LEGAL CHALLENGES POSED BY WI-FI NETWORKS

Maxim DOBRINOIU [*]
Iustin PRIESCU [**]

Abstract
Nowadays, the electronic communications market is in a high development, and this trend will not be diminished even by the newly world economic crisis. Studies show a significant growth in people's interest for Information Society (IS) services, with emphasize on the mobility of the resources. On the other hand, Internet has become more than a "network of networks", but a way of life, and user's addict to computer systems and IS services often reveal interesting aspects and controversial in the same time. Modern forms of electronic communications rely more and more on the wireless Internet connections (Wi-Fi), and this conclusion could be eventually based on the following realities: 1) Users continue to migrate to wireless technology; 2) Users prefer wireless connectivity; 3) Users are attracted by costless Internet connections; 4) Users are fascinated by the possibility of hiding their online activity and behaviour. Although certain security measures can be easily applied in order to prevent the spread of cyber-related crimes, the wireless (Wi-Fi) connection to Internet also rise up a lot of controversial aspects, most of them about the legality of the connection itself, topic that the authors try to approach in this study.

Keywords: *wireless, illegal access, computer system, crime, electronic communications.*

Introduction to Wi-Fi concepts

Nowadays, the electronic communications services market is in full development, and this trend cannot be diminished even by the newly emerged world economic crisis. Regardless the country in question or the rank comparing to other states, studies show a significant growth in world people's interest in Information Society (IS) services, with a strong emphasize on the mobility of the resources.

The Internet has become more than a „network of networks", but a way of life, and the addiction of the users for computer systems and electronic services often highlights interesting aspects, but controversial in the same time.

Right now, assuming the inevitable exceptions, we could launch an analysis based on the following facts:

a. Users are more and more interested in Information Society services. Beyond the simple connection to Internet, a large number of the socio-economic segments of life acknowledge a significant development in cyberspace (for example, electronic commerce, e-banking, e-payment, e-media, e-petition and so forth);

b. Users continue to migrate to a larger extent towards mobile equipments and „wireless technology". Electronic consumer markets is oriented mainly to Bluetooth and Wi-Fi-enabled electronic devices, while the selling of smartphones, PDAs and Notebooks providing Internet connectivity is beyond any expectation;

c. Users prefer, more and more, the wireless connectivity. The entire world is in a continuous movement, and time seems to compress day by day. Even if we are talking about keeping in touch with business partners, friends or family members through VoIP connections, about reading electronic mail messages, reading of the online newspapers or magazines, finding

[*] Lecturer, Ph.D., „Nicolae Titulescu" University, Bucharest (e-mail: office@e-crime.ro).
[**] Lecturer, Ph.D., „Titu Maiorescu" University, Bucharest.

out the forecast, realizing financial transactions (e-banking, e-payment or stock exchange) or just browsing for news or information, people uses a large scale of performing or state-of-the-art electronic devices which assure the much needed level of mobility and connectivity;

d. Although the costs have diminished significantly, people often consider different ways to connect to Internet without paying. Ordinary citizens, businessmen, students or employed, young or elder, men or women, we are altogether tempted to enjoy benefitting from a costless service. The same satisfaction we come across in what regards the Internet connection or the access to electronic communications services, although telecom operators or providers offer now a large scale of subscription possibilities or attractive tariffs;

e. For security reasons or just to hide certain actions or behaviour, more users are really fascinated by the possibility of masking their own activity or identity while in cyberspace. To realize such „own security" today there could be found various technical means or ways facilitating the anonymizing of the Internet browsing, hiding the identity of an email sender or the location of a certain electronic terminal which initiates a cyber attack. Apart from using the well-known Proxy Servers or Spoofing methods, anonymous connection to Wi-Fi Access Points is by far the newest and dangerous one, providing the type of electronic environment hackers are searching for.

Wi-Fi Architecture and Security

Wi-Fi[1] is the word the IT specialists use to define IEEE 802.11 Protocol, while the large public identify nowadays, technologically or commercially, the wireless access to Information Society services. In other words, is about the wireless-enabled electronic devices to connect to Internet through so-called Wi-Fi Access Points in order to get hold of electronic communications services.

According to IEEE 802.11 standard specifications, the logical architecture of a Wi-Fi network consists of various components, like: a Station (STA) which connects to a wireless Access Point (AP), a Set of Internet Base Services (BSS), the services' Distribution System (DS), as well as an Extended Set of Services (SSE).

The Access Points (known also as Hotspots, Wireless Routers or IP Routers) are those electronic devices which receive the Internet signal from a Internet Service Provider (via a cable link) and distribute it as electromagnetic emission (radio broadcast) in a certain cover area (based on the strength of the signal and the existence of the electronic disturbances), from 1 to 100 m. The Wireless Access Point runs as bridge between the Wi-Fi-enabled Stations (STA) and the classic Local Area Network – which usually provide the Internet connection or services.

The assembly resulted following the connection of one or more Wireless Stations (according to IEEE 802.11 Standard) to an Access Point (AP) is called *Wi-Fi Network* or *WLAN*.

