Adres Çözümleme Protokolü Zehirlenmesi (Address Resolution Protocol-ARP) Ağın Korunma Yöntemleri

Mehtap Erdil[1], Ayşenur Erdil[2]

[1] Marmara Üniversitesi, Çevre Mühendisliği Bölümü, İstanbul

[2] Yalova Üniversitesi, Endüstri Mühendisliği Bölümü, İstanbul

erdilmehtap@gmail.com, aysenurerdil@gmail.com

Özet: Yönlendiriciler bünyelerine ulaşmış IP paketlerin varış adreslerini dikkate alarak bu bilgi ışığında paketi bir sonraki düğüme node'a gönderirler fakat bu aktarım sırasında paketlerin farklı özelliklere sahip alt ağlar

üzerinden geçebilme durumları olabilmektedir. Ethernet ortamında üretin bir paket bir FDDI ağından, bir sonraki adım olarakta bir ATM ağından geçebilir. Üst kısımdaki IP yapısını destekleyen alttaki ağlar fiziksel ağlar (ya da alt ağlar) olarak adlandırılabilir. Fiziksel ağların kendilerine yönelik adresleme ve şablon mekanizmaları mevcuttur. Bu adres bilgisi üretim-proses zaman diliminde bir daha değişmeyecek biçimde Ethernet kart elemana şifrelenerek kaydedilir.

Bu adres bilgisine donanım adres bilgisi ya da mac (medium access control) adres bilgisi de denir. Bu koşullar altında bir IP paketi geçtiği her fiziksel ağ üzerinde o ağın kapsamı alanı içine yerleştirilir ve varış IP adres bilgisine ulaşma koşulları içerisinde fiziksel ağ içinde ilerleyerek hedefine varış adresine ulaştırılır. Bu çalışma kapsamında kablosuz ağ güvenliğinin sağlanması yönünde Adres çözümleme protokolü zehirlenmesi hakkında bilgi verilmiş ve Ethernet Ağın korunması yöntemlerine değinilmişti.

Anahtar Sözcükler Kablosuz ağ (Wi-Fi),Güvenlik, Ethernet, Lan(Yerel Ağ)

Address Resolution Protocol Poisoning-ARP-Network Security Methods

Abstract: Routers send IP packet to the next node via looking the destination address of the

IP , but it can be said that have different characteristics during the transfer of packets subnets to pass through. A package has been created in Ethernet environment, firstly passing from a FDDI network, then passing an ATM network. it can be said physical networks (or subnets) that support the upper structure of IP networks. Their own physical network also has an addressing mechanism and framework. For example, an Ethernet address of each computer connected to the Ethernet network has. This address will not change during production are recorded on the Ethernet card.

This address is the physical address, hardware address or MAC (Medium Access Control) address is called. In this case, an IP packet every occurrence of the physical network that the network's frame into the subject and destination IP address, you can reach within a physical network .The study of wireless network security in the provision of Address resolution protocol poisoning given information about and Ethernet network protection methods had been mentioned.

Keywords: Wireless network (Wi-Fi), Security, Ethernet, LAN (Local Area Network)

1. Giriş

Günümüzde güvenlik kapsamında akıllara önce güvenlik duvarı (Firewall) geliyor. Bu durum altında güvenlik duvarı ile sadece internetten gelen saldırılara karşı önlem alınmaktadır.

Yerel alan ağ kapsamına girme amaçlı korsanlar doğrudan anahtara bir ağ kablosu ile kendini bağlıyor ya da kurumun kablosuz ağını (Wi-Fi) kullanır. Bu tür saldırı durumlarında güvenlik önlemi ise anahtarlarla sağlanır[27].

Günümüz ağ yapısında kurumsal işletmelerin büyük kısmı, bu tarzdaki saldırılara açık olduğunu söylemek mümkündür.Kimseye farkettirilmeden bu tarz saldırılar, işletme bünyesindeki ağlara yapılmaktadır. Şu anki bir çok işletme kapsamındaki BT yönetici ve organizatörler ağ güvenliğininisadece güvenlik duvarı ile sağlandığını düşünmektedir. Önemli olan unsur iç bünyedeki iletişim bilgi ağın güveliğinin en üst düzeyde sağlamaktır.İnternal kapsamda yapılan saldırılar daha kolay yapılmakta ve saldırının yerinin belirlenmesi daha zordur. Belirtilen sebeplere bağlı olarak local kapsamdaki yerel ağ güvenliğine daha çok önem verilip, çalışmalar bu kapsamda arttırılması gerekir. [10,11,27].

