YÖNETİM BİLİŞİM SİSTEMLERİ DERGİSİ
http://dergipark.ulakbim.gov.tr/ybs/

Yayın Geliş Tarihi: 30.05.2016
Yayına Kabul Tarihi: 15.08.2016
Online Yayın Tarihi: 05.10.2016

ilt:1, Sayı:3, Yıl:2016, Sayfa 150-156
ISSN: 2148-3752

PCAP PAKETLER İLE RESTFULL API'Yİ GERÇEK ZAMANLI DİNLEME

Eda Sena KARAAĞAÇLI

Ahmet Anıl MÜNGEN

Hakan ERDÖL

Öz

Sosyal medya kullanım oranı, internet ve mobil cihaz kullanımının hızla artmasıyla birlikte artmaktadır. Birçok kişi sosyal medya hesaplarında kişisel bilgilerini paylaşmakta veya kişisel yazışmalar yapmaktadır. Yaptığımız çalışma bulunduğumuz ağı dinleyen ve ağdan geçen iletişim paketlerini (PCAP) elde ederek kullanıcıların özel sosyal medya ağındaki verilerini almayı ve çözmeyi amaçlar. Çalışmada sadece sosyal ağlar için değil, aynı zamanda yerel ağ içinde iletişim kurup bilgi alışverişi yapan iki sistem arasındaki veri iletişiminin dinlenip, kişisel bilgilerin kolayca elde edilebileceği gösterilmiştir.

Anahtar Kelimeler: Paket Yakalama, Paket Koklama, Restfull, Ağ Dinleme

SNIFFING RESTFULL API VIA PCAP PACKAGE IN REAL TIME

Abstract

Usage rate of social media has increased with mobile internet penetration rate and advanced mobile phones. A lot of people shares their personal information and making personal conversations on social media platform. In this study, we are aimed that to receive and decode users' personal information in social network by listening the network gathering communication frames (PCAP). This study showed that personal information can be easily acquired not only in social media, but also between two communicating system in local area network.

Keywords: Packet Capture, Packet Sniffing, Restfull , Network Listening

GİRİŞ

Ağ üzerinde haberleşme yapılırken veriler parçalanmadan bir bütün halinde iletilemez ve iletilmek istenen veri, bloklara ayrılır. Bloklara ayrılan veriler ağ katmanında paket olarak isimlendirilirler (Sinha and Gupta, 201: 33). Bilgisayar, mobil cihaz vb. iletim aygıtları ile internet arasındaki iletişim bu veri blokları tarafından gerçekleştirilir. Paket yakalama ise ağdaki bu veri paketlerinin izinsiz olarak kopyalanması ya da dinlenilmesi işlemidir. Bu işlem iletilmek istenen veri paketlerinin TCP/IP ağında takip edilmesi ve ethernet kartında yakalanması ile gerçekleşir. Takip sonucunda gelen ve giden veri paketlerinin port/IP numaraları hakkında bilgi elde edilir. Aynı zamanda gelen ve giden verinin içerikleri hakkında da bilgi sahibi olunur. Paket yakalama işlemi sayesinde ağdan istenilen, işe yarar paketler elde edilebilir ve iletişim sağlanan ağı izinsiz dinleyenler tespit edilebilir (Daiki et al., 2012). Paket yakalama işlemi ağlarda meydana gelen olumlu gelişmeler sayesinde zorlaşmıştır. Yüksek paket hızı ve yüksek bant genişliği sayesinde güvenlik açısından gelişmiş paketleri yakalamak oldukça zordur (Binti et al., 2013).

