

## Slide 1: Title & Speaker

Ladies and Gentlemen:

I'm going to talk to you about Wardriving, Warchalking, and Wireless Hacking, as well as share with you my experience from EC-Members' legal framework to cope with Cyber-Crime such as this one of wireless hacking.

## Wardriving

## Slide 2: Wardriving

The term “Wardriving” is used in order to describe that practice at which an individual, an Internet user, wanders in the streets of districts equipped with electronic devices capable for wireless access to the Internet with the aim to locate wireless networks for access to the Internet, either house-based or corporate-based wireless networks, map their existence for statistical or any other reason, and hack them.

The first time Wardriving was reported, it was in the USA, around the year 2000, when Peter M. Shipley, a specialist on telecommunications and networks security made a research on wireless networks deployed by that time in Berkeley, California. In 2001, Shipley presented the findings of his research at the annual DefCon Congress Meeting, which was—it still remains—one of the most widely known events in the hackers' community. Peter Shipley's goal was to show the security loopholes of wireless networks used at that time and to attract the attention of wireless networks manufacturers as well as specialists upon the security issue of

said technology which had been perceived—and it is still being perceived—as a killer-app spreading like fire in Berkeley, California and the rest of the U.S.A. In consideration of his findings, Shipley proved that an individual can access easily a wireless network upon which he has no legal rights, by making use of simple tools, even from a distance of forty kilometres away from the top of a building upon which wireless technology—i.e. a transmitter or a network hub—is set up to operate.

In 2001, the Peter Shipley succeeded in intercepting and managing signal between wireless transmitter and receptor (Wi-Fi technology) in a distance of twenty five miles between transmitter and receptor. In 2005, members of the so called iFiber Redwire team, a team of scientists and university students presenting themselves as experts in wireless networks, publicised the results of their research and experimentation on the successful interconnection of Wi-Fi transmitter and receptor based on the Protocol 802.11b. Interconnection was successful at a distance of one hundred and twenty five miles, that is to say more than two hundred and one kilometres (201.007,06 m)!

Wardriving does not require the use of expensive or difficult to find in the market equipment in order to implement. It can happen with the use of an average laptop or a personal digital assistant (PDA).

**Slide 3: Equipment for Wardriving with a laptop**

Slide 3 describes you the minimum necessary equipment for Wardriving committed with a laptop-based set of tools.

**Slide 4: Equipment for Wardriving with a PDA**

Slide 4 describes you the minimum necessary equipment for Wardriving committed with a PDA-based set of tools.

**Slide 5: Networking devices for Wardriving with laptop**

Slide 5 presents you the networking devices—i.e. how to set them up—for Wardriving with a laptop computer which is powered through a vehicle’s lighter and battery.

Almost from the beginning it was made known, Wardriving took dimensions. It was identified as a “grassroots” movement and was presented by American mass media as brilliant idea. Also in Europe, Wardriving appeared to have symptoms of a mass movement phenomenon. Early enough, various consulting organisations tried to depict and project the situation with wireless networks. In 2003, KPMG presented findings indicating an increase of people’s attempts to hack wireless networks set up in London. Most of these attempts were made by Wardrivers, i.e. people who were passing by the areas in which wireless networks had been set up, and who were trying to hack them either for fun or for a certain malicious purpose. In another research conducted in 2004 by RSA Security, it was found that only 66% of corporate wireless networks made use of some technology for protection against Wardrivers and hackers. In consideration of the fact that by 2004 London was met with an increase of wireless networks in the range of 235%, then one can understand that the 34% of wireless networks in London by that time—2004—that were not protected against wireless hacking, represented a vary big number of corporate wireless networks left unsecured and available to commit malicious and illegal actions either against the

corporation which owned said wireless networks or against any third party.

## **Warchalking**

### **Slide 6: Warchalking**

More often than not, Wardrivers, once they locate in an area one or more available wireless networks, either home-networks or corporate networks, they make public onto the Internet their findings so that people who tend to have the same habits, i.e. people who tend to make unauthorized use of proprietary wireless networks, may find good information directing them into available wireless networks. The term “Warchalking” has been coined to mean the action of making public information indicating available wireless networks in an area. Warchalking mainly describes the labelling with semiotics, symbols, which is usually set on buildings or constructions that are found in the area wherein unauthorised access to available wireless networks was attempted. Said labelling is used so that people who tend to make unauthorized and illegal use of wireless networks may find the place where from they could do so.