Gelişen güvenlik duvarı yazılımlarıyla işletme bünyesinde internet ağı üzerinden güvenlik duvarını geçmek zorlaşmıştır, bu bağlı olarak korsanlar (Hacker) uygulama takdiği değiştirerek yapılacak saldırıları direk iç bünyede yerel alan ağ üzerinden yapmaya başlamışlardır. Bu uygulamayla korsanlar yerel alan ağına ulaştıklarında güvenlik duvarındaki alınmış önlemler etkisiz hale gelmekte ve yerel alan ağ kapsamında bütün elemanlar saldırıya açık olup, ağ Güvenliği minumum seviyeye inmiş olmaktadır[8,9].

LAN kapsamına sızan kötü amaçlı kişi anahtar kapsamındaki tüm clientlerdaki şifrelenmemiş her türlü ağ trafiğini rahatça dinleyebilmekte ve üzerinde değişikliklere yapabilmektedirler. Bu alandaki çalışmalar, yerel ağ alanından gelen tehlike içeren saldırı oranının yüzde 60 ve bu oranı geçtiğini göstermektedir.

Kötü amaçlı kişilerin yani korsanların işletme kapsamındaki ağa bağlanma amacı için kullanılmayan veya kişisel bilgisayarın ağ kablosunu kendisine bağlaması veya kablosuz ağ bünyesinde bağlanması yeterli olmaktadır.Böylece ağ üzerindeki her türlü bilgi akışına müdahale edebilmekte ve ağları dinleyebilmektedir[22,25].

Ağlara saldırılar kolaylaşınca bu kapsamda yapılan kötü amaçlı uygulamalar artış göstermektedir.Yerel alan kapsamında olası saldırılara örnek vermek gerekirse en sık karşılaşılan ARP Zehirlenmesi verilmektedir.

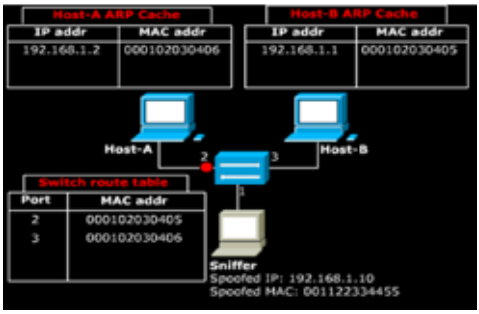
2. ARP (Address Resolution Protocol)

Yerel ağların oluşturulup her türlü bilgi akışını sağlama yönünde çoğu çalışma alanında en çok başvurulan ve kullanılan ağ arayüzü Ethernet'tir.Sistem kapsamına Ethernet arayüzü elemanı olarak kullanılan ağ kartları eklenerek LAN kapsamına kolayca erişilebilmektedir.

Ethernet arayüzleri karşılıklı iletişimi sağlama yönünde, iç bünyelerinde üretim proses aşamasında oluşturulana fiziksel adresleri kullanırlar; 48 bit olan bu ara yüzlerde ilk 24 bit üreticiyi gösterir ve 48 bitlik bloğun eşi bulunmamaktadır. . TCP/IP protokolü bünyesindeki ağlarda 32 bit olan IP adresi kullanılmaktadır.

Şekil 1. Adres Çözümleme Protokolü

Fiziksel katmanda Şekil 1 'de gösterildiği gibi Ethernet ara yüzü bulunuyorsa, IP adresten fiziksel adrese dönüşüm yapılması zorunludur. Bu sağlayabilmek için de sistemlerde adres çözümleme protokolü olarak Şekil 2 'de örnek olarak gösterildiği gibi kullanılan ARP(Address Resolution Protocol) ve ARP tablolarına başvurulur.



Şekil 2. ARP Zehirlenmemiş Normal Trafik

2.1 ARP İstek ve Cevap Paketleri

Bir IP paketini yer ağ kapsamında sisteme gönderilip iletilmesi için IP adres bilgisinin yanında donanımsal adres bilgisine de ihtiyaç duymaktadır. IP (Internet Protokol) kapsamında , fiziksel adresin öğrenilmesi doğrultusunda yerel ağ içinde bulunan tüm bilgisayarlara özel olarak sorgulama paketi gönderir[27].

