SECURITY IN THE ERA OF MOBILE WIRELESS ENTERPRISES

STEGĂROIU CARINA-ELENA,
LECTURER PHD, „CONSTANTIN BRÂNCUŞI" UNIVERSITY, TÂRGU JIU, ROMANIA
carinastegaroiu@yahoo.com

Abstract

In modern times, the mobility of people and data are becoming essential to business. An important role in this development is played by wireless technology, but the risks to users of wireless technology have increased as the service has become more popular.

As mobility and the use of smaller, personal devices increases, it is obvious that the security must be implemented as close to the source as possible, meaning in all end devices, but such solutions are difficult to deploy and very hard to manage.

Wireless security is just an aspect of computer security, however organizations may be particularly vulnerable to security breaches.

There are effective countermeasures (like disabling open switchports during switch configuration and VLAN configuration to limit network access) that are available to protect both the network and the information it contains, but such countermeasures must be applied uniformly to all network devices.

Consequently, a security policy must be described and written down to allow managers as well as technicians to react correctly to undesired circumstances

Key words: *wireless security, internet, security policyl*

JEL Classification : *A10, B23, C61*

1. Introduction

The advent of the Internet brought with it a great deal of excitement around the ability to deliver dynamic content to the consumer. However, soon, corporations realized that the Internet is not only a more convenient and inexpensive way to communicate, but also a modern day marketing, sales and distribution channel. Nowadays, millions of business-to-business transactions are being executed over the Internet, across supply and distribution chains and with numerous enterprise resource applications.

As a result of this development, new business models and services are being invented, as part of a complex society of networks, partnerships and people. That is to say, companies must be able to work with customers and suppliers form any location; enterprises must be able to distribute and provide access to information across the globe and around the clock and employees need to access up-to-date corporate information remotely. This has lead to confidential information being created, stored and accessed outside corporate networks. Consequently, this information has become more and more accessible via public non-secure networks, leaving the critical challenge to become the protection of corporate information everywhere and at all times.

An important role in this development is played by wireless technology, but the risks to users of wireless technology have increased as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Crackers had not yet had time to latch on to the new technology and wireless was not commonly found in the work place. However, there are a great number of security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. Cracking methods have become much more sophisticated and innovative with wireless. Cracking has also become much easier and more accessible with easy-to-use Windows or Linux-based tools being made available on the web at no charge.

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks [1]. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits, as mentioned before. However, wireless networking is prone to some security issues. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into wired networks.[1]As a result, it's very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless Intrusion Prevention

Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies [6].

Some organizations that have no wireless access points installed do not feel that they need to address wireless security concerns. In-Stat MDR and META Group have estimated that 95% of all corporate laptop computers that were planned to be purchased in 2005 were equipped with wireless. Issues can arise in a supposedly non-wireless organization when a wireless laptop is plugged into the corporate network. A cracker could sit out in the parking lot and gather info from it through laptops and/or other devices as handhelds, or even break in through this wireless card-equipped laptop and gain access to the wired network.

2. Security of the mobile workforce

As mobility and the use of smaller, personal devices increases, it is obvious that the security must be implemented as close to the source as possible, meaning in all end devices. The worst situation regarding the security of a network is that in which a breach occurs without our knowledge. The longer a hacker is attached to the systems in our network, the greater the damage will be. We are not talking only of the initial damage – sensitive information theft or destruction of important data – but also of the time we are granting the hacker to plant the germs of a future infestation.

The 'Perimeter Defense' solution based on firewalls, Virtual Private Networks (VPNs) and intrusion detection gateways is not viable any more, because these solutions are physically tied to the office building and the network cabling in it. For example, an employee may think that he is secure since his Internet connection is going through a secure ISP, but what the employee does not realize is that, as soon as he begins to roam outside the area covered by his ISP, his security goes away.

Anyone within the geographical network range of an open, unencrypted wireless network can 'sniff' or capture and record the traffic, gain unauthorized access to internal network resources as well as to the Internet, and then use the information and resources to perform disruptive or illegal acts.

If router security is not activated or if the owner deactivates it for convenience, it creates a free hotspot. Since most 21st-century laptop PCs have wireless networking built in (cf. Intel 'Centrino' technology), they don't need a third-party adapter such as a PCMCIA Card or USB dongle [5]. Built-in wireless networking might be enabled by default, without the owner realizing it, thus broadcasting the laptop's accessibility to any computer nearby.

