KABLOSUZ AĞLARIN GÜVENLİK AÇIKLARININ EĞİTİM AMAÇLI İNCELENMESİ İÇİN UYGULAMA TASARIMI

Deniz Mertkan Gezgin[*]
Ercan Buluş[**]

ÖZET

Bilişim ve internet güvenliği özel sektör ve kamu kuruluşları yanında eğitim merkezleri ve okullarda da günden güne önemi artan bir konudur. Üniversite yerleşkelerinde ve okullarda kurulan yerel alan ağlarına (LAN-Local Area Network), kablolu ya da kablosuz alt yapıda olsa birden çok saldırı düzenlenmektedir. Daha önce kablolu ağlarda yapılan bazı saldırılar, kablosuz ağlarda da kullanılmaya başlanılmıştır. Bunlardan en önemlisi Servis Reddi (DoS-Denial Of Service) saldırılarıdır. DoS saldırıları kullanılan ağdaki dağıtıcı cihazlara veya bant genişliğine yapılmaktadır. Bunun ana sebebi ağ protokollerinin temelinde yatan açıklardır. Ev ve genel kullanım alanına sahip kablosuz ağlarda, bu zaafları kullanan saldırı teknikleri ile yapılan DoS saldırılar başarılı olmaktadır. Bilgi ve iletişim teknolojilerinin etik ve güvenli kullanımı konusunda Bilişim Teknolojileri Öğretmenlerinin bilgi sahibi olmaları gereklidir. Ayrıca bu bağlamda gerek öğrencilerini gerekse iletişim halinde oldukları sosyal çevrelerini bilgilendirmeleri, bilinçlendirmeleri gerekmektedir. Bu nedenledir ki Bilişim Teknolojileri Öğretmen ve öğretmen adaylarının alanları ile ilgili kuramsal ve meslek bilgisi derslerinin yanı sıra teknik temelli alan derslerinde bilgi ve iletişim teknolojileri tabanlı güvenlik sorunlarına yönelik bilgiler de edinmeleri bir tür zorunluluk haline gelmiştir. Bu çalışmada Trakya Üniversitesi Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Eğitimi (BÖTE) Bölümü öğretmen adaylarının internet ve ağ güvenliği konusunda bilgilendirilmesi için protokol zaaflarını kullanarak bir kablosuz ağ saldırı için UDP (User Datagram Protocol) taşma atağı (Flood Attack) uygulaması yapılmıştır.

1.Giriş

Kablosuz ağlar günümüzde yoğun olarak kullanılmaktadır. Bunların tercih edilmesinin temel sebepleri, kablodan bağımsız taşınabilirlik sağlaması ve kablolu ağ gibi yüksek erişim hızlarına sahip olmasıdır. Kablosuz ağlarda kullanılan standart Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE-Institute of Electrical And Electronics Engineers) 802.11 a/b/g/n kablosuz ağ standardıdır [4]. Bu gelişmeler doğrultusunda evlerde olsun, genel internet kullanılan alanlarda kablolu ağların devri yavaş yavaş sona ermektedir. Kablosuz ağların kullanım alanları arttıkça, güvenlikte de bazı problemler oluşmaya başlamıştır. Saldırganlar kablosuz ağların şifrelerini kırmak, internet erişimini engellemek veya tüketmek için bazı saldırı

[*] Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Trakya Üniversitesi, EDİRNE mertkan@trakya.edu.tr

[**] Bilgisayar Mühendisliği Bölümü, Çorlu Mühendislik Fakültesi, Namık Kemal Üniversitesi, Çorlu-TEKİRDAĞ ercanbulus@nku.edu.tr

teknikleri kullanmaktadır. Kablosuz ağlara yapılan en ilginç saldırılar şifre kırmak için yapılanlardır. Kabloluya Eşdeğer Gizlilik(WEP- Wired Equivalent Privacy) ve Wi-fi Korumalı Erişim (WPA-Wi-Fi Protected Access), Mac Adres filtreleme gibi WPA2 öncesi güvenlik standartları saldırılara karşı zayıf kaldığından saldırıları engellemek için AES (Advanced Encryption Standard) algoritması kullanan WPA2 şifrelemesi kullanılmaya başlanmıştır [7,15]. Kablosuz ağlara diğer çok yapılan saldırı türü DoS saldırılarıdır. Saldırıların temel amacı ağın bant genişliğini veya cihazların hafızasını tüketmektir. DoS saldırıları bunun için ağ tasarımının zaaflarını kullanmaktadır. Saldırılardan bazıları TCP (Transmission Control Protocol) ve UDP protokollerini kullanarak yapılan taşma saldırılardır [9].