ARP(Adres Request Packet) istek paket olarak bilinen bu bilgi pakette alıcı taraftaki sistemin adres bilgisi bulunur ve buna bağlı olarak fiziksel adres bilgisinin gönderilmesi talep edilir. Ağ bünyesindeki tüm ARP'ler, aktif olan düğümlerce bu talep edilen paketleri görür. Talep paket bilgisini gönderen yerel fiziksel adres bilgilerini de gönderebilirler[1,3].

Ağ içindeki bazı düğümler, fiziksel adres öğrenme zamanını kısaltma yönünde diğer sistemlere ait ARP sorgulamalarını dinleyebilirler ve böylece kendilerine ait ARP tablo bilgilerini güncel tutmuş olurlar.

Buna ek olarak ARP, IP adres bilgilerinin fiziksek adres kapsamında haritalanmaları dışında kendine özel donanım türlerine de izin verebilirler. Şekil 3 ve Şekil 4 'de ARP isteği ve cevabı gösterilmektedir.

2.2 ARP Paket Formatı

İhtiyaç durumlarına bağlı olarak mesajlaşmaları sağlama yönünde bir ARP mesaj format yapısı oluşturulur. Oluşturulan bu mesaj format yapısı olası protokol yönünde fiziksel/donanımsal yönden adresin çözümlenmesini hedeflemiş olsa da genel olarak IP ağları bünyesinde Ethernet adreslerine ulaşabilme yönünde kullanılması hedeflenmiştir.

Donanım Adres Tipi: Her bir veri hattı katman protokolüne bu alanda kullanması için verilen numara. Örneğin Ethernet 1.

Protokol Adres Tipi: Her bir protokole bu alanda kullanılması için verilen numara. Örneğin, IP 0x0800.

Donanım Adres Uzunluğu: Donanım adresinin byte cinsinden uzunluğunu gösterir. Ethernet adresi 6 byte uzunluğundadır.

Protokol Adres Uzunluğu: Logical Adresin byte cinsinden uzunluğu. IPv4 adresi 4 byte uzunluğundadır.

Operasyon: Gönderici belirli operasyonları sergiler: istek için 1, cevap için 2, RARP isteği için 3 ve RARP cevap için 4.

Gönderen Donanım Adresi: Donanım adres gönderici.

Gönderen Protokol Adresi: Göndericinin protokol adresidir[23,24].

Varış Donanım Adresi: Alıcıya yönelik donanım adresi. Bu alanda istekler önemsenmez.

Bir istek mesajı gönderilirken Varış Donanım Adresinin tamamı sıfır yapılır.

Varış Protokol Adresi: Alıcıya yönelik protokol adresidir.

Şekil 3. ARP Request[3-6]

Şekil 4. ARP Reply[3-6]

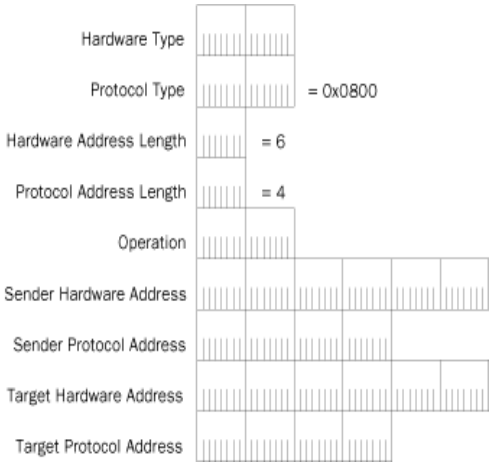
2.3 ARP Mesajının İşlenmesi

1)Mesajın ilk geldiği zaman diliminde düğüme ait IP adresi ve MAC adreslerinin ARP'ye ait cep belleği kısmında olup olmadığı testi yapılır. Eğer bu bilgi mevcutsa eski donanım adresinin yerine, gelen yeni mesaja ait donanım adres bilgisi yazılır.

2) Mesaja ait operasyon işlemlerinin yapıldığı kısma bakılır. Bu bölümde istek mesajı varsa buna yönelik cevap mesajı hazırlanıp, gönderilir. Cevap mesajı formatında, gelen mesajdaki gönderen ve varış adreslerinin yerleri değiştirilir. Gönderen donanım adresi bölümüne ait kısma mesajı hazırlayan bilgisayarın donanım adres bilgisi yazılır. Operasyon alan kısmına , 2 değeri verilir.

Hazırlanmış olan bu cevap mesajı ise önceden istek olarak gönderilmiş olan gelen bilgileri cep bellek kısmına eklenir.