### **Slide 7: Warchalking semiotics**

A Warchalker makes use of the symbols that you see in slide 7. Said symbols have become common knowledge, and are used to give information upon the type and the bandwidth of a spotted access point in a wireless network.

The first of these symbols, notifies the existence of an accessible access point in a wireless network. On top of said symbol is marked information for the Service Set Identifier (SSID) or the name of the wireless network. SSID is, sort of, the identification card of the wireless network. Every wireless technology is making use of a SSID. The most widely known SSIDs are the IBSSID, which stands for Independent Basic Service Set Identifier and the ESSID, which stands for Extended Service Set Identifier. Coming back to the first symbol as it appears in the slide, at the bottom of it, the Warchalker marks information pertaining to the bandwidth of the wireless network. The first symbol indicates an open node, a rogue access point, as it is usually called, through which penetrating a wireless network can be successful. The second of these symbols, notifies the existence of a non-accessible access point—a closed node. The third of these symbols, notifies the availability of an access point in a wireless network connected to the Internet and also the WEP cryptographic software code used in that network. On top of said symbol and in the left side, it is marked the SSID information, while the password or other information to access the network is marked at the right. At the bottom of that symbol it is marked information indicating the bandwidth of the network.

### Slides 8, 9: Examples of Warchalking

These photos appearing in slides 8 and 9 give you understand the common way in which Warchalking symbols are used by hackers of wireless networks worldwide.

## **A r g u i n g   a b o u t   t h e   l e g a l i t y**

There is a dispute worldwide about the legality of Wardriving and Warchalking. Those who are in favour of these actions, claim that mapping rogue access points in wireless networks is not an illegal action, but rather an action aiming at providing Internet users and wireless technology consumers with information upon the loopholes of that technology. Supporters of the legality claim rogue access point mapping to be an action of warning for the security weakness of wireless networks, and an attempt to make consumers understand that once they decide to deploy wireless networks, private or corporate, they have to take additional security measures in order to prevent unauthorised use of these networks. In that opinion, people who just map rogue access points but do not make any unauthorized use of them, do not commit any crime. More often than not, you will find Wardrivers claiming that they adhere to a strict code of ethics, and that their actions are not illegal simply because they don't do the following things:

- 1) Don't examine the contents of a network;
- 2) Don't add, delete, or change anything on the network, and
- 3) Don't even use the network's Internet connection for Web surfing, email, chat, FTP, or anything else.

The least a Wardriver can gain out of his actions is the cost-free use of the Internet through the rogue access point and the wireless network connected to it. When the network is public, like the wireless network that is in operation in Constitution Square—the most central square in Athens, Greece, right in front of the Parliament building of Greece—then accessing said network as a Wardriver is not an illegal action. But what if the network is private and proprietary? Private networks may either be accessed by any people who just bought the right to access them, such as the case of wireless networks in Starbucks café or may be proprietary

networks in which only authorised personnel may make use of it. In both last cases, accessing the private wireless network without the right to do so is obviously an illegal action.

**Slide 10: The legality of Wardriving is in question**

Until today, no court case has reached a verdict verifying the legality of either Wardriving or Warchalking. On the contrary, the U.S.A. Government considers Wardriving to be a threat against security in Cyberspace in the National Strategy to Secure Cyberspace issued since February 2003, wherein the threat of Wardriving is described as follows:

«A person driving in a car around a city [who] can access many wireless local area networks without the knowledge of their owners unless strong security measures are added to those systems.»

The U.S. Government has been dealing with the illegality of Wardriving and Warchalking since 2002 when FBI got involved in a case of wireless hacking. At that time, Special Agent Bill Shore composed a Memorandum to FBI headquarters in which he expressed the following view:

«Identifying the presence of a wireless network may not be a criminal violation; however, there may be criminal violations if the network is actually accessed including theft of services, interception of communications, misuse of computing resources, up to and including violations of the Federal Computer Fraud and Abuse Statute, Theft of Trade Secrets, and other federal violations. At this point, I am not aware of any malicious activity that has been reported to the FBI here in Pittsburgh; however, you are cautioned regarding this activity if you have implemented a wireless network in your business. You are also highly encouraged

to implement appropriate wireless security practices to protect your information assets».

