin çoğu uygulama ilgili izini gerektiren bir işlem yaptığı sırada talep edilir. Böylece işletim sistemi çalışma zamanında kullanıcıdan ilgili işlem için izin vermesini ister.

2.3. Kökleme (Rooting)

Köklendirme, kullanıcıların normal kullanıcı kipi altında normalden daha yüksek ayrıcalıklı işlevler gerçekleştirmesine olanak tanır. Yasal veya gayri meşru amaçlar için kullanılabilir. Kullanıcılar, güvenlik kısıtlamalarını atlamak veya DroidWatch gibi bir uygulama aracılığıyla toplanan verilere müdahale etmek isteyebilir. Kök erişimi meşru olarak da kullanılabilir.(J. Grover / Digital Investigation 10 (2013) S12-S20 S13 adli araştırmacılar tarafından bir cihazdan veri çıkarılması) Ancak, mümkün olduğunca bundan kaçınılmalıdır. Süreç tipik olarak belirli bir aygıtta veya işletim sisteminde bir güvenlik açığını kullanır ve daha fazla güvenlik açıklarına neden olabilir. Köklendirme, bir cihazın bölümlerini de değiştirir (adli bilişim uygulamalarıyla çelişen bir eylem); Bununla birlikte, gerekli koşulların ve verilerin türüne bağlı olarak köklenme kaçınılmaz olabilir (Vidas ve diğerleri, 2011). Kök erişimi, DroidWatch gibi bir uygulamanın özellik sayısını artırabilir; bunun sonucu olarak sistemin güvenliğini zayıflatabilir, birlikte çalışabilirliği düşürebilir ve akıllı telefon sağlayıcının garantisini tehlikeye sokabilir.

2.4. Akıllı telefon araştırmaları

Suçları araştırmaya ve hassas hükümet bilgilerini yetkisiz erişimden korumak için yetkilendirilmiş mobil güvenlikte birincil oyuncular kolluk kuvvetleri ve devlet kurumlarıdır. Şirketler ayrıca ticari casusluk, finansal hırsızlık ve fikri mülkiyet hırsızlığına karşı kendilerini korumak için mobil güvenlikle çok ilgilidirler. Boşanma kararları, velayet savaşları, emlak anlaşmazlıkları vb. alanlardaki özel menfaatler de bu alandaki ilerlemelerden kazançlı çıkmaktadır (Hoog, 2011). Sonuç olarak, akıllı telefonların izlenmesinden menfaat sağlayacak soruşturma türleri, kanun uygulama soruşturmaları, iç soruşturmalar ve özel soruşturmalardır. Bu araştırma, potansiyel politika ihlallerini, fikri mülkiyet hırsızlığını, kötüye kullanım, zimmete para geçirme, sabotaj, casusluk ve diğer soruşturmaları araştırmak için bir organizasyonda sözleşmeli veya başka bir şekilde (örneğin, adli olay inceleyicileri, güvenlik denetçileri vb.) personel tarafından gerçekleştirilen dahili soruşturmalar üzerine yoğunlaşmaktadır. Dahili araştırmacıların kolluk soruşturmalarının sıkı adli muamele ve koruma prosedürlerine uymaları gerekmez, ancak genellikle yaygın olarak uygulanan adli bilişim tekniklerine ve kurallarına uymaya çalışılmalıdır. Dahili araştırmalar için değerli akıllı telefon verileri elde etmek için, geleneksel olarak bir cihaza fiziksel olarak erişmek gereklidir. Buna bir istisna olan EnCase Enterprise, Ekim 2012 tarihinden itibaren bir ağ üzerinden Android cihazların uzaktan adli görüntülerini çıkarabilimektedir. Bazı MDM'ler ayrıca sınırlı izleme yapabilir (belirli ürünler Bölüm 3.1'de ele alınmıştır), ancak araştırmacıların ihtiyaçlarını etkin bir şekilde ele alacak kadar yeterli değildir. Bir

mobil cihazın fiziksel olarak alındığı varsayılarak, araştırmacılar, cihazın mevcut durumunun mantıksal veya fiziksel anlık görüntüsünü almak için çeşitli araçlar kullanabilirler. Andrew Hoog, (Hoog, 2011), Android akıllı telefonlardan bilgi toplamak için mevcut araçların çoğunu listeliyor. Cihazların bazıları taşınabilir donanım aygıtları ve diğerleri yazılım ürünleridir; Bununla birlikte, hepsi evrensel bir seri veri yolu (USB) bağlantısı üzerinden çalışır ve çalışması için akıllı telefona fiziksel erişim gerektirir. Buna ek olarak, araçların birçoğu kök erişim gerektirir (Valle, 2013).

2.5. Gizlilik endişeleri

DroidWatch, kullanıcıları gizlilik beklentileri hakkında bilgilendirmek ve onaylarını almak için bir telefonun önyükleme işlemi sırasında bir kullanıcı onayı bayrağı görüntüler (izin kartı afişinin uygulanmasına ilişkin daha fazla ayrıntı Bölüm 4.1.2'de bulunur). Bu, uygulamanın bir casus yazılım sınıflandırmasını önlemesine yardımcı olur ve sistem hatalarını engelleyebilir. Tablo 1'de, geçerli bazı mobil cihaz gizlilik davaları listelenmiştir. Kullanıcıları DroidWatch'ta izleme politikaları hakkında bilgilendirmek için istenen izinlerin kabul edilebilir kullanımı, ABD v. Ziegler'de (ABD Temyiz Mahkemesi, 2007) karar veren ABD Temyiz Mahkemesinden alınabilir. Potansiyel BYOD etkileri ile ilgili argümanlar, ABD Büyük Anayasa Mahkemesi davası Ontario v. Quon kararından (ABD Yüksek Mahkemesi, 2010) alınarak yapılabilir.

Sonuç olarak, bir organizasyon, DroidWatch gibi izleme uygulamalarını, şahsen sahip olunanlar da dahil olmak üzere tüm kurumsal akıllı telefonlara kurma hakkına sahip olduğunu düşünebilir; çünkü telefonlar özel olarak kontrol edilen ağında çalışırlar. Carrier IQ davası, bu yazının yazıldığı tarih itibariyle halen beklemede olmasına rağmen, kullanıcı verilerinin kullanıcı onayı olmadan akıllı telefonda izlenmesinden kaynaklanabilecek yasal sorunlara örnek teşkil etmektedir (Davis, 2012).