The connection of the Wireless Stations to the IP Router could be done:

- Freely, without requesting the authentication of the client in order to use the available Internet services

- Protected, for limiting the use of Internet services to the authenticated (accepted) users by implementing various security protocols and encryption procedures

Aside from the advantages of their implementation (e.g. mobility, reduced costs, flexibility, ubiquity and so), Wi-Fi networks also poses various disadvantages, such as: low quality of

[1] Wi-Fi is a trade mark of the Alliance for Internet Wireless Compatibility, founded in 1993 by over 300 companies producing wireless electronics, certified according to IEEE 802.11 standard (known as WLAN standard).

communication, high energy consumption, electromagnetic pollution, rather weak security of communication etc.

Wireless networks are relatively less secure than the cable ones, due to the much easier way to connect of the unauthorized users present in the covering area of an Access Point. In order to prevent such unauthorized connections, the security of the wireless networks is assured by the following measures:

a. SSID (Service Set Identifier) – represents the identifier or the name of the IP Router (by default, this is the factory name of the device, but this is usually changed by the administrator into a more representative one, like "John's Network" or "Titulescu University" etc.)

b. Wired Equivalent Privacy, Wi-Fi Protected Access and Wi-Fi Protected Access – 2 – are security protocol specially designed to protect and secure the access of a client to the Access Point. The electronic traffic between the Stations and the AP is encrypted using one of the above mentioned protocols

c. MAC Address Validation – the filtering of the all MAC addresses of the electronic devices willing to connect to Internet services provided by a certain Access Point, allowing just those known or authorized

Unfortunately, none of these measures can ensure a high level security. Even WEP Protocol was recently reported as being cracked by hackers. In these conditions, the IT specialists continue to actively work on improving the Wi-Fi-related security measures, this still being one big challenge.

Modus operandi in Wi-Fi Networks

The aim of the present analysis is to emphasize not just the advantages of using Wi-Fi networks, but the controversial aspects too. There are numerous insufficiently regulated aspects to be approached by the legislators, especially in what regards the connection to Access Points and the use of wireless provided Internet services.

As *modus operandi*, the respective both IT and non-IT literature highlighted two types of activities associated by the interested persons (bad guys, hackers etc.) with the wireless networks, such as:

Wardriving – meaning walking or driving a car with the intent to discover and mark on a map all the available Wi-Fi networks. Technically speaking, the Wi-Fi-enabled electronic devices used by the would-be perpetrator (PDA, smartphones, laptop etc.) receive (catch) the radio signal broadcasted by the wireless IP Router and, through a specialized interface, make available information related to it, such as: name of the Access Point (SSID), signal strength, existence of security measures in place (for example – WEP, WPA or WPA2), and Domain Name System' server address.

All this data is stored accordingly for a later analysis that could provide clear information regarding the identified Wi-Fi Access Points (Hotspots) which allow Internet access in a specific cover area.

Has to be mentioned that, in this case, the Wi-Fi-enabled equipment used does not necessarily (automatically) obtain electronic communications services, because for that to happen a several commands have to be launched directly by the interested person.

Piggybacking, which defines the intentionally connection to wireless Internet by placing a Wi-Fi-enabled device in the cover area of a certain Access Point and starting using the Internet services without the acknowledgement or the permission from the owner or legal beholder of the IP Router (and the Internet connection as well).

More often, the connection to electronic communications services through Wi-Fi networks takes place in public spaces, such as bars, restaurants, hotels, cafe, airports, railway stations, universities etc.) And the access of a person to such connections is somehow considered as being legal, permitted, accepted and so.

For all that, usually, the network (AP) owner or legal beholder could request, directly or indirectly, a certain economic compensation for the Wi-Fi facility provided or to control the client's connection to Internet services through a non-economic exchange, such as providing of a connection password only after obtaining the personal data of the client.

For example, the owner of a cafe-bar provides to his clients electronic communications services through a wireless Access Point, and they pay the bill in return. But, what happens when a passer-by discover, accidentally or intentionally, the wireless signal broadcasted from the cafe-bar and try to connect to Internet to check his emails? Would that connection be legal or illegal in terms of actual legislation?

On the other hand, in our opinion, the most dangerous situation is posed by the piggybacking used against private-owned Wi-Fi networks (irrespective to the nature of the beholder – individual or legal person).

Talking about a radio broadcast, the signal could be easily received through the wall which separate us from the neighbour's apartment, through the window of the company located just opposite the street, or the fence which enclose a certain institution, but in fact the connection itself strictly depends on the security measures applied by the AP (WEP, WPA or WPA2 protocols, fixed IP addressing, MAC address filtering, use of Tokens etc.).

How legal or illegal is such a connection to the Information Society services through wireless Access Points is to be further analyzed, the topic being brought anyway now to the attention of the legislators in many countries.

The Legal Challenge Posed By Wi-Fi Networks in Romania

In Romania, the respective legal practice have not yet recorded such cases, but we cannot come to the conclusion that they do not really happen, while the approach from the legal professionals (judges, prosecutors, policemen, lawyers) could be an interesting criminal law challenge.

Considering the actual legal instruments in place, the simulation of certain scenarios highlights the following aspects:

The **Access Point**, identified as an electronic device by the IP Router could be regarded as a *computer system* as stated by article 35, Title III, Law no. 161 from 2003, taking into consideration that:

- it is an electronic device (eventually interconnected with other electronic devices)
- runs based on a *computer program* (which is the Firmware of the device – state-of-the-art software which, following a set of instructions, assure the functionality of the device)

The technical analysis shows that, in the case of **piggybacking**, the IP Router is not directly or remotely accessed by the eventually intrusive Wi-Fi-enabled laptop or PDA, because the full attention of the interested persons **is directed only to the service provided** (e.g. the radio signal carrying Internet computer data broadcasted by the Access Point), and not to the wireless network itself or the Router's internal files (ex. logs) or settings.