2.DoS Atakları

DoS saldırılarında, saldırgan legal istemcilerin bilgi erişimi ya da servislere erişimini engellemeye çalışır. Hedef bir cihaz, bilgisayar; ağ bağlantınız, site erişimi olabilir. Örneğin Amazon.com adlı siteye 2000 yılında yapılan bir DoS saldırısında Site sunucusu (Server) 20 dakika servis dışı olmuştur. Süreç şöyle işlemektedir: Kullanıcılar siteyi görüntülemek için site sunucusuna istek gönderirler, sunucu bu isteklere cevap verir, saldırgan bu istekleri devamlı göndererek sunucuya yük bindirir, bir süre sonra sunucu işlem yapamaz hale gelir. Kısacası kaynaklarını tüketir. Siteye bir süre erişim yapılamadığından bu saldırı DoS saldırısı olarak nitelenir. DoS saldırıları spam e-posta mesajları da kullanarak, kotaları şişirip, diğer mesajların kullanım alanını bitirebilir ya da elektronik posta sunucusunu (e-mail sever) devre dışı bırakabilir [6]. DoS Saldırısı belirtileri:

a. Alışık olunmayan düşük ağ performansı

b. Web sitelerinin belli bölümlerinin kullanılamaması

c. Bir Web sitesine erişmede güçsüzlük

d. Email kutusundaki spam emaillerinin artışı [10]

2.1. DoS Atak Türleri

Son günlerde kablosuz ağlara yönelik pek çok saldırı geliştirilmektedir. Bu saldırılar için DoS saldırı çeşitleri de mevcuttur. DoS saldırılarının temelinde yatan amaç yukarıda anlatıldığı gibi cihazı ya da ağı protokolün kullandığı veri paketlerine boğmaktır. Yani taşma tekniği kullanmaktır. Bu taşma saldırılarından önemli olanlarını maddeler halinde sıralarsak;

- **Tcp/Syn Taşması Saldırısı,** Bu saldırı türü klasik bir DoS saldırısıdır ve modern ticari bilgisayar sistemlerinde bu saldırılara karşı önlemler alındığından fazla etkili değildirler. Bu saldırı tekniğine göre hedef sisteme gelen Syn (Synchronize) paketleri hedef sistemin hafızasını doldurur. Hafızası dolan sunucu diğer sisteme bağlı istemcilere servis veremez duruma gelir.[5]
- **UDP Taşması Saldırısı,** Udp hızlı, ancak güvensiz bir iletişim protokolüdür. Gönderici bilgisayar veriyi gönderir ancak verinin ulaşıp ulaşmadığını

kontrol etmez. Bu saldırı hızın önemli olduğu durumlarda tercih edilir. DoS saldırısı için Udp'yi kullanmak Tcp kadar kolay değildir. Udp Taşma saldırısı uzaktaki erişim noktası üzerinde ki rastgele portlara büyük değerli Udp paketleri göndererek saldırı yapabilir [1.] Genel mantığı sahte olarak üretilen IP (Internet Protocol) adreslerinden paket yollamaktır. Örneğin bir bilgisayara taşma saldırısı yapılıyorsa verinin doğru gidip gitmediğinden çok, verinin çabuk gidip gitmediği hesaplanır.

- **Ping Taşması Saldırısı,** Ping taşması temel bir DoS saldırı türüdür. Bu tekniğe göre saldırganlar kurban sistemlere büyük boyutta (64 KB) ICMP (Internet Control Message Protocol) paketleri göndererek sistemin bant genişliğini doldururlar. Böylece ağ iletişimini sabote ederler. Buna örnek Ping of Death atağıdır. Ping of Death atağı, Ping uygulamasını kullanarak IP tanımlamasında izin verilen büyüklüğü aşan 65535 byte IP paketleri oluşturur. Daha sonra normalden büyük paket ağa gönderilir. Sistemler çökebilir, durabilir veya kapanıp açılabilir [8].
- **802.11 Associate/ Authenticate Taşması Saldırısı,** Erişim Noktasının ağa dahil olma (association) tablosunu doldurmak için rastgele Mac adresleri üzerinden Kimlik doğrulama ve Ağa Dahil Olma istekleri göndererek zorlama yapar.
- **802.11 Beacon Taşması Saldırısı,** istasyonların yasal bir erişim noktası bulmasını zorlaştırmak için binlerce sahte beacon üretirler.
- **802.11 Deauthenticate Taşması Saldırısı,** erişim noktasından kullanıcıları bağlantısını düşürmek için kimlik doğrulama ve ağ üye olmama istekleri ile zorlama yapar.[9]