3. İlgili Çalışmalar

Aşağıdaki alt bölümlerde, bu araştırmayı tamamlayan veya başka şekilde etkileyen çeşitli araştırmalar tartışılmıştır. Ticari ürünler ve akademik çabalar sırasıyla Bölüm 3.1 ve 3.2'de tartışılmaktadır.

3.1. Ticari ürünler

Üçüncü taraf MDM ürünleri mobil cihazlarla bir şirketin genel güvenliğini artırır; Bununla birlikte, çoğu MDM'de derinlemesine kullanıcı izleme özellikleri yoktur. **Zenprise**, **AirWatch** ve **MobileIron** gibi bazı önde gelen MDM seçenekleri, sınırlı izleme yetenekleri (ör., GPS izleme ve SMS izleme) sunmaktadır, ancak dahili araştırmalara yardımcı olan diğer mevcut veri setlerini toplamayı başaramamaktadır. Araştırılan MDM ürünlerinin Juniper Pulse Mobil Güvenlik Paketi (v.3.0R3) en çok kullanıcı izleme yetenekleri sundu ve bu araştırmanın bir parçası olarak değerlendirildi. Bulgular, ürünün DroidWatch'ta kapsanan veri kümelerinin yaklaşık %50'sini topladığını gösterdi; Bununla birlikte, verilerin depolanması ve Juniper kontrollü sistemler tarafından barındırılması gerekir. Bu, bir kuruluşun denetim verilerini dahili olarak saklama şartını engelleyebilir.

Kişisel "casus" uygulamalar (örn., **Mobistealth**, **StealthGenie**, **FlexiSpy** ve **Mobile Spy**) gibi piyasada bulunan diğer ürünler, DroidWatch ile aynı veri kümelerinin çoğunu toplayabilir, ancak yükseltilmiş ayrıcalıklar için gereksinimler ve eksiklikler gibi sınırlayıcı faktörlere sahiptir. Ayrıca kurumsal depolama ve analiz yetenekleri açısından kullanıcı bilgisi olmadan kişisel bilgiler toplayan, genellikle casus yazılım olarak sınıflandırılırlar (Juniper Networks, 2012).

U.S. v Ziegler (2007)	Kullanıcıların politikadan haberdar olması durumunda bir kuruluş kendi ekipmanını izleme hakkına sahiptir
City of Ontario v. Quon (2010)	Denetlemeler, bir çalışan tarafından ödenen ek ücret

	ödemeleri bile şirket tarafından sağlanan bir cihaz üzerinde gerçekleştirilebilir
Carrier IQ	Mevcut değil. Bekliyor.

Tablo-1: Mobil cihaz mahremiyet davaları

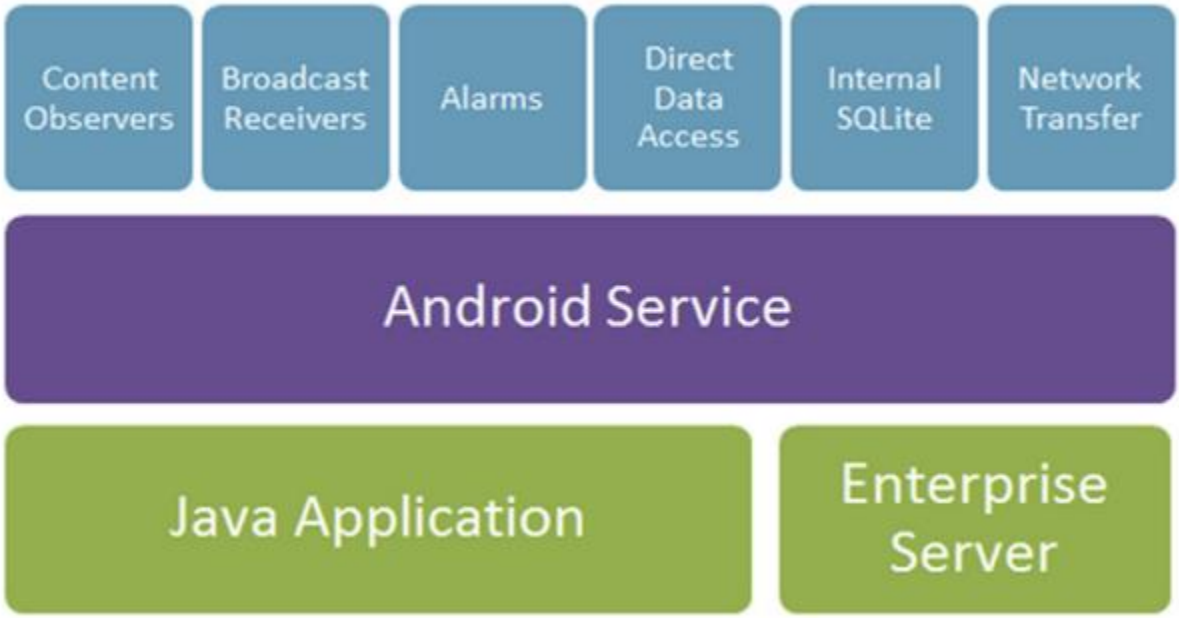
Uzaktan kurumsal adli delil toplama araçları da kuruluşun güvenliğini artırmayı hedeflemektedir**. Google Rapig Response** (GRR), adli araştırmacılara ve olaya müdahale eden kişilere, adli olarak bir ağ üzerinden çok sayıda makinadan kanıt elde etmesini sağlar (Cohen ve diğerleri, 2011). GRR'ye benzer ticari çözümler EnCase Enterprise, **AccessData Enterprise**, **F-Response Enterprise Edition** ve **Mandiant Intelligent Response**'dır. EnCase Enterprise, Android'i desteklerken, diğerleri şu anda bunu desteklemez. Sözü edilen uzaktan adli araçlar, verileri sürekli olarak toplamayıp depolamadıkları için DroidWatch'tan farklıdır. Bunun yerine, operatöre talimat verildiğinde verilerin bir kerelik fotoğraflarını çekerler. DroidWatch kodu bu araçların yeteneklerini genişletmek için kullanılabilir.