Yayınlanmış tüm ARP mesajlarında verilen ARP cep belleğine yerleştirilmesi, cep belleğin kısa zaman dolmasına sebep olabilmektedir.. Bu sebepten dolayı, bilgisayarlar sadece kendilerini hedef alan ARP mesajlarına yönelik işlem yaparlar[4,6,7,8].



Şekil 3. ARP Paket Formatı[24]

2.4 RARP
(Reverse Address Resolution Protocol)

RARP, yeni çalışmış bilgisayarlar üzerinde yeni çalıştırılmış (new-booted) bilgisayarların Ethernet adreslerinin ağa duyurulmasını ve kendi IP adresinin sorulmasını sağlar. Bu kapsamdaki bilgisayarlar disksiztir ve RARP sunucusu ilgili sorulara cevap verir. IP adresinin yerel ağı dışına çıkamaması sorununu çözmek amaçlı alternatif olarak başlangıç protokolü (bootstrap) önerilmiştir:

BOOTP, UDP mesajları ile haberleşir ,buna bağlı olarak yerel ağlardan geçebilir. BOOTP'nin detayları RFC 951,RFC 1048 ve RFC 1084'te verilmiştir. BOOTP'a dezavantaj olarak IP ve Ethernet adres eşlemesinin manuel olarak yapılması verilebilir [13,15].

ARP ve RARP birbirinden farklı, bağımsız işlemlerdir. ARP, her sunucunun kendi donanım adresi ve protokol adresi arasındaki haritalamayı bildiğini tahmin eder. Bütün sunucular aynı durumdadırlar.. İstemci ve sunucu arasında hiçbir ayrım yoktur. RARP' de ise durum biraz farklıdır. Bu aşamada, İstemcilerden gelen istekleri cevaplamak ve protokol adresinden donanım adresine veritabanı haritalanması için daha çok sunucuya ihtiyaç duyulmaktadır [2,13].

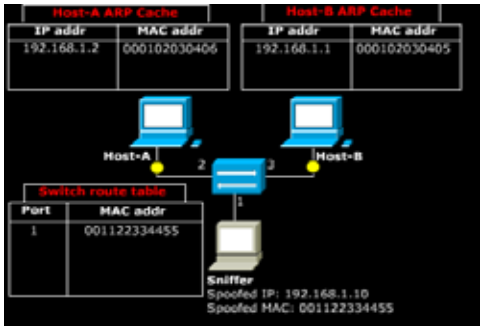
4. ARP Zehirlemesi

Eski zamanlarda ARP zehirlemesi yapmak zordu ve kapsamlı şekilde ağ ve donanım bilgisi gerekiyordu. Ancak günümüzde internetten indirilebilen ücretsiz ve kullanımı çok kolay yazılımlar sayesinde bu saldırı çok kolay hale gelmiştir. ARP zehirlenmesi kapsamında saldırıda bulunan bilgisayar ağ trafiğini kendi üzerine alıyor ve bu trafiği izleyebilir duruma geliyor. Bu koşullar altında şifresiz giden MSN konuşmalarından dosya transferine kadar her türlü "text" kapsamındaki bilgiler kolayca izlenebilmektedir. Aynı şekilde şifrelenmemiş, SSL(Service Security Layer) kullanmayan siteleri, şifrelenmemiş POP3 e-posta parolaları saldırıyı yapan bilgisayar tarafından kolaylıkla izlenebilmektedir[9,27].

İzlenen trafik şifrelenmiş olsa bile bunu izleyenler parolaları kırmak için kullanılan programları kullanarak bu şifreler çözebiliyor. Sonuçta bilgi casusluğunun yanında endüstri casusluğu işten bile olmuyor.

4.1 ARP Zehirlemesi Nasıl Yapılır?

ARP zehirlemesi, temel olarak bilgisayarların ARP önbelleğinin değiştirilmesi ile ağda dolanan verilerin ele geçirilmesidir. Veri alışverişi iki host arasında yapılacakken zehirlenmiş bir ağda, veri kaynaktan çıktıktan sonra dinleyiciye uğrar daha sonra hedefe yönlendirilir. Bu işlem üç aşamada gerçekleştirilir. Bu işlemlerin sonucunda da ağ trafiği aşağıdaki resimde olduğu gibi manipüle edilmiş hale gelir[5,10].