Modern operating systems such as Linux, Mac OS, or Microsoft Windows make it fairly easy to set up a PC as a wireless LAN 'base station' using Internet Connection Sharing, thus allowing all the PCs in the home to access the Internet via the 'base' PC [3]. However, lack of knowledge among users about the security issues inherent in setting up such systems often may allow others nearby access to the connection. Such "piggybacking" is usually achieved without the wireless network operator's knowledge; it may even be without the knowledge of the intruding user if their computer automatically selects a nearby unsecured wireless network to use as an access point.

The best way to counter these threats is to ensure that the corporate security policies are enforced at all times, by everyone. Next, we will focus on three principal ways of securing information via a wireless network.

Firstly, for closed networks (such as organizations) the most common way is to configure access restrictions in the access points. Those restrictions may include encryption and checks on MAC address. Another option is to disable ESSID broadcasting, making the access point difficult for outsiders to detect. Wireless Intrusion Prevention Systems can be used to provide wireless LAN security in this network model.

Secondly, for commercial providers, hotspots, and large organizations, the preferred solution is often to have an open and unencrypted, but completely isolated wireless network. The users will at first have no access to the Internet nor to any local network resources. Commercial providers usually forward all web traffic to a captive portal which provides for payment and/or authorization. Another solution is to require the users to connect securely to a privileged network using VPN.

Thirdly, wireless networks are less secure than wired ones; in many offices intruders can easily visit and hook up their own computer to the wired network without problems, gaining access to the network, and it's also often possible for remote intruders to gain access to the network through backdoors like Back Orifice. One general solution may be end-to-end encryption, with independent authentication on all resources that shouldn't be available to the public.

There is no ready designed system to prevent from fraudulent usage of wireless communication or to protect data and functions with wirelessly communicating computers and other entities. However there is a system of qualifying the taken measures as a whole according to a common understanding what shall be seen as state of the art. The system of qualifying is an international consensus as specified in ISO/IEC 15408.

A Wireless Intrusion Prevention System (WIPS) is a concept for the most robust way to counteract wireless security risks. However such WIPS does not exist as a ready designed solution to implement as a software package. A WIPS is typically implemented as an overlay to an existing Wireless LAN infrastructure, although it may be deployed standalone to enforce no-wireless policies within an organization. WIPS is

considered so important to wireless security that in July 2009, the Payment Card Industry Security Standards Council published wireless guidelines for PCI DSS recommending the use of WIPS to automate wireless scanning and protection for large organizations.

Once the new technologies were introduced in the operating, transmitting and storing of data processes, a series of threats and vulnerabilities have begun affecting the information system. But, since nowadays, using computers and IT programmes has become a vital element in the informational system of a company, managers must deal with guarateeing the fairness and security of the operations within the information systems and converging these objectives with the organizational strategies.

3. An integrated solution to wireless security

There are two axes that need to be considered when discussing integrated security: the distribution axis and the management axis.

Distribution defines how far and how widely security is managed. We have previously mentioned the perimeter solution and the problems wireless technology development has caused for this option. The alternative was to rely on individual products to secure each device – often depending on the end user to install and run the products. Because of device specific management, such solutions are difficult to deploy and very hard to manage.

Moreover, nowadays, there is almost full wireless network coverage in many urban areas - the infrastructure for the wireless community network (which some consider to be the future of the internet) is already in place. One could roam around and always be connected to Internet if the nodes were open to the public, but due to security concerns, most nodes are encrypted and the users don't know how to disable encryption. Many people consider it proper etiquette to leave access points open to the public, allowing free access to Internet. Others think the default encryption provides substantial protection at small inconvenience, against dangers of open access that they fear may be substantial even on a home DSL router [2].

The density of access points can even be a problem - there are a limited number of channels available, and they partly overlap. Each channel can handle multiple networks, but places with many private wireless networks (for example, apartment complexes), the limited number of Wi-Fi radio channels might cause slowness and other problems.

According to the advocates of Open Access Points, it shouldn't involve any significant risks to open up wireless networks for the public:

- The wireless network is after all confined to a small geographical area. A computer connected to the Internet and having improper configurations or other security problems can be exploited by anyone from anywhere in the world, while only clients in a small geographical range can exploit an open wireless access point. Thus the exposure is low with an open wireless access point, and the risks with having an open wireless network are small. However, one should be aware that an open wireless router will give access to the local network, often including access to file shares and printers.
- The only way to keep communication truly secure is to use end-to-end encryption. For example, when accessing an internet bank, one would almost always use strong encryption from the web browser and all the way to the bank - thus it shouldn't be risky to do banking over an unencrypted wireless network. The argument is that anyone can sniff the traffic applies to wired networks too, where system administrators and possible crackers have access to the links and can read the traffic. Also, anyone knowing the keys for an encrypted wireless network can gain access to the data being transferred over the network.
- If services like file shares, access to printers etc. are available on the local net, it is advisable to have authentication (i.e. by password) for accessing it (one should never assume that the private network is not accessible from the outside). Correctly set up, it should be safe to allow access to the local network to outsiders.
- With the most popular encryption algorithms today, a sniffer will usually be able to compute the network key in a few minutes.
- It is very common to pay a fixed monthly fee for the Internet connection, and not for the traffic - thus extra traffic will not be detrimental.
- Where Internet connections are plentiful and cheap, freeloaders will seldom be a prominent nuisance.