3.2. Akademik Araştırma

Bu araştırmayı çeşitli bilimsel çabalar şekillendirmiştir. Lee ve diğerleri tarafından önerilen bir sistem; bir akıllı telefondan Android Uygulama Programlama Arayüzünü (API) kullanarak aynı SDCard'a hızlıca veri çıkarmak için bir Secure Digital Card (SDCard) üzerinde bulunan bir Android uygulamasını kullanıyor (Lee ve ark., 2009). Verilerin toplanmasına yönelik bu mantıklı yaklaşım, sisteminin bir cihazı sürekli olarak izlemesi dışında DroidWatch'a benzer. Bununla birlikte, çalışma sırasında kök ayrıcalıkları olmadan elde edilebilen çeşitli veri setlerini vurgulamaktadır. **ViaForensics** tarafından açık kaynaklı ürün olarak piyasaya sürülen **AFLogical** benzer bir yaklaşım benimser. Ayrıca, özel bir SDCard kullanır ve alınan veri kümelerinin sayısını genişletir (Hoog, 2010). Yang ve ark.'nın takip çalışmaları SDCards için bulut bilgi işleminin yerini almasını önerdi; Bununla birlikte, araştırmaları bir cihaza fiziksel olarak erişmeyi gerektirir ve sürekli veri toplamaz (Yang ve Lai, 2012).

Villan ve ark. , Sanal bir ağ bilgisine (VNC) benzer gerçek zamanlı izleme gerçekleştiren yerli bir Android uygulamasını, bir akıllı telefon üzerinde kök ayrıcalıkları kullanmadan gerçekleştirdi (Villan ve Esteve, 2011). Araştırma kullanıcıların ekranını kullanılabilirlik amacıyla uzak bir yere akıtmayı (yani, kurumsal yardım masalarında kullanmak için) akıtmayı içerir ancak bir kullanıcının ekranını izleyebilme özelliği DroidWatch'ta gelecekteki bir özellik olarak uygulanabilir. Shields ve ark. Tarafından sunulan araştırma. Yeni bir nesne parmak izi yaklaşımı (Shields ve ark., 2011) kullanarak sürekli ve proaktif bir şekilde bir ağ üzerinden gerçek adli bilişim edinimlerini gerçekleştiren ilk sistem olan Proaktif Nesne Parmak İzi ve Depolama (PROOFS) adında bir edinim ve izleme sistemi başlattı. **PROOFS**, Android akıllı telefonlarda çalışmazken, bir izleme aracının adli olarak kabul edilmesi gereken kriterlerini vurgulamaktadır. DroidWatch ile ilgili gelecekteki çalışmalar, bu kriterlerden bazılarının dahil edilmesini içerir.

Android platformundaki eski anti-adli bilişim çalışması, DroidWatch'ın nasıl tehlikeye atıldığını veya engelleneceğini değerlendirmede etkili oldu. Birkaç genel anti-adli kavramlar, Distefano ve diğerleri tarafından Android'e aktarıldı ve DroidWatch uygulamasının anti-adli değerlendirmesi sırasında bir rehber olarak görev yaptı (Bölüm 4.3) (Distefano ve ark., 2010). Azadegan ve arkadaşlarının yaptığı araştırma. Ek anti-adli bilişim konsepti sundu ve ayrıca yukarıda anılan DroidWatch değerlendirmesine dahil edildi (Azadegan ve ark., 2012).



Şekil-1: DroidWatch sistem mimarisi

Broadcast Receiver →Content Observer→Alarm

Şekil-2: Tasarım Stratejisi

Strateji, göreceli olarak kolay uygulanabilirlik, gerçek zamanlı bildirimleri işleme yeteneği ve yanlış pozitif ve çoğaltılması konularına odaklanmaktadır. İlk önce, sistem yayınları üretip üretmediğini belirlemek için veri setleri analiz edilmelidir. Eğer yaparlarsa, yayın alıcıları koleksiyonlar için uygulama bileşeni olarak düşünülmelidir. Yayınlar mevcut değilse, içerik gözlemcilerini uygulamaya geçirmeyi düşünün. Yayınlar ve içerik gözlemcileri hedeflenen veri koleksiyonları için kullanılamıyor veya etkisiz ise alarmlar kullanılmalıdır.

4.1.4. Yerel depolama

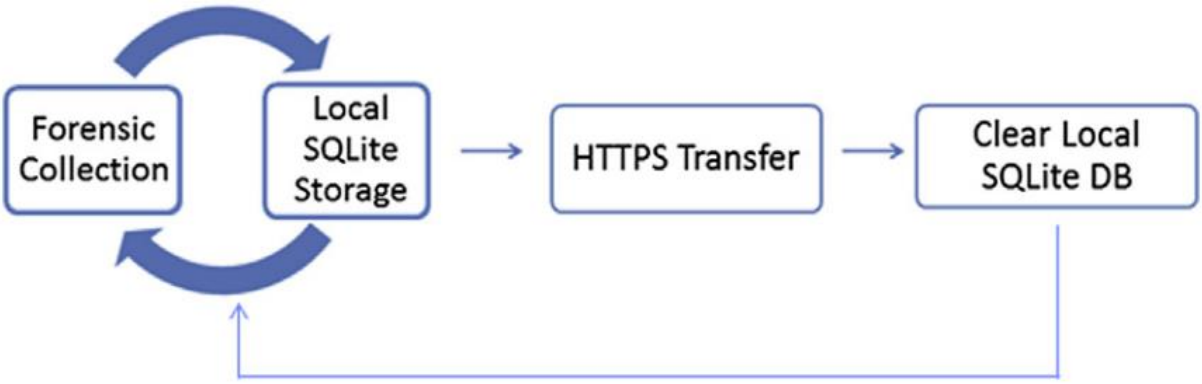
Tüm toplanan veriler telefonda yerel bir SQLite veritabanında geçici olarak saklanır ve sadece DroidWatch uygulaması tarafından erişilebilir olacak şekilde yapılandırılır. Standart Yapısal Sorgulama Dili (SQL) veritabanı fonksiyonları, özel bir DroidWatch içerik sağlayıcısı tarafından işlenir. Bu, her bir DroidWatch koleksiyonunun iş parçacığına göre güvenli ve yapılandırılmış bir biçimde gerçekleştirilmesini sağlar. Zamanlanmış bir alarm periyodik olarak yerel SQLite veritabanı dosyasını güvenli köprü metni aktarım protokolü (HTTPS) POST üzerinden işlenmek üzere kuruluş sunucusuna aktarır. Aktarım işlemi, veritabanı dosyasının nispeten küçük boyutunun (ortalama 75 kilobayt) yardımıyla bir kullanıcının deneyimine en az etkisi olan arka planda çalışacak şekilde tasarlanmıştır.