3.Udp Protokolü[13]

Udp, Tcp/Ip protokol takımının iki aktarım katmanı protokollerinden birisidir. Verileri bağlantı kurmadan yollar. Gelişmiş bilgisayar ağlarından olan paket anahtarlamalı bilgisayar ağlarında iletişim oluşturabilmek için Udp protokolü yazılmıştır. Bu protokol minimum protokol mekanizmasıyla bir uygulama programından diğerine mesaj göndermek için kullanılır. Paketin teslim garantisini isteyen uygulamalar Tcp protokolünü kullanır. Özellikleri:

- Geniş alan ağlarında (WAN-Wide Area Network) ses ve görüntü aktarımı gibi gerçek zamanlı veri aktarımlarında Udp kullanılır.
- Udp bağlantı kurulum işlemlerini, akış kontrolü ve tekrar iletim işlemlerini yapmayarak veri iletim süresini en aza indirir.
- Udp ve Tcp aynı iletişim yolunu kullandıklarında Udp ile yapılan geçek zamanlı veri transferinin servis kalitesi Tcp'nin oluşturduğu yüksek veri trafiği nedeniyle azalır.

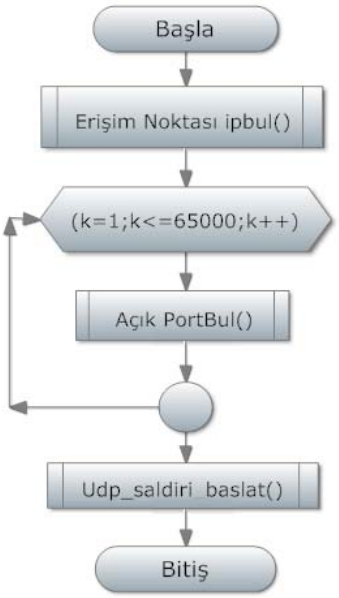
Udp'yi kullanan protokollerden bazıları; Dns(Domain Name Server), TFtp(Trivial File Transfer Protocol), Arp(Adress Resulation Protocol), RArp(Reverse Adress Resulation Protocol) ve Snmp protokolleridir. Uygulama programcıları birçok zaman Udp'yi Tcp'ye tercih eder, zira Udp ağ üzerinde fazla bant genişliği kaplamaz.

Udp güvenilir olmayan bir aktarım protokolüdür. Ağ üzerinden paketi gönderir ama gidip gitmediğini takip etmez ve paketin yerine ulaşıp ulaşmayacağına onay verme yetkisi yoktur. Udp üzerinden güvenilir şekilde veri göndermek isteyen bir uygulama bunu kendi yöntemleriyle yapmak zorundadır [13].

4.Udp Taşma Saldırısı

4.1.Geliştirilen Saldırı Tasarımı

Udp Saldırısı için yapılan uygulama Visual Basic Görsel Programlama dili ile Winsock.dll [2,14] kullanılarak yazıldı. Programın başlangıcında ağ geçidi ya erişim noktasının IP numarası bulunulmaktadır. Programın devamında Erişim noktası üzerinde açık olan portlar bulunulmaktadır. Bulunan port numaraları bir diziye atılmaktadır ve açık port kontrolü 65000 değerine kadar yapılmaktadır. Açık portlar bulunduktan sonra istenilen soket sayısı ve zaman aşımı süresinde açık portlardan Udp paketleri gönderilmeye başlanıldı. Böylece Erişim noktasının Udp paketlerine boğulmasına sebebiyet verildi ve diğer legal istemcilerin internete çıkışlarında yavaşlama ve kesilmeler olduğu görüldü. Geliştirilen saldırının akış diyagramı şekil 1'de de gösterilmektedir.