İletilmek istenen veri bilgisayar, mobil cihaz vb. aygıt tarafından internet aracılığıyla kullanılan ağa çıktıktan sonra, ağdaki bütün sistemlere ulaşır. Diğer bilgisayarlar ve alıcı cihazlar ağı dinler ve gelen veri paketlerinin başlıklarına bakarak onlara ait olup olmadıklarının tespitini yapar. Eğer veri başlığı kendilerine gönderilmişse kabul ederler aksi takdirde reddederler. Bu sırada paket yakalamak için özelleşmiş Wireshark, Ettercap veya NetworkMiner gibi uygulamalar ağ üzerindeki kendilerine ait olmayan ve o an ağda iletilen her veriyi dinleyerek kullanıcıya anlaşılır bilgiler vermektedirler (Wang et al., 2010; Waheed et al., 2013; Meethaisong and Premchaiswadi, 2015). Paket yakalama işlemi pasif ve aktif olarak 2'ye ayrılmaktadır (Ibrahim and Vaclav, 2015) .

Pasif paket yakalama işlemi genellikle hub ile yönetilen ağları dinlemek için kullanılır. Hub kullanan ağlarda iletilecek veri paketi ağa bırakılır ve tüm ağda bulunan cihazlara iletilir. Pasif paket yakalama işleminde, ağı dinlemeyi gerçekleştiren kişi kullandığı ağ üzerinde bulunan hiçbir cihaza saldırıda bulunmaz. Bu yüzden paket yakalama işlemi gerçekleştirilirken ağda bulunan diğer cihazların güvenlik duvarları, anti virüs programları ya da herhangi bir koruma amaçlı program uyarı vermez. Bunun anlamı kullanıcının haberi olmadan verilerinin bir başkası tarafından dinlenebileceğidir (Chen and Chan, 2012).

Aktif paket yakalama işlemi ise genellikle switch ile yönetilen ağları dinlemek için kullanılır. Switch kullanan ağlarda iletilmek istenen veri paketinin MAC adreslerine bakılır ve sadece iletilmek istenen ağdaki cihaza iletilir (Iyer and MCKeeown, 2013). Bu çalışmada da aktif paket yakalama işlemi uygulanmaktadır.

Aktif paket yakalama işlemi yaparken, iki sistemin haberleşmesinde yaygın olarak kullanılan gelişmiş servis haberleşmeleri vardır. Bu servis haberleşmelerine SOAP (Simple Object Access Protocol – Basit Nesne Erişim Protokolü) ve REST (REpresentational State Transfer) örnek verilir (Li et al.,2013; Takeuchi et al., 2005).

Çalışmada kullanılan REST servis haberleşmesi istemci-sunucu haberleşmesinde bir mimaridir. Bu mimari sisteminde kullanılan servislere RESTfull adı verilir (Razieh et al., 2014).

RESTfull istemci-sunucu arasındaki haberleşmeyi karışık sistemlerle sağlamak yerine HTTP protokolü üzerinden sağlamaktadır. Bunun sebebi World Wide Web yapısının HTTP protokolü üzerine kurulu olmasıdır. RESTfull sistemler basit olmalarının yanı sıra esnek ve değiştirilebilir bir yapıya sahiptirler. SOAP gibi kesin çizgiler ile sınırlandırılmış standartları yoktur (Li et al.,2013). Üzerinde C#, Java gibi birçok programla dili ile yazılmış çerçeve yapısı olmasına rağmen kolay ve hızlı bir şekilde standart kütüphaneler kullanılarak, RESTfull servisleri geliştirilebilir. Rest servisler platform bağımsızdırlar. Yani istemcinin Windows ya da Linux olmasının hiçbir önemi yoktur. Herhangi bir programlama diline bağımlı değildirler. Kolaylık sağlayan avantajları yüzünden, Twitter gibi çok yaygın kullanılan sosyal medya aracı

Rest API'yi tercih etmiştir. Amazon'un çeşitli amaçlar için kullandığı birçok Rest servis yapısı vardır. Dünyanın ileri gelen oyun firmalarından Blizzard Word of Warcraf, kullanıcılarına karakterler ile ilgili bilgileri RESTful servisler sayesinde sağlar (Bilizzard, 2016).

Makalenin geri kalanı şöyle düzenlenmiştir. İkinci bölümde PCAP paketini işleme süreci sunulmuş, bu süreçler içinde filtrelerden ve çalışmada kullanılan kütüphanelerden bahsedilmiştir. Üçüncü bölümde ise karşılaşılan problemler ve ileriki çalışmalar tartışılmıştır. Son bölümde ise çalışmanın sonucu sunulmuştur.