4.1.5. Şirket sunucusu

Toplanan verilerin aktığı kurumsal sunucu prototipi, **Apache**, **PHP**, **MySQL** ve **Splunk** çalıştıran özel yerel bir ağdaki Ubuntu sanal makinesidir. Apache kendinden imzalı bir güvenli soket katmanı (SSL) sertifikasıyla yapılandırılmış ve DroidWatch uygulaması içinde bir varlık dosyası olarak dahil edilmiştir. Bu, bir HTTPS bağlantısı üzerinden veri aktarılmasına izin verir. PHP kodu, SQLite dosya yüklemelerini yönetir ve olayları bir MySQL veritabanına ayıklar. Splunk, periyodik olarak MySQL veritabanından veri çeker ve analiz ve raporlama için olayları arabiriminde kullanılabilir duruma getirir.

4.1.6. Veri Akış Süreci

DroidWatch uygulaması içindeki veri akış süreci (Şekil 3) sürekli bir işlemdir, transferler her 2 saatte bir denenir (bu değer konfigüre edilebilir). Kurumsal sunucuya başarılı bir şekilde aktarıldıktan sonra, aktarmadan önce tarihli olaylar yerel telefon veritabanından silinir ve bu da o veritabanının boyutunu en aza indirir. Başarısız olan dosya aktarımları günlüğe kaydedilir ve herhangi bir etkinliğin silinmesine yol açmaz.



Şekil-3: Veri İşleme Akış Diyagramı

Cihaz hesabı bilgileri, DroidWatch hizmeti başlatıldıktan sonra doğrudan Android API üzerinden toplanır.

Data set	App component used		
	Broadcast receiver	Content observe	Alarm
App install/removal	x		
Browser navigation			x
Browser search			x
Calendar event			x
Call log		x	
Contact list		x	
Device accont[a]			
Device ID			x
GPS location			x
GPS location setting	x		
MMS	x		x
Pictre gallery		x	
Screen lock stats	x		
SMS	x	x	
Third-party app log			x

[a] *Cihaz hesabı bilgileri, DroidWatch hizmeti başlatıldığında doğrudan Android API aracılığıyla toplanır*

Tablo-2: Toplanan Veri Seti

4.1.7. Veri Kümeleri

Tablo 2, DroidWatch tarafından toplanan veri setlerini listeler. Bu veri setleri, mevcut içerik sağlayıcıları, iç araştırma için ihtiyaçlar ve erişilebilirlik seviyesine (yani kök gerekmez) bağlı olarak seçildi. Her veri kümesi, derleme aralıklarının ayarlanmasını sağlayan (yani, sistemin koleksiyonlar arasında ne kadar süre beklediğini) uygulama kaynak kodundaki bir varlık dosyası olan ***droidwatch.properties*** aracılığıyla yapılandırılabilir. Kuruluşlar, karşılık gelen aralık değerini sıfıra ayarlayarak bir veri kümesinin atlamasını seçebilirler. On beş benzersiz veri setine erişilebilir; İki veri kümesi ve hesap şifresi araştırılmıştır ancak kullanılmamıştır (aşağıda açıklanmıştır). E-posta uygulamasına erişmek için kullanılan mekanizmalar standart Android Yazılım Geliştirme Seti'nin (SDK) parçası değildir (CommonsWare, 2010). Buna ek olarak, e-posta uygulaması, üçüncü parti uygulamaların özel verilere erişmesini yasaklayan bir ***signatureOrSystem*** izniyle sınırlandırılmıştır (Android Open Source Project, 2008). Hesap

şifreleri benzer korumalarla korunmaktadır; Arama uygulaması, AndroidManifest'te AUTHENTICATE_ACCOUNTS yetkisine izin vermeli ve kullanıcı kimliğini istediğiniz hesaba (Google (N.D.). Hesap Yöneticisi) eşleştirmelidir. Bazı veri setleri, koleksiyonları gerçekleştirmek için birden fazla uygulama bileşeni kullanıyordu. Örneğin, Multimedya Mesaj Servisi (MMS) mesajları, bir yayın alıcısı ve bir alarm kullanılarak algılanır; Kullanılan bileşen mesaj odaklıdır.

4.2. Analiz ve Değerlendirme

Bu bölüm, DroidWatch denemesinin sonuçlarını açıklar ve bunları iç araştırmanın yardımcı olabileceği durumlara uygular. Senaryo dosyası deneyleri, mevcut veri kümelerine ve yazarın önceki iş deneyimine dayanır. Tüm sonuçlar tek bir cihazdan ve kullanıcıdan elde edilmiştir. Splunk'ın maliyeti (günlük 500 megabite kadar ücretsiz) nedeniyle bu araştırma için kullanıldığını unutmayın, diğer ürünler benzer işlevleri yerine getirebilir.

Şekil 4, Splunk'ta kaydedilen günlük olayların sayısını, veri seti ile ayrılmış olarak, tek bir gün aralığı boyunca göstermektedir. Örnek, bir cihaz tarafından üretilen 442 gün içeriyor ve kaydedilen nispeten az sayıda olayı vurguluyor. Günlük toplamlar kullanım alışkanlıklarına göre değişir; Ağır biçimde kullanılan bir cihaz, günlük toplamda bir artış görür. Deney sırasında kullanıcı deneyimi veya artan pil tüketimi üzerinde olumsuz bir etkisi yoktur.