On the other hand, the management axis defines how security is controlled and implemented – in a fragmented way, managing every device separately, or in a centralized fashion using policy based management. Taking into consideration the implications mentioned above, the solution is to base security on corporate policies and ensure that the policies are enforced on every device – whether remote or local – at all times. This would

mean that such policies are set once and distributed everywhere. Consequently, we also need to ensure that the various software and hardware components used to enforece these policiesare aware of one another and work well together.

One benefit of such an integrated approach is that the enterprise can purchase products and support from a single organization. This would reduce the cost of training and implementation and provides a more comprehensive infrastructure for managing security across the widely distributed enterprise. Another benefit is that it reduces the distance between the increasing value of information - and of connectivity to business – and the decreasing level of internal security expertise. A well- implemented integrated security solution can provide global immediacy [7].

4. Conclusions

Security in computer world determines the ability of the system to manage, protect and distribute sensitive information. Data Security was found many years before the advent of wireless communication due to the mankind's need to send information (in war or in peace time) without exposing its content to others. The first and most known machine (Enigma) was used in WWII by the German military to encrypt their messages. The machine was something similar to a simple typing machine with a scrambler unit to obfuscate the content of the messages [4].

From that time till now, many solutions to security threats have been introduced, and most of them were abandoned or replaced by better security standards. These ongoing changes promoted the security field to be a permanent hot topic. In the wireless world security threats were not known to public people till prices of wireless equipment went down around 2000. Before that date, the military was the number one client for wireless security products especially during the cold war.

Over the years, the realization of the benefits of wireless technology began to sweep through corporations. In the business world, with it frantic pacing, time is the most precious commodity and wireless solutions provided services which were: automatic, invisible, always on and up-to-date.

Wireless data networks have spread between home users and companies in an increasing fashion. The main reason behind this fast adaptation is due to the nature of wireless networks where it provides the flexibility and freedom that wired networks lack. The increasing of bandwidth capabilities has inspired people to think seriously about replacing wired networks with wireless networks especially in places where it is hard or expensive to have wired networks. As mentioned before, the main difference between wired and wireless networks is the medium it transfers its data through. This difference made the burden of securing the network heavier. The broadcast nature of wireless networks makes it easy for everyone to attack the network if not secured, due to the absence of physical barriers, where the range of wireless transmission ranges from 300 ft to half a mile

This means that the exponential growth of wireless networks add another obstacle on enhancing the network security. Also such enhancement of security is expensive in terms of time, money and effort that many users do not have or wish not to spend. It is not surprising that the main reason for security breaches is the human error factor or what is known as social engineering.Consequently, a security policy must be described and written down to allow managers as well as technicians to react correctly to undesired circumstances.

There are three levels of security policy that must be taken into consideration:

- Organization specific,
- Issue specific (for certain types of technologies)
- Systems-specific for individual PCs that hold important information

The availability of the wireless network and the downtime for the network must be taken into consideration while writing these specifications .

However, security hazards will always be around, but they can only be avoided if the correct policies and standards are used. Security still evolves and it will remain a hot topic as long as there are ways to threaten data security.

5. References

[1] **Oprea D.**, *Protecţia şi securitatea informaţiilor*, Ediția a II-a, revăzută şi adăugită, Editura Polirom, Iaşi, 2007.
[2] **Mihai I. C., Popa I. F.**, *Securitatea în Internet*, Editura Sitech, Craiova, 2008.
[3] **Popa S. E.**, *Securitatea sistemelor informatice*, note de curs şi aplicaţii pentru studenţii Facultăţii de Inginerie, Universitatea din Bacău, 2007.
[4] **Senft S., Gallegos F**., *Information Technology Control and Audit*, Auerbach Publications, 2009.
[5] Design and Implementation of WLAN Authentication and Security(2010) - ISBN 978-3-8383-7226-6
[6] "The Evolution of 802.11 Wireless Security". ITFFROC. 2010-04-18
[7] http://www.cse.wustl.edu/~jain/cse574-06/ftp/wireless_security.pdf