PCAP Paketini İşleme

Çalışma birçok kurumda da örneği görülebileceği gibi fiber optik kablolarla bir server'dan internete çıkılan, ağ yapısı üzerinde uygulanmıştır. Ağ üzerinde bulunan access pointler bir rooter'a bağlı, rooter'da direk server'a bağlıdır. Server üzerinden geçen tüm PCAP paketlerinin bir kopyasını dâhili sabit diskine kaydeder.

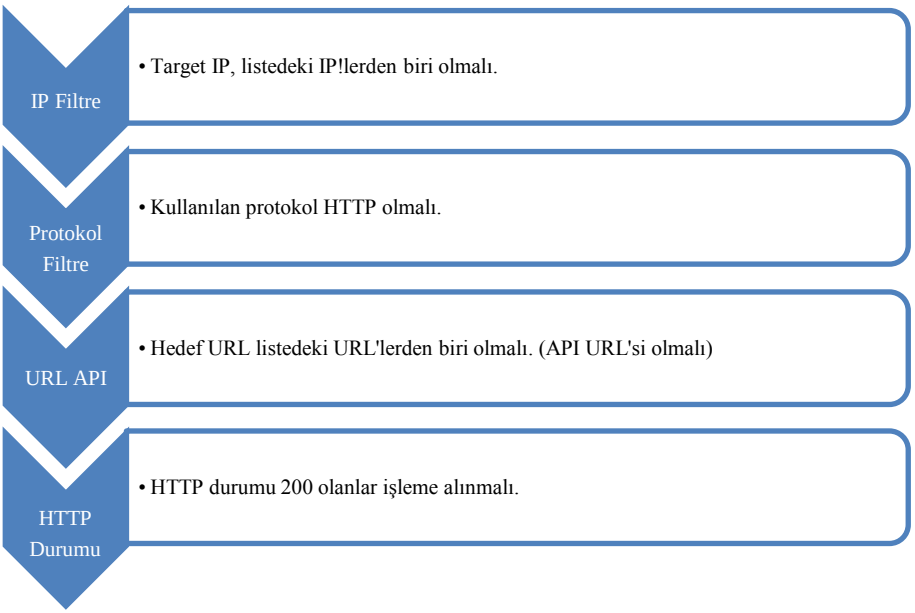
İlk karşımıza çıkan filtre protokol ve IP filtresidir. SSL ve ARP gibi protokollerin çözülmesi zor ve konumuz dışı olduğundan ele alınmaz sadece HTTP protokolleri takip edilir. Aynı zamanda yerel ağ'daki iletişimlerin de takip edilmesinin gereği olmadığı zamanlarda yerel ağ IP'li PCAP'larda silinir.

İkinci filtre, yazdığımız C# programı ile sabit disk'e kaydedilen her PCAP dosyası incelenir eğer şifreli değilse ve listemizde bulunan sosyal ağlardan birinin adresini içeriyorsa saklanır, içermiyorsa silinir.

Üçüncü filtre, PCAP içindeki target URL'nin bir API aracılığı ile mi yoksa tarayıcı aracılığı ile mi istenildiği takip edilir. Eğer tarayıcı tarafından gelmiş bir talep veya cevap ise bu girdi de silinir. Filtrelerin uygulanması hususu şekil-1'de şema olarak gösterilmiştir.

Son filtre, dönüş HTTP koduna uygulanan filtredir. Eğer talep 200 kodu ile dönüş yaparsa PCAP paketi işleme alınır. Eğer cevap tek PCAP paketi ile bitmemişse (standart bir haber sitesi sadece ana sayfası için çok sayıda PCAP paketi gönderir) bir sonraki PCAP paketi şuan işlemde olan PCAP paketinin meta datasından öğrenilir. Bir sonraki PCAP paketi de alınır. Bu işlemin pseudocode gösterimi şekil-2 de gösterilmiştir. PCAP paketinden alınan girdiler birleştirildikten sonra JSON -XML olup olmadığına göre test edilir. Eğer gelen veri JSON veya XML verisi ise o sosyal medyanın şablonuna göre çözülür ve veri elde edilir.