4.2.1. Genel Kullanım Eğilimleri

Splunk'teki "Ekran Kilidi Açılmamış" arama, etkin telefon kullanımını gösteren kullanıcı eylemlerinin zaman çizelgesini (örn. PIN kodu, hareket veya parola girdileri) görüntüler. Birkaç güne kadar elde edilen sonuçlar Şekil 2'de görülebilir. Bu veriler belirli bir zamanda telefon etkinliğini belirlemek, maskeli kullanıcıları (ilk atanmış kullanıcı dışındaki kullanıcılar) bulmak veya çalışanlar için kullanım desenleri oluşturmak için kullanılabilir.

4.2.2. Şüpheli Kişiler ve İletişim

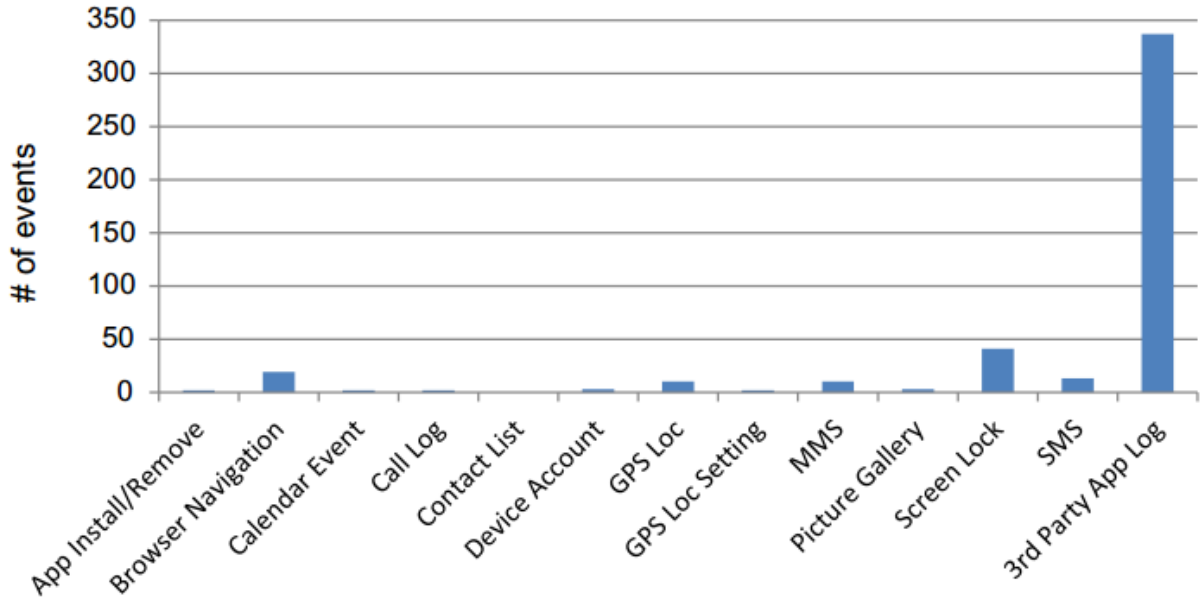
Bir kuruluşu riske atan kişilerin veya telefon numaralarının adlarını, arama yaparak veya bunları Splunk tetikleyicilerine (Splunk Enterprise'da bulunur) bulabilirsiniz. Bunlar, bir şirketin telefon defterinin dışındaki numaralar veya kara listeye girmiş insanlar olabilir. Kaydedilen SMS ve MMS içeriği de şüpheli etkinlikler için aranabilir. DroidWatch'te gelen SMS, zaman damgasını ham SMS olarak işleyerek üçüncü parti bir zaman kaynağı olarak da hizmet edebilir. SMS yapısında gömülü olan zaman, telefonun zamanına bağlı değildir (Casey, 2009). Bu verilerin analizi sırasında karşılaşılan bazı sorunlar şunlardı:

Şekil-5 :Algılanan ekran kilidi açma aksiyonları (Splunk)

- Birden fazla kişiye gönderilen mesajlar, günlüklerde yalnızca bir alıcı listeledi.
- Gelen SMS'lerde saat dilimleri eksik.
- MMS mesaj metni mevcut değildi.

Bir fotoğraf cihaz kamerasıyla çekilip hemen MMS ile gönderildiğinde, etkinlik koşullara bağlı olarak daha fazla soruşturma yapılmasını gerektirebilir. Şekil 6, 22 Aralık 2012 Cumartesi günü 03.20'de çekilen bir resim günlüğünü gösteren bir aramayı göstermektedir. Kullanıcının ofiste ve yalnız olduğunu tespit edilirse (muhtemelen GPS izleme yoluyla) bir

veri sızıntısının olup olmadığını belirlemek için daha fazla analiz gerekli olabilir.



Şekil-4: 24 saatte kaydedilen olaylar

Şekil-6: Fotoğraf ve MMS arama sonuçları

4.2.3. Konum izleme

DroidWatch tarafından kaydedilen bilinen son konumlar arasında cihaz kimliği, enlem, boylam ve yakalama süresi bulunur. DroidWatch'ın konumları toplamak için kullandığı yaklaşım pil ömrünü korur ancak kaydedilen yerlerin seyrek kaydedilmesine neden olur. Yedi günlük süre boyunca yalnızca dört yer olduğu bildirildi. GPS sağlayıcı ayarı etkinleştirilmiş olsa da, GPS aktif olarak kullanılmadıkça bilinen en son konumlar bir cihazda saklanmaz (diğer bir deyişle, Google Haritalar uygulaması mevcut konumu görüntülemek için açılır). Ayrıca bir telefonun son bilinen konum değeri, cihazın yeniden başlatılması üzerine silinir ve kaydedilen bir koordinat kümesinin kaydedilmeden önce kaybolmasına neden olur.

Konum sağlayıcı ayarında yapılan değişiklikler izleme için de kullanılabilir. Telefonun fiziksel konum verileri daha güvenilir hale gelirse, bu veriler potansiyel olarak yararlı olur. GPS ayarı manuel olarak kapatıldığında bir cihazın konumunun tanımlanmasına izin verir.

Kaydedilen takvim olayları araştırmacılara da faydalıdır. Bir kullanıcının randevuları için yapılan aramalar, geçmişteki kontrol, gözetim planlaması veya seyahat planlarını belirleme konusunda yardımcı olabilir.