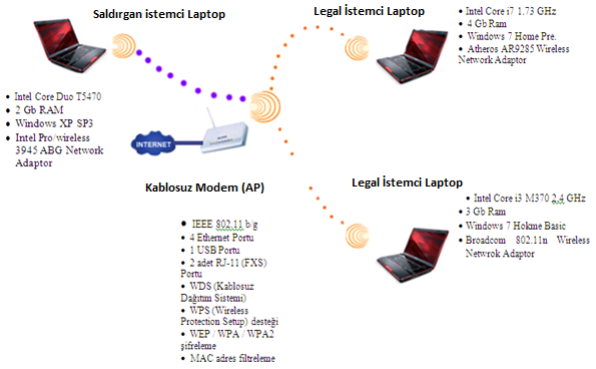
Şekil 1: Udp Taşma Saldırısı Programının Akış Diyagramı

4.2 Test ortamı

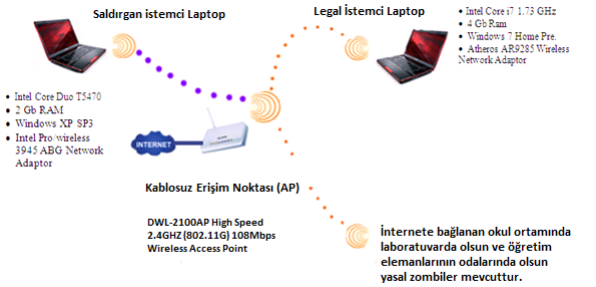
DoS saldırılarının deneysel çalışmaları için iki farklı test ortamı kullanılmıştır. İlk Deneysel çalışmada ev ortamında bulunan kablosuz bir ağdan yararlanılmıştır. İlk Çalışmada bir adet 802.11g/802.11b uyumlu, 2.4 GHz Aralığında, 54 Mbps'e kadar çıkan hız kapasitesi içeren erişim noktası ve aynı

zamanda kablosuz modem görevi gören bir cihaz kullanılmıştır. Bunun yanında 3 adet diz üstü bilgisayar (Laptop) kullanılmış olup, bu laptoplardan biri saldırgan, diğer ikisi de yasal kullanıcı olarak bu kablosuz erişim noktasından internete girebilmektedir. İlk Deneysel çalışma için kullanılan erişim noktası olarakta görev yapan bir kablosuz modem ve 3 taşınabilir bilgisayarın özellikleri aşağıda şekil 2'de gösterilmiştir.

İkinci deneysel ortamda ise Trakya Üniversitesi Eğitim Fakültesi kablosuz yerel alan ağına saldırı yapılmıştır. Bu çalışmada da bir adet 802.11g /802.11b uyumlu, 2.4 GHz Aralığında, 54 Mbps'e kadar çıkan hız kapasitesi içeren erişim noktası bir cihaz kullanılmıştır. . Bunun yanında iki adet dizüstü bilgisayar, biri saldırgan, diğeri ise erişim sonuçlarını görebilmek açısından yasal kullanıcı olarak bu kablosuz erişim noktasından internete girebilmektedir. Bu çalışmada tek fark kablosuz ağı kullanan okulda birçok makine olmasıdır. İkinci Deneysel çalışma için kullanılan bir erişim noktası ve 2 taşınabilir bilgisayarın özellikleri aşağıda şekil 3'de gösterilmiştir.



Şekil 2*: Udp Taşma Saldırısı Birinci Test Ortamı*

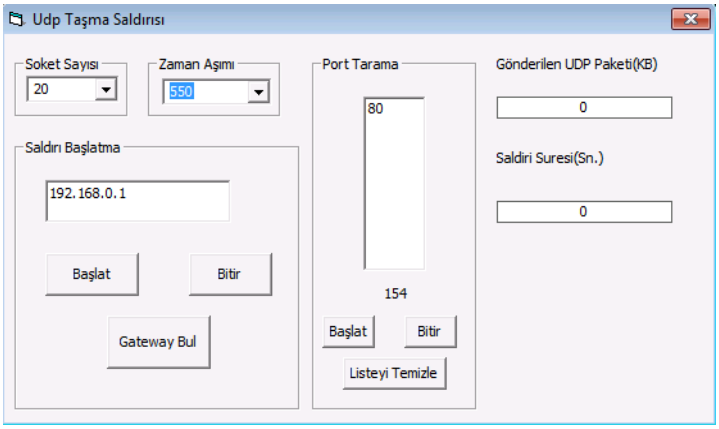


Şekil 3: Udp Taşma Saldırısı İkinci Test Ortamı

4.3 Saldırı örneği

4.3.1 Netmaster Kablosuz Modem (kablo net)[11]

Kablonet içinde kullanılan Kablosuz Modem Netmaster cihazına saldırıldı. Program çalıştırıldığında kablosuz cihazın IP adresinin 192.168.0.1 olduğunu ve açık portunun 80 olduğunu bulunuldu (Şekil. 4).