Şekil 4. ARP Zehirlenmesi

4.1.1 Pasif Dinleme

Bu aşamada dinleyici ağda hiçbir zararda bulunmaz. Kendisine ulaşması istenmeyen bir veriye de ulaşamaz. Sadece ağda yayın (broadcast) yapılan verilere ulaşabilir. Bu aşama en önemli aşamalardan birisidir. Kullanıcı ağa yayın şeklinde gönderilen ARP istek paketlerini dinler ve bu sayede tüm hostların IP ve MAC eşleşmelerine ulaşır. Bu eşleşmeleri de daha sonra kendisine gelen verileri doğru hedeflerine göndermede kullanacaktır [13,15].

4.1.2 Zehirleme

Ağdaki tüm IP-MAC eşleşmelerini öğrenen dinleyici, artık harekete geçmeye hazırdır. Hedef hostlara ARP reply paketleri göndererek, ARP ön belleklerini kendi isteği yönünde değiştirir. Bu aşamada genellikle ağda bulunan hostlara internete çıkış sağlayan IP adresi ile ilişkili olan gateway'in MAC adresi olarak dinleyicinin MAC adresi gösterilir. ARP protokolünde herhangi bir doğrulama işlemi olmadığından bu paketleri alan bilgisayarlar veriyi doğru olarak kabul eder. Bu aşamanın tamamlanması ile zehirleme işlemi tamamlanmış ve ARP ön bellekleri değiştirilmiş olur[6,7,8].

4.1.3 Aktif Dinleme

Hedefteki kullanıcının ARP ön belleği manipüle edildiği için artık internete göndermek istediği veri doğrudan dinleyiciye gelecektir. Aktif dinlemede en önemli nokta kullanıcının veri iletişimin kesilmemesi için gelen veriyi yeniden yönlendirmektir. Bu yeniden yönlendirme

işlemi de pasif dinleme aşamasında toplanan veriler sayesinde gerçekleştirilir[16,17,18].

5. Ağın Korunması

İlk önlem en uçta yönetilebilir ve bu tarz saldırılara karşı güvenlik önlemlerine sahip anahtar (Switch) kullanmasıdır. ARP zehirlenmesine karşı anahtarlar, üzerindeki Mac adresleri ve IP adreslerinin eşleştirildiği bir tablo tutabilirler. Bu tabloya uymayanların ya da bunlardan herhangi birini değiştirenlerin ağla ilişkisi kesilebilir. Buna ek olarak gelen her pakette kontrol yapılarak korsanların isimlerini gizlemek amacıyla Mac adreslerini değiştirerek Mac spoofing yapmaları engellenir[14,26].

Anahtarlar, DHCP (Dynamic Host Configuration Protocol) Snooping'i önleme amacıyla sistemde bulunan DHCP sunucunun belirlenen portlarda çalışmasını veya buna ek olarak yalnızca belli bir IP'den gelmesi sağlayabilir. Böylece sahte DHCP'ler engellenir. [18,19,20].

Bazı kurumlar yerel alan ağına sızıntıları önlemek için kurumun içine ziyaretçilerin hiç birinin cep telefonu ya da dizüstü bilgisayar sokmalarına izin verilmez. Bu önlemin üzerine yabancı bir bilgisayar ağa bağlanma durumunda, bilgisayar anahtar tarafından kontrol edilerek ağa kabul edilmez ve sistem yöneticisine durum hakkında bilgi verilir[20,23,27].

Çok bilinen saldırı yöntemlerinin dışında bazı anahtarlar ve kablosuz vericiler üzerinde istemcilerin birbiriyle haberleşmesi de önlenebilir. Bu kapsamda anahtar üzerindeki her port ayrı hareketi sağlamayı ve sadece kendini ve internete çıkartan yönlendiriciyi görmeye başlar. Bu kapsamdaki yazılımlar arasından ömür boyu ücretsiz yazılım yükseltimi sağlama imkânı sunanlar vardır. Bu imkan sayesinde yeni saldırılara karşı her güncelleme aşamasında ağ yöneticisi bilgi verilerek, istediği anda internet üzerinden güncellemeyi indirerek anahtara yüklemesi sağlanabilir[13,24,25].