Şekil 1. Filtre Uygulaması Şeması



Çalışmada IOT cihazları ve SSL sertifikası kullanmayan ağ içi uygulamalarının verileri kolaylıkla alınabilmiştir. Amazon Alexa'ya göre dünyadaki Playlist, ExperienceProject ve Cozycot gibi en popüler 190 sosyal medya ağının 99 adedi SSL ile şifrelenmediği tespit edilmiştir (Friedl and Brodley, 1997). Bu da kullanıcının ister tarayıcıdan isterse uygulama içinden bağlandığı tüm verilerin elde edilebileceği anlamına gelir.

Şekil 2. Bağlı PCAP Alımının Pseudocode Gösterimi

```
frame [] dizi = null
Int dizi_sayac=0
boolean frame_son=false
while(frame.hasnext() && frame_son=true)
  if(filtres(frame)==true)
    dizi[dizi_sayac++]=frame
  end
end
String veri = null
Int i = 0
While i less than dizi length
  veri = veri + frame.getAttributes("HTTP","POST/response","Content")
end
If(isJson(veri)==true)
  Analizet(veri);
end
```

Alınan veriler kullanıcı isimleri, yorumlar ve ya mesajlar gibi metin içerikli olabildiğinin yanı sıra resim adresi de olabilir. Birçok sosyal medya resmi SSL ile şifreleyip göndermektense resmin o oturumID için üretilmiş bir adresi göndermektedir. Uygulamada ve tarayıcıda bu görüntü resminin adresini iletmektedir. Sistem PCAP'lardan topladığı görüntüsünün kodunu birleştirip uzantısını atamadan ve bulmaya gerek kalmadan windows medya görüntüleme aracı ile açabilmektedir. Buna karşın PCAP'den alınan oturumID'yi CURL gibi bir kütüphaneye tanıtarak bu ID ile ve görüntü adresi ile de görüntüyü çekebilmektedir. Sosyal medya tarafından üretilen adresler genelde tek kullanımlık adreslerin yanı sıra belirli bir

süre geçerli ve belirli bir oturumID ile çalışacak şekilde üretilirler. Bundan dolayı da oturumID ve adres bilindiğinde kolaylıkla ulaşılabilir durumdadırlar.

Çalışmada ağ kartlarını dinleyip PCAP'a ulaşmak için WinPcap programı kullanılmıştır (Lu et al., 2010). Çalışmanın ilk safhalarında Wireshark ile WinPcap'dan alınan veriler görsel olarak incelenmiş ve C# programı yazılırken hangi öznitelikleri alınacağı ve neye göre filtreleneceği bulunmuştur (Wang et al., 2010).

Çalışmanın son aşamasında ise WinPcap programının sağladığı PCAP'lar PcapDotNet açık kaynak kodlu kütüphanesi ile alınmış ve işlenmiştir (Pcapdotnet, 2016).

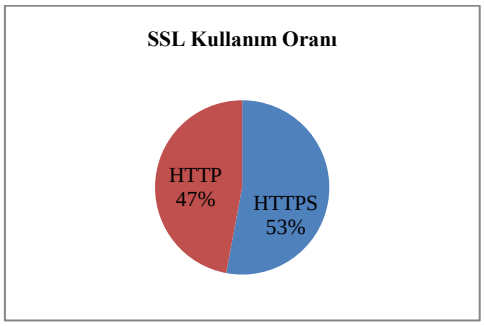
TARTIŞMA

Günümüzde sadece kurumsal ağlar ve kurumlar server üzerinden internet bağlantısı sağlamaktadır, birçok evde ve küçük kurumda direk modem üzerinden bağlantı sağlanmaktadır. Bu tür kullanıcılar ile kamu kullanımına sunulan açık ağlarda PCAP paketi toplamak için ağın izin vermesi ve ağı dinlemek gerekmektedir.