Şekil 4*: Netmaster için Udp Taşma Saldırısı Ekranı*

Programda 80 (HTTP-Hypertext Transfer Protocol) portu üzerinden istediğimiz miktarda veri byte olarak gönderildi. Soket sayısını arttırdıkça programın etkinliği artığı gözlenildi. Bir süre sonra cihazın devre dışı kaldığı ve diğer legal istemcilerin internete bu kablosuz modem üzerinden çıkamadığı gözlenildi.

Servis Adı	**Port Numarası/ Protokol**	**Servislerin Açıklamaları**
ftp	21/tcp	File Transfer [Control]
ftp	21/udp	File Transfer [Control]
telnet	23/tcp	Telnet
telnet	23/udp	Telnet
http	80/tcp	World Wide Web HTTP
http	80/udp	World Wide Web HTTP
www	80/tcp	World Wide Web HTTP
www	80/udp	World Wide Web HTTP
www-http	80/tcp	World Wide Web HTTP
www-http	80/udp	World Wide Web HTTP

Tablo 1: Saldırı için Açık olan bazı portlar[12]

```
Açık Portları bulmak için kullanılan kod(pseduo)
……..
```

```
Winsock(0).Protocol = sckTCPProtocol
Winsock(0).RemoteHost = txtAdres
timer(0).Enabled = True
……
If Index = 0 Then
  Winsock(Index).Close
  lblportsayac.Caption = Int(lblportsayac.Caption) + 1
  Winsock(Index).RemotePort = lblportsayac.Caption
  Winsock(Index).Connect
```

Şekil 5: AP üzerindeki Açık portları bulan kod

```
Private Sub Winsock_Connect(Index As Integer)
If Index = 0 Then
Winsock(Index).Close
Portlist.AddItem lblportsayac
End If
j = Portlist.ListCount
dizi(j) = lblportsayac
End Sub
```

Şekil 6: Açık portları diziye aktaran kod

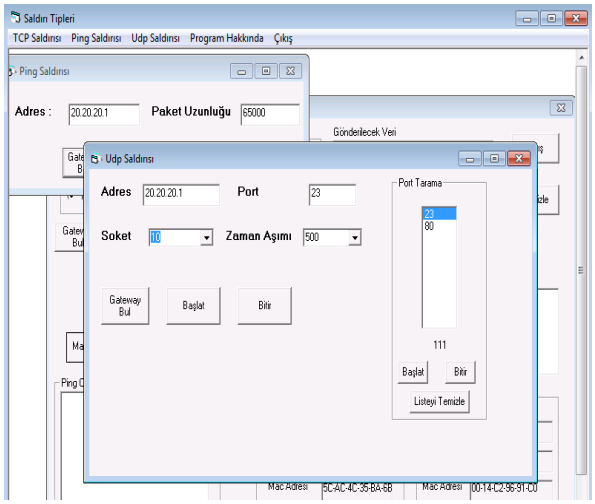
4.3.2 Dwl-2100 Kablosuz Erişim Noktası[3]

Dwl-2100 Erişim Noktası cihazına saldırıldı. Program çalıştırıldığında kablosuz cihazın IP adresinin 20.20.20.1 olduğunu ve açık portlarının 23,80 olduğu bulunuldu (şekil.8).

```
AP'ye dizideki portlara göre veri gönderen Kod

  With Winsock(i)
  While k > 0
    .Close
    .Protocol = sckUDPProtocol
    .Connect txtAdres.Text, CInt(dizi(j))
    .SendData dmg
    k = k - 1
  Wend
  End With
```

Şekil 7: Udp üzerinden veri gönderen kod



Şekil 8: Dwl-2100 için Udp Taşma Saldırısı Ekranı

Programda ağ geçidi (gateway) adresine istenilen soket sayısı kadar açık olan portlardan belirli aralıklarda UDP paketleri gönderildi. Bu deney ortamı okul olduğu için birden çok makine internete çıkmaktadır. Böylece bu makineleri saldırıya dahil edip, bunların yaptığı işlemlerin sonucu olarak (zombie bulduğumuzda) programın amacına ulaşmasının hızlandığı gözlenildi. Bir süre sonra cihazın sağladığı internetin yavaşladığı ve ping cevaplarının gelmediği izlenildi.