Therefore, we consider that there are no specific legal conditions in place for an **illegal access to a computer system** (offence criminalized by article 42, Title III prevention and combating cybercrime, Law no. 161 from 2003).

On the other hand, also from a technical point of view, the simple connection to Internet by Wi-Fi radio signal could be often automatically achieved, depending on the factory settings of the wireless-enabled PDA or laptop used by the would-be perpetrator, without his acknowledgement, and that excludes the existence of the guilt, thus excludes the existence of the crime.

If the Access Point is secured by the means of WEP, WPA, WPA2 protocols or other similar measures, and the would-be perpetrator is acting for the infringement of those measures, could be an indictment under the provisions of article 42, 3rd alignment, Title III - prevention and combating cybercrime, Law no. 161 from 2003 ("illegal access to a computer system committed with the intent to obtain computer data by infringing security measures"), but only if strong evidence is provided to consider the intention of the person to access the settings or log files of the IP Router (ex. through a web based interface, trying several admin names and passwords), and not just the simple desire to connect to Internet services.

Other specialists' opinions, considering that we could be in the framework of an **illegal interception of an electromagnetic emission from a computer system carrying non-public computer data** (as stated in article 43, 2nd alignment, Title III, Law no. 161 from 2003), cannot stand for a criminalization because the respective computer data (contained in the electromagnetic emission – radio broadcast), representing the Internet signal, is **public**.

In this conditions, seems that the only way to indict the connection to Internet services provided by a wireless network (Wi-Fi Access Point) could be using the legal provisions of the Criminal Code (article 208, 2nd alignment) in what regards the **theft**, with an emphasize to the „theft of an economic-valued energy" (like in the case of theft of electricity, theft of TV cable signal etc.), taking into consideration that Internet signal or the access to Information Society services are obtained initially by the owner or legal beholder of the Access Point from an Internet Service Provider (ISP) in exchange to a certain amount of money (e.g. the monthly subscription fee).

We are aware of the fact that this indictment is compelled and, in some ways, immoral, but until an adequate rule in place, could be practical – especially in what regards the connection to private-owned Wi-Fi networks.

The supporters (as well as the practitioners) of **piggybacking** think that that action is more likely as[2]:

- *Reading of someone else's newspaper over his shoulder;*
- *Listening or dancing on the music aired by a neighbour (from radio, TV, music player etc.)*
- *Sleeping on a bench in a public place*
- *Reading a book, during the night, under a streetlight*
- *Eating the food rests of somebody else in a restaurant*

In return, the opponents of piggybacking consider that the action is similar to[3]:

- *Entering another's home on the basis that „the door was opened"*
- *Hanging-up on the back of a public bus for a costless ride*
- *Connection to the neighbour's TV cable or electricity infrastructure*

For all that, in a comprehensive and adequate possible incrimination of this action, we have to consider that piggybacking is now the most used by those willing to launch cyber attacks or to commit cyber-related crimes, such as:

- Identity Theft

[2] http://en.wikipedia.org/wiki/piggybacking
[3] Idem

- Phishing[4]
- Pharming[5]
- Computer fraud
- Online Child Pornography
- Keylogging[6]
- Email Spoofing[7]
- Spam[8]
- Denial of Service[9]

Using the Wi-Fi unprotected Access Points, hackers or other would-be perpetrators aim at the possibility of hiding their own online identity, based on the fact that, at the ISP level, just the IP address of the Router is visible – and that is uniquely associated with the subscriber (which could be a possible victim in this case).

Even if, in relation with the IP Router, the „intrusive" Wi-Fi-enabled device (PDA, laptop etc.) will communicate its own MAC address during the entire length of the connection, the later identification of this device (or of the owner – hacker etc.) will be extremely difficult (sometimes impossible), especially when that device was only once connected to the IP Router and just for a short period of time.

For this legal-technical analysis to conclude in a concrete and academic approach, we consider that the following *de lege ferenda* proposal would be useful to further official steps in creating new (criminal or administrative) legal provisions regulating the access to Internet services by connecting to a (not just)Wi-Fi Access Point:

„Obtaining of electronic communications services through the connection to an access point and using such services without the permission of the right person to grant it is a crime and shall be punished with a fine or imprisonment"

The permission being presumed as granted when:

- The Access Point to the Information Society services (Internet) is a public one

- The connection is realized to a Access Point located in a public place and not secured accordingly

Last but not least, we also have to take into consideration that some of the Telco operators stipulated in their subscription contracts concluded with the clients the ban for the redistribution of the signal to third parties (irrespective to the way of distribution of the signal, cable or radio). The infringement of this provision could only be regarded in an administrative perspective, added to the possibility of the service being suspended or even forbidden by the operator.

---

[4] Type of computer forgery by which a certain user is lured, by electronic communications means and social engineering to access a spoofed website, taken under attacker's control, and to provide own personal and financial data.