## **S e c u r i t y   w e a k n e s s i n   w i r e l e s s   n e t w o r k s**

### **Slide 11: Security Protocols**

Since the approval of 802.11 standards from the Institute of Electrical and Electronics Engineers (IEEE), the interest of technologists in relation to wireless technology has delved into the security issues of said technology. It has been noticed that the WEP protocol—the Wireless Equivalent Protocol—with which most Wi-Fi systems were introduced in the market, is weak in security.

Understanding WEP's security weakness, has directed technologists towards the creation of a new protocol, the Temporary Key Integrity Protocol (TKIP) which was first become known as WEP2. Initially, TKIP was developed as a temporary alternative solution for security weaknesses of WEP. In the following years, efforts to cope with security problem of wireless technologies has led to the development of the Wi-Fi Protected Access 2 (WPA2) protocol which is based on 802.11i standard of IEEE and makes use of the sophisticated cryptographic technique of the Advanced Encryption Standard (AES). AES is applicable to the Federal Information Processing Standards FIPS 140-2 of the National Institute of Standards and Technology (NIST) of the U.S.

Most of the security problems faced with WEP can now be solved with the WPA2 protocol. However, reinforcing security in wireless networks

is an advisable step to take further when deploying wireless networks, because knowledgeable and competent hackers will find the way to sneak into once they realise that “the door is locked and the key is under the mat.”

### Slide 12: Hacking attacks

One can list hacking of wireless networks in two basic categories: passive attacks and active attacks. An attack is passive when the attacker gains access to a wireless network but does not cause any change or damage to the data moving in said network. On the other hand, an attack is active when the intruder aims at causing damage or altering either the data or the network settings at which he has gained unauthorised access. Additionally, there are various types of hacking attacks against wireless networks which may include attacks such as Eavesdropping or Wireless Network Sniffing, Traffic Analysis, Passive Scanning, Masquerading, Replay, Message Modification, Denial-of-Service, Wireless Spoofing, MAC Address Spoofing, IP Spoofing, Frame Spoofing, Wireless Network Probing, Detection of SSID, Detection of APs, Wireless Man-In-The-Middle (MITM) attacks, Session Hijacking attacks, etc.

## **T o p 8 T i p s f o r W i r e l e s s N e t w o r k S e c u r i t y**

Before I proceed further with some thoughts upon noticeable weaknesses in the Law regarding legal treatment of wireless hacking, let me give tip you briefly on eight things you need to know those of you who make use of wireless networks:

### Slide 13: Tips for Wireless Network Security

### 1) Change Default Administrator Passwords (and Usernames)

Changing the default password is important because everyone that purchases the same Wireless access device knows your password.

### 2) Turn on (Compatible) WPA / WEP Encryption

By default, your Wireless device comes without the encryption enables. WPA / WEP are security programs that forced your computer to provide an encrypted password before you are allowed access to the wireless access point.

### 3) Change the Default SSID

SSID is the network name of your wireless network; most people leave the default name, such as, Linksys or NetGear. By changing the name, intruders have a more difficult time identifying your system and use known vulnerabilities. (And of course, use the unchanged default password.) One mistake people make is naming their home network their family name and or address.

### 4) Disable SSID Broadcast

In Wi-Fi networking, the access point or router typically broadcasts the network name (SSID) over the air at regular intervals. This feature was designed for businesses and mobile hotspots where Wi-Fi clients may come and go. In the home, this feature is unnecessary, and it increases the likelihood an unwelcome neighbour or hacker will try to log in to your home network.

### 5) Assign Static IP Addresses to Devices

Most home networkers gravitate toward using dynamic IP addresses. This means that the IP Address, (the IP Address is needed to participate on a network.) is typically assigned automatically. A dynamic IP address on an unsecured system can also supply a hacker with a IP Address.