Alan adları genelde tarayıcıdan bağlanılan site sürümüne yönlendirilmektedir. API'ler ise harici bir alt-alan adında veya IP adresinde olabilir. Bu IP adreslerinin sisteme önceden tanımlanması gerekir, eğer API hizmeti veren server'ın IP adresi zamanla değişiyorsa, değişikliklerin sisteme uygulanması gerekir.

Facebook, Instagram, Twitter gibi birçok bilinen ve popüler sosyal medya API iletişiminde de HTTPS yani SSL kullanmaktadırlar (Lanjuan, 2006). Kullanım oranları şekil 3'de SSL kullanım oranı olarak verilmiştir. Bu sosyal ağlardan veri alırken şifrelemenin de kırılması gerekmektedir.

Şekil 3. SSL Kullanım Oranı



IOT'ler son yıllarda çok popüler olmuş ve kullanım alanları çok artmıştır, keza çoğu zaman aynı ağda bulunan uygulamalar kendi aralarında iletişimi şifrelememektedir (Kraijak and Tuwanut, 2015). En sık görülen örneği, bir hastane otomasyonu ile röntgen otomasyonu veya özlük haklarının tutulduğu personel otomasyonu arasında SSL şifreleme yapılmamaktadır. Bu tip durumlarda da ağdan paket toplanması halinde aradaki iletilen veri çözülebilir.

İleriye yönelik çalışmaya SSL şifrelemesini kıran kodlar eklenerek kapsamı geliştirilebilir. Buna karşında SSL kırma işlemi hesaba katıldığına sistemin gerçek zamanlı özelliği ortadan kalkacaktır (Lanjuan, 2006).

Uygulama sadece Windows Server işletim sistemine sahip server'larda çalışmaktadır. Bunun nedeni uygulamanın kullandığı platform '.Net' platformudur. Linux server'lar için PCAP toplayıcı ve PCAP çözücünün tekrar ve güvenilir bir şekilde yazılması gerekmektedir (Libpcap, 2016).

PCAP paketlerinin toplanmasını veya çözülmesini engellemek için başlıca çözüm gerek sosyal ağ API'lerini gerekse yerel ağda bulunan sistemlerin tüm iletişim kanallarının da SSL kullanmaktadır (Lanjuan, 2006).

Ağ üzerinde bulunan hub sayısını azaltmak ve güvenli router'lar devreye sokarak router ve ağ cihazlarını doğru ayarlamak diğer bir çözümdür (Jarray and Jaumard, 2005).

SONUÇ

Çalışma ağdaki PCAP paketlerini toplayarak, kullanıcıların sosyal ağ üzerindeki aldıkları ve ilettikleri verilerin kolayca elde edilebileceğini ve bu verilerin çözülebileceğini ortaya koymuştur. Yeni ve yaygın olarak kullanılan Restfull servisi üzerinden iletilen verilerin güvenliği ortaya konulmuştur. Sadece sosyal ağlarda değil, yerel ağda bulunan iki sistem arası iletişiminde eğer SSL gibi bir şifreleme mekanizması yoksa kolayca dinlenip çözülebileceği ve kişisel verilerin erişilebileceğini ortaya koymaktadır. Çalışmada kullanılan filtreler sayesinde kullanıcıların eriştikleri web siteleri ve içerikleri gerçek zamanlı okunabilmektedir. Bu çalışma, PCAP paketlerinin toplanmasının hem adli bilişim alanında hem de art niyetli bilgisayar korsanlarının kişisel verileri çalmak için kullanılabileceğini göstermektedir. İletişim ağına konulan verilerin ya da iletim yollarının güvenliğinin artırılarak, istenmeyen kişi veya kişilerin verilere erişiminin engellenmesi gerektiği ortaya konulmuştur.

KAYNAKÇA

Bilizzard Support. "Restfull Character", https://us.battle.net/support/en/article/200576, 25 Mayıs 2016.

Binti A. S., Selvakumar M. and Mohammed K. M., A Study on Packet Capture Mechanisms in Real Time Network Traffic, Advanced Computer Science Applications and Technologies (ACSAT) International Conference, 23-24 Dec 2013, Kuching, pp. 456-460.