[5] Complex type of computer forgery by which an attacker achieve to modify in a Domain Name System server the table of correspondence between IP addresses and the domain names in Internet with the aim to redirect that user to a spoofed website in order to provide personal or financial information.

[6] The action of installing and run a special designed electronic device or computer program able to capture, store and send using SMTP protocol of all the keystrokes a user makes while online. In this way, the attacker can obtain user's personal or financial data, passwords, email content, documents content, iRC messages, screen captures, URL accessed and so on.

[7] Technique by which the attacker modify the data in the header of an email message with the intention to mislead the recipient in what regards the real source of the message.

[8] The act of sending unsolicited messages (with or without commercial content) by electronic communications means.

[9] Computer attack which aims at creating a system interference by flooding the ports with fake requests with a final result in service refusal.

Conclusions

The development and large scale use of (mobile) wireless-enabled devices and Wi-Fi networks allow users to travel to different locations while having access to Information Society services.

Hotspots (Access Points) could be private as well as public. They could be located (could broadcast) in either private or public places. On the other hand, radio waves propagate multi-directional, and thus could easily reach from public places to private ones as well as from private places to public ones.

Now, due to the fact that Wi-Fi communications' security protocols and techniques did not reach the „technological maturity", is necessary for new legal provisions to be enforced. Therefore, we consider that simple use of wireless-enabled devices (PDA, smartphones, and laptops) and their connection to Wi-Fi networks also represent a real legal challenge that should be properly addressed as soon as possible.

As a final remark, we reaffirm that until the legislator comes with new and comprehensive provisions to approach all the situations and scenarios described above, only the appliance of the IT&C security principles will assure the proper climate for the development of the Information Society and the stimulation of the connection mobility for all the citizens to such services, including through the use of Wi-Fi networks.

References

1. M. Dobrinoiu, *Need for New Legal Provisions in Combating* Cybercrime, "Justice in Digital Era" Analytical Report, Sofia, April 2009
2. I. Priescu, V.V. Patriciu, S. Nicolaescu, *Electronic Mail Security in Internet*, Military Technical Academy Publishing, 2006
3. Stewart S. Miller, *Wi-Fi Security*, McGraw-Hill, 2003
4. Pejman Roshan, Jonathan Leary, *802.11 Wireless LAN Fundamentals*, Cisco Press, 2003
5. http://www.oppapers.com/essays/Wifi-History/115029, 2007
6. http://en.wikipedia.org/wiki/IEEE_802.11a-1999, 2009
7. http://en.wikipedia.org/wiki/802.11n, 2009
8. 802.11n: Next-Generation Wireless LAN Technology, White Paper, Broadcom, www.broadcom.com, 2006

PROVOCAREA LEGISLATIVĂ A REȚELELOR WI-FI (IEEE 802.11)

Maxim DOBRINOIU [*]
Iustin **PRIESCU** [**]

Cuvinte cheie: *wireless, acces ilegal, sistem informatic, infracțiune, comunicații electronice.*

Introducere. Premise în utilizarea rețelelor Wi-Fi

În momentul de față, piața serviciilor de comunicații electronice este în plină dezvoltare, iar acest avânt nu va putea fi estompat nici măcar de criza economică prin care trece în acest timp întreaga omenire. Diferențiat pe state, dar indiferent de clasament, studiile în domeniu indică o creştere a interesului persoanelor pentru serviciile societății informaționale, cu un accent semnificativ pe mobilitatea resurselor.

Internetul este acum mai mult decât o „rețea a rețelelor", a devenit un mod de viață, iar dependența utilizatorilor de echipamentele de calcul şi serviciile de comunicații electronice relevă adesea aspecte interesante, dar în acelaşi timp controversate.

În acest moment, asumându-ne excepțiile inerente, putem totuşi lansa o analiză în baza următoarelor premise:

a. Utilizatorii sunt din ce în ce mai interesați de serviciile societății informaționale. Pe lângă simpla conectare la Internet, tot mai multe segmente ale economiei şi societății cunosc o dezvoltare accentuată în mediul informatic (de exemplu, comerț electronic, e-banking, plata electronică a taxelor sau impozitelor, e-mass-media, petiționare etc.)

b. Utilizatorii continuă să migreze tot mai mult către echipamentele mobile şi „tehnologia fără fir" (wireless). Piața de produse electronice este orientată cu prioritate pe segmentele de echipamente cu tehnologii Bluetooth şi Wireless, vânzările telefoanelor inteligente (smartphones), PDA-urilor sau laptop-urilor care oferă conectivitate la Internet „fără fir" întrecând orice aşteptări.

c. Utilizatorii preferă din ce în ce mai mult „conectivitatea fără fir". Lumea este într-o continuă mişcare, iar timpul pare a se comprima. Fie că este vorba despre asigurarea legăturii cu partenerii de afaceri sau prietenii prin conexiuni voce-video tip VoIP, de consultarea mesajelor de poştă electronică, de cititul presei, aflarea prognozei meteo, fie de realizarea transferurilor bancare sau plata facturilor, efectuarea tranzacțiilor la bursă sau simpla căutare a unor informații (inclusiv de localizare), oamenii utilizează o gamă largă de dispozitive electronice performante care să le asigure nivelul de mobilitate şi conectivitate dorit.