5.Sonuçlar

Bu çalışma sonucunda Trakya Üniversitesi Eğitim Fakültesi BÖTE bölümü öğrencilerine ev, okul gibi kablosuz ağ kullanım alanlarında DoS saldırılarının tam anlamıyla önlenemediği ve güvenlik için iyi politikalar geliştiremezlerse geliştirilen program yardımıyla DoS'un etkili olduğu gösterilmiştir. Makalede geleceğin Bilişim Teknolojileri Öğretmenleri olacak olan BÖTE Bölümü öğrencileri için meslek hayatlarında çalıştıkları okullarda internet ve ağ güvenliğini sağlamaları gerektiği hakkında bilgiler verilmiştir. Sonuç olarak aşağıdaki güvenlik adımları tavsiye edilmiştir.

1. Ağa mutlaka güvenlik duvarı kurulmalı, portlar dinlenilmeli ve bir taşma tespitinde taşmayı yapanla iletişim kesilmelidir.
2. Kablosuz iletişim konusunda uzman bir firmadan gelişmiş güvenlik politikaları içeren bir Erişim Noktası alınmalıdır.
3. Kablosuz ağlarda WPA2 ya da WPA+TKIP(Temporal Key Integrity Protocol) [7] şifrelemesi kullanılmalıdır. Ancak bunları kullanırken bunların kimlik doğrulama saldırılarına karşı açık teşkil ettiği unutulmamalıdır.

5 Kaynakça

[1] Aarti Singh, Dimple Juneja, "Agent Based Preventive Measure for UDPFlood Attack in DDoS Attacks", Aarti Singh et. al. / International Journal of Engineering Science and Technology,Vol. 2(8), 2010, 3405-3411

[2] Bulus E., "Designing attacks for SMTP servers", International Journal of Computer Systems Science and Engineering 26-1, Jan 2011, pages: 43-48.

[3] Dwl-2100AP High Speed 2.4Ghz (802.11g) Wireless 108Mbps Access Point, http://www.dlink.com/products/?pid=292

[4] Gezgin D.M., Buluş E., Buluş H.N., "The Technical Analysis of the Comparison of 802.11n Wireless Network Standard", International Scientific Conference,21 – 22 November 2008, GABROVO

[5] Haining W., Danlu Z., Kang G. S., "Detecting SYN Flooding Attacks",EECS Department, The University of MichiganAnn Arbor, MI 48109-2122, No. N00014-99-1-0465.{ hxw , danlu , kgshin } @eecs.umich.edu

[6] Hole K, "Denial-of-Service Attacks", Nowires research Group, Department of Informatics, University of Bergen, September 1, 2008,available at www.Kjhole.com

[7] Johansson D., Krantz A.S., "Practical WLAN Security", TDDC03 Projects, Spring 2007

[8] Kumar S., Ping attack-How pad is it?, Computers&Security 25, 2006, pages 332-337.

[9] Lisa P., "A list of wirelises network attacks", SearchSecurity.com, 26 June 2009

[10] McDowell M., "Understanding Denial of Servers Attacks", United States Computer Emergency Readıness Team (US-CERT), 4 November 2009

[11] Netmaster wireless gateway modem, http://www.netmaster.com.tr/urunler/cbw-560

[12] PortNumbers,http://www.iana.org/assignments/port-numbers, last updated 2011-04-29

[13] TCP And UDP ,By Steve Steinke, Network Magazine ,Feb 5, 2001 (10:03 AM)URL: http://www.networkmagazine.com/article/NMG20010126S0005

[14] Winsock.exe, SAMPLE: Winsock.exe Getting HostAddress Using Windows Sockets ArticleID:154512,http://support.microsoft.com/ default.aspx ?scid=kb;EN−US; q154512, Microsoft, August 2004

[15] WPA and WPA2 Implementation White Paper "Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise", March 2005