#### 6) Enable MAC Address Filtering

Each piece of Wi-Fi gear possesses a unique identifier called the “physical address” or “MAC address.” Access points and routers keep track of the MAC addresses of all devices that connect to them. Many such products offer the owner an option to key in the MAC addresses of their home equipment that restricts the network to only allow connections from those devices. Do this, but also know that the feature is not as powerful as it may seem. Hacker software programs can fake MAC addresses easily.

#### 7) Turn Off the Network During Extended Periods of Non-Use

The ultimate in security measures for any wireless network is to shut down, or turn off your wireless access point when you are not using. You are the most vulnerable at work or asleep, and mischief minded people know it.

#### 8) Position the Router or Access Point Safely

Wi-Fi signals normally reach to the exterior of a home. A small amount of “leakage” outdoors is not a problem, but the further this signal reaches, the easier it is for others to detect and exploit. Wi-Fi signals often reach across streets and through neighbouring homes. When installing a wireless home network, the position of the

access point or router determines its reach. Try to position these devices near the centre of the home rather than near windows to minimize this leakage.

## **W e a k n e s s   i n   t h e   L a w p u n i s h i n g   t h e   c r i m e   o f   h a c k i n g**

### Slide 14: Weakness in the Law

In all European Community members' legal systems hacking is a crime punished by Law. Therefore, it is not a question whether hacking is a crime, but rather it is worthwhile to consider what kind of a crime—how serious a crime—hacking of wireless networks is. I'm elaborating upon this point because in some EC-members' jurisdictions hacking is not discouraged by Law simply because the Law does not imposed any serious consequences upon those who commit the crime and are found guilty in a Court of Law. In legal systems wherein the rule is that hacking is treated as a minor offence, an infringement, while the exception to the rule—if any—is that hacking is treated as a serious offence, a misdemeanour, the Law's scope from an anti-crime preventive perspective does not produce the desired result. In these jurisdictions, Authorities do not even bother arresting or prosecuting hackers simply because they have more serious crimes to deal with.

But hacking is a crime in which the objective part considers a high risk for all civil property or human rights set at stake by that criminal action. Therefore, it is beyond any understanding what makes an EC-member State Regulator passing Laws in their country that punish hacking, for instance, with a three-month sentence while at the same time the property set at risk or even damaged or the rights violated by a hacker's actions

may have a significant value for their holder. A Court of Law which has imposed a three-month sentence on a hacker does not discourage him from committing the same crime in the future. It simply makes him pause for a while his illegal behaviour.

The legal systems, in which the Law does not cater for hacking as a serious offence as a rule and as a felony as an exception to the rule, are usually incapable to catch up with technological development and changes caused in society because of the penetration of sophisticated technology and especially the application of wireless technology such as Wi-Fi and Wi-Max in citizens' daily life. Thus, for instance, in a country wherein hacking of a wireless network is punished as a minor offence, it is usually hard to project the effectiveness of that country's anti-crime policy in as much as it is hard to prosecute effectively hackers if there is no well organised, financed and trained Computer Crime Police Department.

**Slide 15: Weakness in the Law**

Another regulatory problem which some EC-member countries have faced pertains to the collaboration of the so called Independent Authorities such as the Data Protection Authority, the Authority for Information and Communication Security and Privacy, the National Telecommunications and Post Commission or any other local Authority which by Law is empowered upon related to the subject of this lecture fields of law. First of all, allow me to express my concerns regarding how independent these Authorities they really are. While theoretically the meaning of independency of these Authorities, which is usually provisioned by Constitutional Law, can only be understood in a "black or

white” sense—there is no sense in little independency—in reality independency of said Authorities is questionable. Said Authorities are not Courts of Law, they are not organizations belonging to the Judicature in a State’s system. In most cases, said Authorities are part of the Public Administration which is usually set by the Governmental Party. When the Government commands the selection of Independent Authorities personnel, then there is hardly any independency of them.