d. Deşi costurile s-au diminuat în timp, oamenii au tendința de a „căuta" posibilități de conectare la Internet fără plată. Simpli cetățeni sau oameni de afaceri, studenți sau angajați, tineri sau vârstnici, bărbați sau femei, suntem cu toții tentați adesea să ne bucurăm atunci când avem posibilitatea de a beneficia fără plată de un anumit serviciu. Aceeaşi satisfacție o avem şi în ceea ce priveşte conectarea la Internet şi accesarea serviciilor de comunicații electronice, chiar dacă operatorii de telecomunicații sau furnizorii acestor servicii oferă în prezent o paletă largă de posibilități de contractare.

e. Din rațiuni de protecție sau chiar de ascundere a unor fapte, mulți utilizatori sunt „fascinați" de posibilitatea mascării activității online şi propriei identități în mediul virtual. Pentru

[*] Lect. univ.dr., Universitatea „Nicolae Titulescu", Bucuresti (e-mail: office@e-crime.ro).
[**] Lect. univ.dr., Universitatea „Titu Maiorescu", Bucuresti.

realizarea acestei ”securități individuale” există azi o gamă variată de procedee tehnice care permit anonimizarea navigării pe Internet, ascunderea identității expeditorului unui mesaj de poştă electronică sau a locației unui echipament de calcul care generează un atac informatic. Pe lângă folosirea binecunoscutelor servere Proxy sau a metodelor de Spoofing, câştigă tot mai mult teren conectarea anonimă la punctele de acces tip Wi-Fi (wireless), care oferă exact mediul de lucru căutat de persoanele rău intenționate.

Arhitectura şi securitatea rețelelor Wi-Fi

Wi-Fi[1] este acronimul sub care specialiştii denumesc protocolul IEEE 802.11, iar publicul larg identifică azi, tehnologic ori comercial, accesarea serviciilor societății informaționale prin conectivitatea ”fără fir”. În esență, este vorba despre posibilitatea dispozitivelor echipate wireless de a se conecta la Internet prin intermediul unor **puncte de acces** (Access Point - AP) wireless şi obține servicii de comunicații electronice.

Conform specificațiilor standardului IEEE 802.11, arhitectura logică a unei rețele Wi-Fi conține mai multe componente principale: stație (STA) care se conectează la un Punct de Acces wireless (AP), un set de servicii de bază (BSS) Internet, sistemul de distribuție (DS) a acestor servicii (conectarea mai multor AP între ele prin aceeaşi rețea LAN), precum şi set extins de servicii (SSE), cum este descris în figura nr.2. Stațiile (STA) wireless conțin un adaptor de card, un card PC wireless sau au încorporat un dispozitiv pentru a oferi conectivitate wireless.

Punctele de acces (denumite şi **hotspots sau routere wireless**), reprezintă acele dispozitive electronice care primesc semnal Internet de la un furnizor de servicii (ISP) şi îl redistribuie sub formă de emisie electromagnetică (radio broadcast) într-o anumită arie de acoperire (în funcție de puterea semnalului şi existența factorilor perturbatori, între 1-100 m). Punctul de acces (AP) fără fir funcționează ca o punte de legătură între stațiile (STA) wireless şi o rețea LAN clasică, existentă pentru accesul la serviciile Internet.

Ansamblul rezultat în urma conectării unuia sau mai multor stații (STA) wireless (conform specificațiilor standardului IEEE 802.11) la un punct de acces (AP) poartă numele de *rețea Wi-Fi*, *rețea wireless* sau *WLAN*.

Accesul stațiilor (STA) la AP (routerul wireless) se poate face:

- liber, fără a cere autentificarea utilizatorului la folosirea serviciilor disponibile (de exemplu, rețele wireless din aeroporturi, locurile publice metropolitane etc.)
- protejat pentru a limita folosirea serviciilor numai către utilizatorii autentificați şi prin utilizarea unor protocoale de securitate, aşa cum va descris mai jos.

Pe lângă avantajele evidente ale implementării rețelelor Wi-Fi (mobilitate, cost redus, flexibilitate, ubicuitate – capacitatea de a te plasa în orice loc etc.), acestea prezintă şi o serie de dezavantaje (calitate scăzută a comunicației, consum de energie, poluare electromagnetică, securitatea comunicației).

Rețelele wireless sunt relativ mai puțin sigure decât cele cablate, datorită accesului mai facil la rețea al persoanelor neautorizate aflate în zonele de acoperire ale punctelor de acces (AP). Există, implicit în utilizarea rețelelor wireless, diferite bariere care formează aşa numita securitate de bază a rețelelor wireless, ce împiedică accesul neintenționat al persoanelor străine de rețea, aflate în aria de acoperire a unui punct de acces. Securitatea de bază a rețelelor wireless este asigurată de următoarele funcții implementate:

[1] Wi-Fi este marcă înregistrată a Alianței pentru Compatibilitate Wireless Internet, fondată în 1999, de peste 300 de companii producătoare de dispozitive electronice wireless, certificate în conformitate cu standardul IEEE 802.11 (cunoscut şi sub numele de standardul WLAN)

- SSID (Service Set Identifiers) - un cod propriu care defineşte apartenența la un anumit punct de acces wireless

- WEP (Wired Equivalent Privacy) sau WPA / WPA-2 (Wi-Fi Protected Access) – protocoale ce realizează criptarea traficului dintre clienții wireless şi punctul de acces

- Verificarea adresei MAC (Media Acces Control) – filtrarea adreselor MAC, adică punctul de acces este configurat cu adresele MAC ale clienților cărora le este permis accesul în rețea.