4.2.4. İnternet geçmişi

DroidWatch, yerleşik Android Web tarayıcısı içinde gerçekleştirilen etkinlikleri toplar ve kullanılabilir duruma getirir. Bir İnternet geçmişi etkinliği, alınan eylemi (ör. Göz atma veya arama), arama terimini veya URL'yi, etkinlik

saatini ve ilişkilendirilmiş cihaz kimliği içerir. Bu bilgiler, bir şirkette şüpheli tarayıcı kullanımını tanımlamak için kullanılabilir (örneğin, fikri mülkiyetlerin harici web sitelerine yüklenmesi). Tarayıcı aramaları, tespit edilen işlemlerin ardındaki kullanıcının olası niyetlerini daha iyi tahmin edebilmek için ayrıştırılabilir.

4.2.5. Kötü amaçlı uygulamalar

Yüklü uygulamalar için bir denetim, bir cihazın kötü amaçlı yazılım veya diğer endişe uyarıları içerdiğini ortaya çıkarabilir. Bu, dahili bir soruşturma sırasında ek endişeler ve güvenlik önlemleri alınmasını garanti eder. Sağlanan DroidWatch sonuç alanlarına, uygulamanın adı, gerçekleştirilen eylem ve kurulum / kaldırma tarihi dahil. Üçüncü taraf uygulama günlükleri de DroidWatch tarafından toplanır. Birkaç filtreleme mekanizması, günlükleri, yalnızca telefonda yerleşik olmayan uygulamalar tarafından üretilenlere sınırlar. Filtreleme mükemmel olmadığı halde, toplanan uygulama günlüklerinin toplam miktarı, gün başına 337 günlük (10.000'i aşan) daha yönetilebilir bir ortalamaya düşürüldü.

4.3. Adli bilişim

İzleyen bölümler, anti-adli bilişim kategorileri, Android antiforensi alanında yapılan önceki çalışmalardan alınmış ve anti-adli olabilecek güvenlik açıkları için DroidWatch uygulamasını değerlendirmek için kullanılıyor. Kanıtları gizleme (Bölüm 4.3.2), kanıt kaynaklarını değiştirme (Bölüm 4.3.3), kanıtları taklit etme (Bölüm 4.3.4) ve adli bilişim araçlarını tespit etme (Kısım 4.3.5) kategorileri kanıtları yok ediyor (Bölüm 4.3.1) (Distefano ve diğerleri, 2010; Azadegan ve diğerleri, 2012). DroidWatch'in mevcut haliyle, kök saldırılarına, uygulamanın kaldırılmasına ve işlem sonlanmalarına karşı tamamen duyarlı olduğunu unutmayın. Kök algılama ve uygulama yükleme politikalarının uygulanması gibi MDM'ler tarafından sunulan dış koruma, DroidWatch'ta veri bütünlüğünü sağlamaya dayanır.

4.3.1. Delilleri yok etme

Yayın alıcıları ve içerik gözlemcileri aracılığıyla toplanan veri setleri, olay ortaya çıktıkça her olayın kopyası DroidWatch'ın özel saklama alanına kaydedildiğinden, kanıt imha yöntemlerine karşı muhtemel değildir. Bununla birlikte, kanıtları kaldırmak mümkün olabileceğinden (örneğin, giden MMS mesajları, üçüncü taraf uygulama günlükleri, takvim etkinlikleri, tarayıcı gezintileri, tarayıcı aramaları ve bilinen en son GPS konumları) alarmlardan alınan veri setleri tahribat taktiklerinden etkilenir. Bir sonraki planlanan koleksiyona başlamadan önce. DroidWatch ile ilgili endişe, uygulamaların yükleme sonrasında özel niyet filtresi öncelikleri için kayıt yapabilmesidir. Maksimum maksat filtre öncelik değeri olan 231-1 kullanan bir uygulama, başka bir uygulama tarafından yayınlanmadan önce yayını engelleme ve bırakma özelliğine sahiptir. DroidWatch, bir araştırma prototibi olarak durumundan dolayı varsayılan intent-filter öncelik değerini kullanır.

4.3.2. Kanıt gizleme

Zamanlanmış alarmlar yoluyla toplanan veri setleri veri gizleme taktiklerinden etkilenenler arasındadır. Son gönderilen birkaç MMS iletisini gizlemek isteyen bir kullanıcı, bunları DroidWatch toplama işleminden yönlendirmek için el ile aktarma yöntemlerini kullanabilir. Yukarıda bahsedilen uygulamalar için özel amaçlı filtre öncelikleri kaydetme özelliği, benzer bir şekilde, uygulamanın yayınların engellenmesi ve yeniden yönlendirilmesi yoluyla verileri gizleyebilmesini sağlar. Örneğin, meşru bir üçüncü parti SMS uygulaması olan

GoSMS, gelen SMS mesajlarını aktarmak ve sistem bildirimlerinin çoğaltılmasını ortadan kaldırmak için olası en üst düzey filtre önceliğini kaydetmektedir (Kovacevic, 2011).

4.3.3. Kanıt kaynaklarını değiştirme

Kanıt kaynaklarını değiştirmek, bir veri kümesini bir toplama işlemini engellemek için değiştirmeyi içerir (Distefano ve diğerleri, 2010). Bu, DroidWatch için başka bir endişe alanı. Alarmlar tarafından toplanan veriler duyarlıdır çünkü süreçler, mevcut bir veri setinde belirli değerlere dayanır. Örneğin, yeni giden mesajlar için MMS içerik sağlayıcısı aracılığıyla tarama yapılırken "msg_box" alanı, gönderilen / giden MMS'i temsil eden "2" ile iletinin yönünü belirtir. Bu alanın değeri "5" olarak değiştirilirse, ileti toplama işlemi sırasında yoksayılır.

4.3.4. Taklit kanıtları

Mobil cihazlardaki sahteciliğe dayalı kanıt, araştırmacıların kafasını karıştırmak veya kaçmak için mevcut veri setlerine hayali veri ekleme işlemlerini içerir. DroidWatch koleksiyonları bu açıdan savunmasızdır, çünkü sahte girişleri gerçek olanlardan ayırmak için herhangi bir kontrol gerçekleştirilmez. DroidWatch için bir başka endişe olan hizmet reddi saldırısında kısa sürede büyük miktarda hayali veri eklenmesi. Yeterli veri bir telefona yüklenirse, uygulamanın düzgün çalışması durabilir.