But aside from that independency issue, a major problem larks in making the many Independent Authorities of one country collaborate among them smoothly. And this problem is more than evident in cases wherein Laws provision overlapping competencies among Independent Authorities. What we usually see under these circumstances is an irrational dispute among Independent Authorities which they perceive—each one for itself—that only they and no one else must have the right to intervene when a hacking case crops up. Wherever there is this kind of dispute among Independent Authorities, there is certainly a major regulatory problem to deal with.

**Slide 16: Weakness in the Law**

Another issue in preventing hacking though a legal system pertains to the international collaboration of locally based and internationally based Authorities. There have been a number of proposals in recent years for some form of international co-operation on computer crime. These have often been made on the basis of economic rather than crime concerns, by groups such as the Organisation for Economic Co-operation and Development (OECD). Efforts have been made to establish increased co-operation on the use of extradition, and to deal with questions of

jurisdiction within that. This does not solve the problem, of course, of variation and incompatibility between different legal systems provisioning for computer crime. But it is a mandatory step to take in the cross-boundary regime of wireless hacking, and Cyber-Crime generally speaking.

The European Union has made some progress on a co-ordinated approach to computer crime. With the Maastricht Treaty the work of the European Union has extended to a new “Third Pillar” of home affairs and justice. This has spawned the European project, ENFOPOL, that is Enforcement Police, part of which involves setting standards for the monitoring and investigation of computer crime. While the framework within which ENFOPOL operates is still disputed, especially from a human rights and civil liberties perspective within the EC, the ENFOPOL project per se indicates that only through international collaboration and intra-organizational planning could Cyber-Crime be confronted successfully. This fact is also evident in The Cyber-Crime Convention of the Council of Europe that is a major step forward against the threats of illegal activity committed online. Lithuania ratified the Cyber-Crime Convention on March 18, 2004, and the Convention has entered into force as of July 1<sup>st</sup>, 2004.

## **C o m p u t e r C r i m e p r o v i s i o n s i n t h e L i t h u a n i a n L e g a l S y s t e m**

**Slide 17: The Lithuanian Legal System**

Lithuanian legislation does not provide for a specific law on Cyber-Crimes; however, several legal acts can be applied to computer crimes and offences. Computer crimes are criminalised by the new Criminal

Code of the Republic of Lithuania, enacted as of the year 2000, which includes certain crimes against informatics (destruction or modification of computer information, destruction or modification of computer programmes, appropriation and dissemination of computer information). Computer offences such as spamming, and unauthorized access to transmissions are also penalized by the Administrative Code of the Republic of Lithuania.

In addition, specific legislation regulates separate aspects of computer related activities. For example, the Law on Copyright and Related Rights of the Republic of Lithuania regulates the protection of computer programmes, databases and copyrights related thereto. The Law on Legal Protection of Personal Data of the Republic of Lithuania, the Law on Electronic Communications of the Republic of Lithuania and the Law on Advertising of the Republic of Lithuania inter alia prohibit spam and other forms of unsolicited communications.

The procedure of investigation of computer crimes is mainly governed by the Code of Criminal Procedure of the Republic of Lithuania. The procedure of investigation of certain other forms of computer misconduct and misuses is governed by the Administrative Code, the Law on Administrative Proceedings of the Republic of Lithuania and other legal acts.

#### Slide 18: The Lithuanian Legal System

There are currently no special legal acts in the Republic of Lithuania with regard to reporting of violations not related to content. However, reports on any misuse of computers and network are in practice accepted by the

following institutions through the phone numbers and email addresses for general contacts:

1. National Consumer Rights Protection Board under the Ministry of Justice of the Republic of Lithuania;
2. Information Society Development Committee under the Government of the Republic of Lithuania;
3. State Data Protection Inspectorate.
4. Criminal offences related to computers and network misuse may also be reported to local police authorities.

**Slide 19: Thank You!**

That said, while I believe that Lithuania is on the right path regarding its legal framework for regulating hacking and Cyber-Crime, generally speaking, yet it seems there is a long way to go ahead. This fact should not discourage you. It should only ring you a bell and make you go faster towards the EC regulatory framework direction. Moving in that direction, you could avoid hazards, some of which I have just mentioned to you, which could only delay your country's full harmonization to the EC environment and refrain foreign direct investments in Lithuania.

Thank you for your attention!