Din nefericire, niciuna dintre aceste metode nu asigură o securitate prea mare. În aceste condiții, specialiştii în domeniu caută să îmbunătățească securitatea rețelelor Wi-Fi, fiind una din provocările actuale pentru aceştia.

Modus operandi în rețelele Wi-Fi

Scopul analizei de față este acela de a scoate în evidență, nu atât avantajele utilizării rețelelor Wi-Fi, cât mai ales aspectele contradictorii sau insuficient reglementate care se circumscriu conectării la punctele de acces wireless.

Ca *modus operandi*, literatura de specialitate (nu neapărat tehnică) a reținut două tipuri de activități pe care persoanele interesate le practică în legătură cu rețelele Wi-Fi, şi anume:

Wardriving, care presupune deplasarea pe jos ori cu un vehicul în scopul descoperirii şi marcării pe o hartă a rețelelor (punctelor de acces) wireless care oferă conectivitate la Internet. Tehnic, dispozitivul folosit de persoana interesată (PDA, Smarphone, laptop etc.) captează semnalul radio (broadcast) emis de punctul de acces (routerul wireless) şi, printr-o interfață specializată, oferă informații despre acesta, cum ar fi: numele punctului (SSID - Service Set IDentifier), puterea de emisie (puterea semnalului radio), existența măsurilor de protecție şi algoritmul de criptare utilizat (de exemplu, WEP - Wired Equivalent Privacy, WPA - Wi-Fi Protected Access sau WPA-2), adresa de IP alocată, adresa serverului DNS (Domain Name System – care permite translatarea unui nume de domeniu într-o adresă IP în Internet şi invers).

Toate aceste date sunt consemnate electronic, o analiză ulterioară putând oferi informații clare despre situația punctelor de acces Wi-Fi care furnizează servicii de comunicații electronice (conectare la Internet) într-o anumită arie de interes.

Important de reținut este faptul că în acest caz, echipamentul Wi-Fi al persoanei nu obține automat servicii de comunicații electronice, pentru aceasta fiind necesară lansarea unei comenzi de conectare.

Piggybacking (traducere „cărat în spate"), care defineşte accesarea cu intenție a unei conexiuni Internet wireless prin plasarea unui dispozitiv echipat Wi-Fi în raza de acoperire a unui punct de acces (Access Point) şi utilizarea serviciilor Internet fără cunoştința ori permisiunea expresă a posesorului (deținătorului legal, abonatului etc.) respectivei conexiuni.

Cel mai adesea, conectarea la serviciile de comuncații electronice prin intermediul rețelelor Wi-Fi are loc în spații publice (baruri, cafenele, hoteluri, aeroporturi, universități etc.), iar accesul se prezumă a fi legal, permis, îndreptățit.

Cu toate acestea, este foarte posibil ca deținătorul rețelei ori punctului de acces (AP) să solicite, direct ori indirect, o anumită compensație financiară pentru facilitatea Wi-Fi oferită sau să supravegheze conectarea clienților la rețea printr-un schimb nepatrimonial, ca de exemplu comunicarea parolei de conectare după obținerea datelor de identificare ale persoanei interesate.

De exemplu, proprietarul unei cafenele oferă servicii de comunicații electronice printr-un punct de acces wireless clienților săi, aceştia „răsplătind" facilitatea oferită de acesta prin plata consumației. Dar ce se întâmplă în momentul în care un trecător pe stradă descoperă, accidental sau intenționat, semnalul radio de acces la Internet emis de punctul de acces din cafenea şi se

conectează la diferite servicii de comunicații electronice? Cât de legală sau ilegală va fi acea conectare?

Pe de altă parte, îngrijorător este, în opinia noastră, faptul că piggybacking-ul se manifestă din ce în ce mai frecvent în raport cu rețelele wireless particulare (private), fie că acestea aparțin unor persoane fizice sau juridice.

Fiind vorba despre o emisie radio (broadcast), semnalul poate fi captat cu ușurință prin zidul care ne desparte de apartamentul vecinului, prin geamul firmei de vis-a-vis sau gardul care împrejmuieşte o instituție, însă accesul la serviciul Internet depinde strict de măsurile de securitate asociate punctului de acces (routerului wireless), cum ar fi, folosirea unor protocoale de criptare a datelor (WEP, WPA sau WPA2), filtrarea adreselor MAC (Media Access Control), adresare IP fixă, token-uri hardware sau software etc.

Cât de legală sau de morală este însă o asemenea conectare la serviciile societății informaționale prin intermediul punctelor de acces wireless rămâne de analizat, subiectul aflându-se deja în dezbaterea legiuitorilor din multe țări.

Provocarea legislativă a rețelelor Wi-Fi în România

În România, practica judiciară în materie nu a înregistrat (încă) astfel de cazuri, ceea ce nu înseamnă însă că acestea nu se manifestă în realitate, abordarea lor de către practicieni (polițişti, procurori sau judecători) putând fi o adevărată provocare legislativă.