Chen X. ve Chan X., Study on Layout Strategy of Transit Hub Network, Industrial Control and Electronics Engineering (ICICEE), 2012 International Conference, 23-25 Aug. 2012, Xi'an, 258-261.

Daiki C., Kazuhiro T., Tatsuya M. and Shigeki G., Detecting Malicious Websites by Learning Ip Address Features, Applications and the Internet IEEE/IPSJ on 12th International Symposium , 16-20 July 2012, Izmir, pp. 29-39.

Friedl M. A. ve Brodley C. E., "Decision tree classification of land cover from remotely sensed data," Remote Senss. Environ., vol. 61, no. 3, pp. 399–409, 1997.

Ibrahim G. and Vaclav P., DNS traffic analysis for malicious domains detection, Signal Processing and Integrated Networks on 2nd International Conference, 19-20 Feb 2015, Noida, pp. 613-918.

Iyer S. and MCKeown N. W., Analysis of the parallel packet switch architecture, IEEE/ACM Transactions on Networking, Apr 2013, 314-324.

Jarray A. and Jaumard B., Exact ILP solution for the grooming problem in WDM ring Networks, IEEE International Conference on Communications, 16-20 May 2005, 1708-1712.

Kraijak S. and Tuwanut P., A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends, 11th International Conference on

Wireless Communications, Networking and Mobile Computing, 21-23 Sept 2015, Shanghai, 1-6.

Lanjuan L., SCM Security Solution Based on SSL Protocol, 2006 IEEE International Conference on Service Operations and Logistics, and Informatics, 21-23 June 2006, Shanghai, 814-817.

Li Li, Wu Chou, Wei Zhou and Min Luo, Design Patterns and Extensibility of REST API for Networking Applications, IEEE Transactions on Network and Service Management , 12 Jan 2016, 154-167.

Libpcap. https://sourceforge.net/projects/libpcap/, 29 Mayıs 2016.

Lu X., Sun W. and Li H., Design and research based on WinPcap network protocol analysis system, 2010 International Conference on Computer, Mechatronics, Control and Electronic Engineering, 24-26 Aug 2010, Changchun, 486-488.

Meethaisong W. and Premchaiswadi W., Applying social network miner on medical event logs using handover of work metric, ICT and Knowledge Engineering (ICT & Knowledge Engineering 2015) 13th International Conference, 18-20 Nov. 2015, Bangkok, 116-120.

Pcapdotnet. http://pcapdotnet.codeplex.com/, 29 Mayıs 2016.

Razieh S., Ferhat K., Roch G. and Fatna B., A RESTfull architecture for enabling rapid development and deployment of companion robot applications, Computing, Networking and Communications (ICNC), 2014 International Conference on, 3-6 Feb. 2014, 971-976.

Sinha R. and Gupta S. C., Performance evaluation of a protocol for packet radio network in mobile computer communications, IEEE Transactions on Vehicular Technology, 33(3): 250-258.

Takeuchi Y., Okamoto T., Yokoyama K. and Matsuda S., A differential-analysis approach for improving SOAP processing performance, IEEE International Conference on e-Technology, e-Commerce and e-Service, 29 March- 1 April 2005, 472-479.

Waheed A. H. M. and Belaton B., Improving accuracy of applications fingerprinting on local networks using NMAP-AMAP-ETTERCAP as a hybrid framework, Control System, Computing and Engineering (ICCSCE) IEEE International Conference, 29 Nov.- 1 Dec. 2013, Mindeb, 403-407.

Wang S., Xu D. and Yan S., Analysis and application of Wireshark in TCP/IP protocol teaching, E-Health Networking, Digital Ecosystems and Technologies (EDT) International Conference, 17-18 April 2010, Shenzhen, 269-272.

Wang S., Xu D. and Yan S., Analysis and application of Wireshark in TCP/IP protocol teaching, E-Health Networking, Digital Ecosystems and Technologies (EDT), 2010 International Conference, 17-18 April 2010, Shenzhen, 269-272.