4.3.5. Adli bilişim araçlarının tespit edilmesi

Adli bilişim araçları tarafından gerçekleştirilen adli bilişim araçlarının araştırılmasının doğrudan DroidWatch için geçerli olmadığı tespit edildi (Azadegan et al., 2012). Onlar, Android telefonlarında bazı tanınmış adli bilişim araçlarının ilk bağlantı imzalarını dinlemeye odaklandı. DroidWatch, geleneksel adli bilişim araçlarının aksine izlemeyi gerçekleştirir ve bir cihaza fiziksel olarak erişmek için herhangi bir ilk bağlantı imzası veya gereksinimi yoktur. Bununla birlikte, imza tespit fikri, DroidWatch'ın tarifeli transferlerine uygulanabilir.

5. Gelecekteki çalışma

DroidWatch ile ilgili gelecekteki araştırmalar, uygulama ve kurumsal sunucu üzerinde çalışmayı içerir. Yaklaşan bölümler, ek veri setleri toplamak (Bölüm 5.1) ve anti-sabotaj mekanizmalarını uygulamak için önerilen gelişmeleri kapsar (Bölüm 5.2).

DroidWatch'ın gelecekteki iyileştirmelerinin yanı sıra DroidWatch'ın bir MDM çözümü içine entegrasyonu, Android güvenlik topluluğu için çok değerli olacaktır. Mevcut MDM sistemleri, dahili soruşturmalara yardımcı olabilecek kullanıcı izleme özelliklerine sahip değildir. Sağlam politikanın uygulanmasını, uzaktan cihaz yönetimini ve Android cihazlarda kapsamlı bir kullanıcı izlemesi kombinasyonu sağlayan genel kurumsal güvenlik sistemi, Android akıllı telefon dağıtımlarını düşünen hükümet ve endüstri kuruluşları arasındaki güvenlik endişelerini azaltmaya yardımcı olacaktır.

5.1. Ek veri setleri

Android adli bilişimi, her yeni işletim sistemi sürümüyle değişen gelişen bir alandır. Yeni veri setleri ve özellikleri ortaya çıktıkça, muhtemel bir izleme sistemine dahil edilmeleri için bunların bir araştırmaya katma değeri değerlendirilmelidir. Gelecekteki DroidWatch içerikleri şunları içerir: USB hata ayıklama ayarları, telefon yeniden başlatma, sesli posta günlükleri ve dumpsys, dumpstate ve dmesg'den ek uygulama ve çekirdek günlükleri.

5.2. Koruma önleyici mekanizmalar

Toplanan ve bir telefonda saklanan veriler, kullanıcıların ve uygulamaların müdahale etmesini önlemek için halihazırda Android yerleşik güvenlik modeli (Kısım 2.2) üzerinde çalışıyor. DroidWatch'ı daha sıkı hale getirmek için bazı yetenek önermeleri şunları içerir:

- Veritabanı olaylarının şifrelenmesi (sağlama toplamı ile)
- Yüksek niyetli filtre öncelik değerleri
- Log günlüğünü tutma
- Etkinliğe dayalı koleksiyonlar ve transferler
- Veritabanı karması

DroidWatch, veritabanındaki olayları şifrelemek, kullanıcıların önceden toplanan olayları görüntülemesine veya müdahalesini engellemeye yarayan bir mekanizma. Her olay bir sağlama toplamıyla eşleştirilebilir ve bir ortak anahtar altyapısı kullanılarak şifrelenebilir (kurumsal sunucuda depolanan özel anahtar ile). AndroidManifest'e maksimum niyet filtre öncelik değerlerini kaydetmek, iki uygulamanın aynı öncelik değerine kaydolması durumunda ne olacağını belirlemek için daha fazla araştırmaya ihtiyaç duyulmasına rağmen, uygulamaların sistem yayınlarını engellemesine engel olabilir. DroidWatch veritabanına "canlı tutma" mesajlarının periyodik olarak günlüğe kaydedilmesi servis kesintilerini vurgulamaktadır. Kütükler arasında zamandaki boşluklar varsa kurcalamaya neden olabilir. Olay tabanlı tetikleyiciler, daha rasgele bir aktarım kalıbı sağlayabilir ve zamanlanmış operasyonlara karşı zaman esaslı engeller girişimleri önleyebilir; Bununla birlikte, bu kabiliyetin etkinliği hakkında daha fazla araştırmaya ihtiyaç vardır.

6. Sonuç

Bu araştırmada tanıtılan sistem, Android topluluğunun kök ayrıcalıkları olmaksızın kurumsal ortamlarda sürekli Android izlemesi tasarlaması ve uygulamak için bir prototip olarak hizmet ediyor. DroidWatch, türünün ilk açık kaynak sistemidir; Ancak, yeteneklerini genişletmek ve geliştirmek için daha fazla gelişme gerekmektedir. Güvenliği artırmak için anti-sabotaj mekanizmalarının da uygulanması gerekecek. Belirtildiği gibi, toplanan veri setleri çeşitli nedenlerle çeşitli iç tetkik türleri için yararlıdır. Bu araştırma, Android uygulamaları bileşenlerini izleme için önceliklendirmek için kullanılabilecek yeni bir geliştirme tasarım stratejisine katkıda bulunuyor. Son olarak, bu çalışma, varsayılan Android API aracılığıyla erişilebilen veri kümelerine erişmek için bir rehber görevi görür.

Teşekkürler

Yazar, giriş ve düzenlemeleri için tez komitesi üyelerine (Bill Stackpole, Dr. Tae Oh ve Dr. Yin Pan), MITER meslektaşları (özellikle Mark Guido) ve Monica Grover'a teşekkür etmek istiyorlar.