Cu instrumentele juridice existente, simularea unor scenarii posibile relevă următoarele aspecte:

Punctul de Acces (Access Point-AP) identificat ca dispozitiv electronic prin **Routerul Wi-Fi** (cunoscut şi ca Router wireless) este un sistem informatic în accepțiunea art. 35 din Titlul III al Legii 161/2003 întrucât:

- este un dispozitiv electronic (eventual, interconectat cu alte dispozitive electronice)
- funcționează în baza unui program informatic (Firmware – software proprietar care, în baza unui set minimal de instrucțiuni, asigură funcționarea de bază a respectivului dispozitiv electronic)

Însă, în cazul piggybacking-ului, routerul nu este accesat fizic, nici direct şi nici de la distanță, iar atenția utilizatorilor se îndreaptă numai spre semnalul radio purtător de date informatice (de conexiune la Internet) şi nu spre datele interne (setări, fişiere log etc.) ori spre Firmware-ul dispozitivului.

Astfel, considerăm că nu sunt întrunite condițiile unui **acces ilegal la un sistem informatic** (faptă prevăzută şi pedepsită de art. 42 din Legea 161/2003, Titlul III – prevenirea şi combaterea criminalității informatice).

Pe de altă parte, din punct de vedere strict tehnic, simpla conectare la Internet prin semnalul Wi-Fi se realizează adesea automat, în funcție de setările dispozitivului folosit de prezumtivul făptuitor, fără ştirea acestuia, ceea ce exclude existența vinovăției, deci şi a infracțiunii.

Dacă, însă, punctul de acces (AP) este protejat prin folosirea protocoalelor de securitate WEP, WPA sau altele, iar făptuitorul acționează pentru „spargerea" acestor măsuri de securitate, poate exista o incriminare în baza art. 42 alin. 3 din Legea 161/2003 doar cu condiția să existe probe din care să rezulte intenția făptuitorului de a accesa setările sau fişierele Routerului Wi-Fi, nu doar simpla dorință de conectare la Internet.

Opiniile exprimate de unii specialişti, potrivit cărora ne-am putea afla în condițiile "*interceptării fără drept a unei emisii electromagnetice provenită dintr-un sistem informatic ce conține date informatice care nu sunt publice…*" (art. 43 alin 2 din Legea 161/2003) nu sunt

pertinente şi sustenabile, întrucât datele informatice conținute în emisia electromagnetică (broadcast-ul radio) ce reprezintă semnalul Internet sunt **publice**.

În aceste condiții, singura posibilitate de încadrare juridică a conectării la serviciile de comunicații electronice furnizate de un punct de acces Wi-Fi ar putea-o reprezenta infracțiunea de furt (prevăzută şi pedepsită de art. 208 alin 2 Cod Penal), în condițiile *„furtului unei energii care are valoare economică”*, întrucât semnalul Internet, respectiv accesul la serviciile societății informaționale este obținut de proprietarul, deținătorul ori utilizatorul legal al Routerului Wi-Fi de la un furnizor de servicii Internet (ISP - Internet Service Provider) în schimbul unei sume de bani (abonament lunar etc.).

Suntem de acord că această încadrare este forțată şi, oarecum, imorală, însă, până la o reglementare adecvată, poate fi practică – mai ales în cazul rețelelor (punctelor de acces) private.

Susținătorii (şi practicanții) *piggybacking* sunt de părere că acțiunile lor seamănă cu[2]:

- Citirea ziarului, într-un mijloc de transport în comun, peste umărul celui care l-a cumpărat;

- Ascultatul şi dansatul pe muzica pusă de un vecin;

- Dormitul pe întreaga suprafață a unei bănci într-un loc public;

- Cititul noaptea la lumina unei lămpi stradale;

- Mâncatul resturilor unui client într-un restaurant etc.

În replică, oponenții *piggybacking* sunt de părere că aceste fapte sunt similare cu[3]:

- Intratul în locuința altuia pe motiv că “uşa era deschisă”

- “Agățatul” pe spatele unui mijloc de transport în comun pentru a călători gratis

- Conectarea la cablul de curent electric sau cel de TV al vecinului (abonat);

Totuşi, în reglementarea adecvată a acestei fapte, trebuie avut în vedere că *piggybacking*-ul este din ce în ce mai utilizat de către cei care intenționează să desfăşoare activități infracționale în mediul cibernetic, cum ar fi:

- Furt de identitate
- Phishing[4]
- Pharming[5]
- Fraudă informatică
- Pornografie infantilă online
- Sniffing[6]
- Email Spoofing[7]
- Spam[8]

[2] http://en.wikipedia.org/wiki/piggybacking

[3] Idem

[4] Tip de fals informatic prin care un utilizator este ademenit, prin mijloace de comunicare abile cunoscute sub numele de *inginerie socială*, sa acceseze o anumită pagină web contrafăcută, aflată sub controlul atacatorilor, şi să furnizeze date personale sau date financiar-bancare

[5] Tip complex de fals informatic prin care atacatorul reuşeşte să modifice în cadrul unui server DNS (Sistem Nume de Domeniu) datele de corespondență între numele de domeniu şi adresele IP asociate în scopul de a determina un anumit utilizator să acceseze pagini web contrafăcute pentru a funiza date personale sau financiar-bancare etc.