6. Sonuç

ARP zehirleme işlemi yapmak günümüzde çok kolay bir duruma gelmiştir. İnternet ortamından indirilecek basit kullanımlı birkaç uygulama ile bilgisayar ağları ile ilgili geniş bilgiye sahip olmadan da bu tarz bir saldırı gerçekleştirilebilir. Dışarıdan gelebilecek saldırılara bu kadar koruma sağlamaya çalışırken ağ içerisinden gelebilecek saldırılar genellikle göz ardı edilmektedir. Halbuki başarılı bilgi çalma saldırıları genellikle yerel ağ üzerinden gerçekleşmektedir. Birçok büyük şirket de dahil olmak üzere yerel ağların çoğu bu saldırılara açık durumdadır. Kullanılacak layer-3 switch'ler aracılığı ile bu saldırıların önüne geçilebilir. Bu sayede ağımızın yani sanal ortamdaki tüm bilgilerimizin güvenliği sağlanmış olur. Geleceğe yönelik çalışmada Adres Çözümleme Protokolün performansının daha güvenilir ve daha hızlı olması yönünde yeni tasarım, çalışmalara odaklanması yönünde çalışmalar yapılabilir.

5. Kaynaklar

[1] Atay Saib, Bitirme Ödevi, CISCO Ağ Akademisi-1, Fırat Üniversitesi, Elazığ, 2006.

[2] B.M. Waxman, Routing of multipoint connections, IEEE Journal on ,Selected Areas in Communications 6 (9) (1988) 1617–1622.

[3] Balık H.Hasan, Ayhan AKBAL, TCP/ IP'nin Dünü Bugünü Yarını, Fırat Üniversitesi, Elazığ.

[4] Dirican, Can Okan, TCP/IP ve Ağ Güvenliği, Açık Akademi Yayınları, İstanbul, 2005.

[5] Craig L., Esther H.-Kwan Y. ,Edwin H.-Wan C., The application of ARP modelling to adaptive reuse projects in Hong Kong, Habitat International 40 (2013)

[6] D. Bruschi, A. Ornaghi, E. Rosti, S-ARP: a secure address resolution protocol, in: Proc. of Annual Computer Security Applications Conference (ACSAC), 2003.

[7] Deering S, Hinden R. Internet Protocol, Version 6 (IPv6) Specification. Dec., 1998.

[8] Gratuitous ARP – The Wireshark Wiki. <http://wiki.wireshark.org/Gratuitous_ARP>.

[9] http://www.hasanbalik.com/dokuman.asp/

[10]http://www.muratyildirimoglu.com/makaleler/TCPIPyiKesfedelim.htm/

[11] http://www.protocols.com/

[12]I.Teterin,Antidote.<http://online.securityfocus.com/archive/1/ 299929>.

[13] K. Levenberg, A method for the solution of certain non-linear problems in least squares, Quarterly of Applied Mathematics 2 (1944) 164–168.

[14] Kılıç Zeynep, Teknik Öğretmen Ders Notları, 2004.

[15] Matthew S, Jacob K P. A new fast stream cipher: MAJE4. In: 2005 Annual IEEE on INDICON. Chenrai, India, 2005: 60-63.

[16] N. Spring et al., Measuring ISP topologies with rocketfuel, IEEE–ACM Transactions on Networking12(1)(2004) 2–16.

[17] Neminath H., Santosh B., S. Roopa, Ritesh R., Sukumar N., LAN attack detection using Discrete Event Systems, ISA Transactions 50 (2011) 119–130

[18] Özkaya İsmail, Teknik Öğretmen Ders Notları, 2004.

[19] R. Philip, Securing Wireless Networks from ARP Cache Poisoning, Master's Thesis, San Jose State University, 2007.

[20] S. Kent, R. Atkinson, IP Encapsulating Security Payload (ESP) (RFC2406), 1998.

[21] S.Y. Nam, D. Kim, J. Kim, Enhanced ARP: preventing ARP poisoningbased man-in-the-middle attacks, IEEE Communications Letters 14 (2) (2010) 187–189

[22] Seung Y., Sirojiddin D., Minho P., Collaborative approach to mitigating ARP poisoning based Man-in-the-Middle attacks, Computer Networks 57 (2013) 3866–3884

[23] V. Goyal, R. Tripathy, An efficient solution to the ARP cache poisoning problem, in: Proc. of Information Security and Privacy, 2005.

[24] W. Lootah, W. Enck, P. McDaniel, TARP: ticket-based address resolution protocol, Computer Networks 51 (15) (2007) 4322–4337.

[25] Y. Guang, B. Jun, X. Peiyao, Source address validation solution with OpenFlow/NOX architecture, in: 19th IEEE International Conference on Network Protocols (ICNP), 2011.

[26] Dr. Sema Oktuğ, İTÜ Bilgisayar Mühendisliği Bölümü, BLG433-Bilgisayar Haberleşmesi ders notları,

[27] Refiksamet.com/
documents/02142013033113.pdf
(Erişim Tarihi :10 Ocak 2014.