Referanslar

References

Android Open Source Project. Android/platform/packages/apps/Email.gitl. https://android.googlesource.com/platform/packages/apps/Email.git/þ/android-2.3.6_r1/AndroidManifest.xml; 2008.
Azadegan S, Yu W, Sistani M, Acharya S. Novel anti-forensics approaches for smart phones. In Hawaii International Conference on System Sciences (pp. 5424–5431). Maui, HI: IEEE; 2012, January 4.
Casey E. Top 7 ways investigators catch criminals using mobile device forensics. http://computer-forensics.sans.org/blog/2009/07/01/top-7-ways-investigators-catch-criminals-using-mobile-device-forensics; 2009, July 1.
Citrix. IT organizations embrace bring-your-own devices. http://www.citrix.com/site/resources/dynamic/additional/Citrix_BYO_Index_report.pdf; 2011, July 22.
Cohen MI, Bilby D, Caronni G. Distributed forensics and incident response in the enterprise. In: Digital forensics research workshop 2011. New Orleans, LA: Elsevier; 2011S101–10; August 2011.
CommonsWare. Access Android emails through content provider. http://stackoverflow.com/questions/3811608/access-androidemails-through-content-provider; 2010, September 28.
comScore, Inc. comScore reports October 2012 U.S. mobile subscriber market share. http://www.comscore.com/Insights/Press_Releases/2012/11/comScore_Reports_October_2012_U.S._Mobile_Subscriber_Market_Share; 2012, November 30.
Davis W. Carrier IQ loses preliminary round in privacy lawsuit. http://www.mediapost.com/publications/article/175096/carrier-iq-loses-preliminaryround-in-privacy-laws.html#axzz2FMwgPlJ6; 2012, May 21.
Distefano A, Me G, Pace F. Android anti-forensics through a local paradigm. In Digital forensics research workshop 2010 (pp. S95–S103). Portland, OR: Elsevier; August 2010.
Google. (n.d.). Application fundamentals. http://developer.android.com/guide/components/fundamentals.html.
Google. (n.d.). ContentObserver. http://developer.android.com/reference/android/database/ContentObserver.html.
Google. (n.d.). Permissions. http://developer.android.com/guide/topics/security/permissions.html.
Google. (n.d.). AccountManager. http://developer.android.com/reference/android/accounts/AccountManager.html.
J. Grover / Digital Investigation 10 (2013) S12–S20 S19
Hoog A. Android forensics: investigation, analysis and mobile security for Google Android. Waltham, MA: Syngress; 2011.
Hoog A. Open source Android digital forensics application. http://computer-forensics.sans.org/blog/2010/03/01/open-source-androiddigital-forensics-application; 2010, March 1.
Juniper Networks. MTC mobile signatures. http://www.juniper.net/us/en/security/mobile-threat-center/#ANDROID:A.Mobistealth; 2012, June 28.
Kovacevic N. SMS broadcastreceiver not called when GO SMS Pro installed. http://stackoverflow.com/questions/6561297/sms-broadcastreceivernot-called-when-go-sms-pro-installed; 2011, July 15.
Lee X, Yang C, Chen S, Wu J. Design and implementation of forensic system in Android smart phone. http://crypto.nknu.edu.tw/publications/2010JWIS_Android.pdf; July 2010.
MarketsandMarkets. Bring-your-own-device (BYOD), consumerization of IT (Co-IT) and enterprise mobility market – Global advancements, business models, market forecasts & analysis (2012–2017). http://www.marketsandmarkets.com/AnalystBriefing/byod-enterprise-mobilitymarket.asp; 2012, September 21.
Marks J. ICE drops BlackBerry in favor of iPhone. http://www.nextgov.com/mobile/2012/10/ice-dumps-blackberry-favor-iphone/58905/; 2012, October 19.
Pettey C. Gartner says two-thirds of enterprises will adopt a mobile device management solution for corporate liable users through 2017. http://www.gartner.com/it/page.jsp?id¼2213115; 2012, October 25.
Rauf DS. More feds ditch BlackBerrys. http://www.politico.com/news/stories/0212/73369.html; 2012, February 28.
Richardson R. 2010/2011 CSI computer crime and security survey. http://gocsi.com/survey; 2010, December 2.
Shields C, Frieder O, Maloof M. A system for the proactive, continuous, and efficient collection of digital forensic evidence. In Digital forensics research workshop 2011 (pp. S3–S11). New Orleans, LA: Elsevier; August 2011.
U.S. Census Bureau. USA quickfacts. http://quickfacts.census.gov/qfd/states/00000.html; 2010.
U.S. Court of Appeals, 9th Circuit. U.S. v. Ziegler. http://www.ca9.uscourts.gov/datastore/opinions/2007/06/20/0530177o.pdf; 2007, June 20.
U.S. Supreme Court. City of Ontario, California, et al. v. Quon et al. http://www.supremecourt.gov/opinions/09pdf/08-1332.pdf; 2010, June 17.
Valle S. Android forensics & security testing. http://opensecuritytraining.info/AndroidForensics.html; 2013, January 7.
Vidas T, Zhang C, Christin N. Towards a general collection methodology for Android devices. In: Digital forensics research workshop 2011, New Orleans, LA 2011S14–24; August 2011.
Villan AG, Esteve JJ. Remote control of mobile devices in Android platform. http://openaccess.uoc.edu/webapps/o2/handle/10609/8131; 2011, June 19.
Yang C-H, Lai Y-T. Design and implementation of forensic systems for Android devices based on Cloud computing. Applied Mathematics & Information Sciences Jan. 2012:243S–7S.

Justin Grover, MITRE Corporation için bir siber güvenlik mühendisi olarak çalışan dijital adli tıp alanında 5 yıllık tecrübeye sahiptir. Geneseo'daki New York Devlet Üniversitesi (SUNY) 'ndan Rochester Institute of Technology'den bilgi güvenliği ve bilgisayar bilimleri alanında bilgisayar güvenliği alanında yüksek lisans derecesine sahiptir. MITRE için çalışırken, Bay Grover, büyük bir hükümet kuruluşu için bir güvenlik operasyonları merkezi dahilindeki iç tehdit analisti ve geliştiricisi olarak ikiye katlandı ve 100'den fazla dahili soruşturmayı destekledi. Yakın zamandaki çalışmaları arasında MITRE'nin yenilik programı kapsamındaki Android cihaz adli tıp araştırmaları yer alıyor.