[6] Captarea pachetelor de date într-o rețea, de către administratorii acesteia, prin folosirea unor dispozitive electronice sau programe informatice special create, în scopul monitorizării şi asigurării bunei funcționări a rețelei. Pe de altă parte, *sniffer-ele* pot fi folosite şi de persoane rău intenționate în vederea obținerii neautorizate de date şi informații din rețea

[7] Tehnică prin care atacatorul informatic modifică datele din antetul unui mesaj de poştă electronică în scopul inducerii în eroare a destinatarului cu privire la adevărata sursă a mesajului

[8] Trimiterea de mesaje comerciale nesolicitate prin intermediul mijloacelor de comunicații electronice (de obicei, poşta electronică)

- Denial-of-Service[9]

Prin utilizarea punctelor de acces Wi-Fi neprotejate la Internet, persoanele rău intenționate mizează pe posibilitatea ascunderii propriei identități, întrucât, la nivelul furnizorului de servicii Internet va fi vizibilă exclusiv adresa de IP a routerului – asociată în mod unic cu persoana abonatului.

Chiar dacă, în raport cu routerul IP, dispozitivul Wi-Fi intrus va comunica propria adresă fizică de rețea (adresa de MAC), pe toată durata conexiunii, identificarea acestuia, respectiv a posesorului (făptuitorului) va fi extrem de dificilă (dacă nu imposibilă), mai ales în condițiile în care acesta s-a aflat o singură dată şi doar pentru o scurtă perioadă de timp în raza de acțiune a punctului de acces.

Pentru ca această analiză juridico-tehnică să concluzioneze într-un demers concret, considerăm că următoarea propunere *de lege ferenda* ar fi utilă în eventualitatea unei viitoare reglementări penale sau contravenționale a accesului la Internet prin intermediul rețelelor Wi-Fi (şi nu numai), astfel:

„obținerea de servicii de comunicații electronice prin conectarea la un punct de acces şi utilizarea acestora fără permisiunea celui în drept să o acorde este infracțiune (contravenție) şi se pedepseşte cu închisoarea de la 00 luni la 00 ani (sau cu amendă de la 00 lei la 00 lei)" urmând ca permisiunea să se prezume a fi acordată în condițiile în care:

- Punctul de acces la serviciile societății informaționale este public
- Conectarea se realizează la un punct de acces situat într-un loc public şi neprotejat prin măsuri de securitate

Nu în ultimul rând, unii operatori de telecomunicații sau furnizori de servicii Internet au prevăzut în cuprinsul contractelor de abonament încheiate cu clienții interdicția ca aceştia să redistribuie la rândul lor semnalul către alți utilizatori (indiferent de modalitatea de realizare cablu sau wireless). Încălcarea acestei interdicții poate avea numai caracter contravențional, în plus existând şi posibilitatea restricționării sau chiar a încetării furnizării serviciului de comunicații electronice.

Concluzii

Dezvoltarea si folosirea pe scară largă a echipamentelor wireless (în special mobile) şi a rețelelor Wi-Fi permit utilizatorilor să se deplaseze sau călătorească în diferite locuri sau zone geografice şi să aibă acces prin hotspot-uri la serviciile societății informaționale.

Hotspot-urile pot fi publice sau private. Ele pot fi situate (pot opera) în locuri publice sau private. Pe de altă parte, undele radio se propagă multidirecțional, putând ajunge din spații private în spații publice şi invers.

Întrucât până în prezent protocoalele si tehnicile de securitate a comunicațiilor în cadrul rețelelor Wi-Fi nu au ajuns la maturitatea necesară, se impune sprijinirea şi prin măsuri de ordin legislativ, special destinate acestei tehnologii aflate in plină dezvoltare.

Tocmai de aceea, utilizarea dispozitivelor wireless, respectiv conectarea la de rețele de tip Wi-Fi reprezintă **o provocare de ordin juridic**, căreia, mai devreme sau mai târziu, legiuitorul român sau străin va trebui să îi găsească o soluție adecvată.

Ca o concluzie, putem afirma că, cel puțin până la o reglementare adecvată a situațiilor descrise anterior, asigurarea unui climat propice dezvoltării societății informaționale şi stimularea mobilității conectării cetățenilor la aceste servicii, inclusiv prin intermediul rețelelor Wi-Fi, rezidă în aplicarea corespunzătoare a principiilor culturii de securitate în domeniul IT&C.

[9] Atac informatic ce vizează perturbarea funcționării unui sistem informatic prin inundarea porturilor acestuia cu solicitări false care determină în cele din urmă „refuzul serviciului"

Bibliografie

1. Maxim Dobrinoiu, *Neajunsuri legislative în combaterea criminalității informatice*, Raport analitic ”Justiție în Era Digitală”, Sofia, aprilie 2009
2. Iustin Priescu, Victor Valeriu Patriciu, Sebastian Nicolaescu, *Securitatea poştei electronice în Internet*, Editura ATM, 2006
3. Stewart S. Miller, *Wi-Fi Security*, McGraw-Hill, 2003
4. Pejman Roshan, Jonathan Leary, *802.11 Wireless LAN Fundamentals*, Cisco Press, 2003
5. http://www.oppapers.com/essays/Wifi-History/115029, 2007
6. http://en.wikipedia.org/wiki/IEEE_802.11a-1999, 2009
7. http://en.wikipedia.org/wiki/802.11n, 2009
8. 802.11n: Next-Generation Wireless LAN Technology, White Paper, Broadcom, www.broadcom.com, 2006