Floppy Disk and Removable Drives

Since the advent of the CD-ROM, the floppy disk drive has largely been relegated to a minor role as an alternative system boot service.

LS-120(Super Disk) drives, which is a floppy drive that can read and write not only the standard 720kB and 1.44MB formats but a high capacity 120MB format as well.

Super Disk drive functions don't need a standard floppy. Zip drive need to install a conventional floppy for backward compatibility, system configuration and system maintenance issues.

CD/DVD-ROM Drive

A CD/DVD-ROM drive should be considered a mandatory item in any PC construction. This is because virtually all software is now being distributed on CD-ROM, and many newer titles are on DVD. DVD drives can read CD-ROM drives as well as DVD-ROMs, so they are more flexible.

DVD-ROM is a high-density data storage format that uses a CD sized disc to store a great deal more data than a CD-ROM from 4.7 – 17GB, depending on the format.

These drives can read standard drums and audio CDs as well as the higher capacity DVD data and video discs.

Keyboard and Pointing Device (Mouse)

Two types of keyboard connectors are found in systems today. The purchasing keyboard must be matched with the connectors on the motherboard.

8. Explain about motherboard installation. (20 marks)

When order the motherboard with a processor or memory, it will normally be installed on the board but may also be included separately.

Preparing the new motherboard

Before install the new motherboard, it should install the processor and memory. This normally be much easier to do before the board is installed in the chassis.

Most processors today run hot enough to require to some form of heat sink to dissipate heat from the processor. To install the heat sink, use the following prodedures:

1. Take the new motherboard out of the anti-static bag it was supplied in and set it on the bag or the anti-static mat.

2. Install the processor. There are two procedures, one for socketed processors, and the other for slot based processor.

Socketed processors

The procedure is as follows:

Find the pin 1 on the processor. Next, find the corresponding pin 1 of the ZIF socket for the CUP on the motherboard or there may be a bevel on one corner of the socket. Insert the CUP into the ZIF socket by lifting the release lever until it is vertical. Then align the pins on the processor with the holes in the socket and drop it down into place.

If the processor does not go all the way into socket, check for possible interface or pin alignment problem but make sure it is fully seated and there is no gap between the bottom of the processor with the holes in the socket and drop it down into place.

Check for proper alignment and any possibly bent pins. If necessary, use a small needle nose pliers to carefully straighten to any pins.

Don't bend them too much or they will break off. When the processor is fully seated in the socket, push the locking lever on the socket down until it latches to secure the processor.

Slot based processor

Start by positioning the two universal retention mechanism brackets on either side of the processor slot so that the holes in the brackets line up with the holes in the motherboard. Push the included fasteners through the mounting holes in the retention bracket and motherboard until it snaps into place.

3. If the CPU does not already have a heat sink attached to it, attach it now. Most heat sinks will either clip directly to the CPU or to the socket with one or more retainer clips. Be careful when attaching the clip to the socket.

In most cases, it is a good idea to put a dab of heat sink thermal transfer compound on the CPU before installing the heat sink.

This prevents any air gaps and allows the heat sink to work more efficiently.

4. Refer to the motherboard manufacturer's to set the jumpers, if any, to match the CPU going to install. Look for the diagram of the motherboard to find the jumper location and look for the tables for the right settings for CPU.

If the CPU was supplied already installed on the motherboard, the jumpers should already be correctly set, but it is still a good idea to check them.

9. Describe connect of the power supply, replacement of the cover and connection of the external cables. (10 marks)

To attach the power connector from the power supply to the motherboard, do the following:

1. If the system uses a single ATX style power connector, plug it in, it can go on only one way. If two separate six-wire connectors are used, the two black ground wires on the ends of the connectors must meet in the middle. Align the power connectors such that the black ground wires are adjacent to each other and plug in the connectors. Consult the documentation with your board to make sure the power supply connection is correct.
2. Plug in the power lead for the CPU fan if one is used. The fan will either connect to the power supply via a disk drive power connector or it may connect directly to a fan power connector on the motherboard.

Replace the cover and connect external cables

Use the following procedures to complete the assembly:

1. Side the cover onto the case.
2. Before powering up the system, connect any external cabels
3. Plug the 15-pin monitor cable into the video card female connector.
4. Attach the phone cord to the modem.
5. Plug the round keyboard cable into the keyboard connector and plug the mouse into the mouse port or serial port.

10. Explain connect I/O and other cable to the motherboard. (20 marks)

There are several connections that must be made between a motherboard and the case. If the motherboard has onboard I/O, use the following procedures to connect the cables:

1. Connect the floppy cable between the floppy drives and the 34 pin floppy controller connector to the motherboard.
2. Connect the IDE cables between the hard disk, IDE CD-ROM, and athe 40-pin primary and secondary IDE connectors on the motherboard.
3. On non-ATA boards, a 25-pin female cable port brackets in normally used for the parallel port.
4. If the ports don't have card slot-type brackets, the essential expansion slots may be port knockouts on the back of the case that can use instead.

5. Advanced motherboards include a built-in mouse port. The connector for this port is not built into the back of the motherboard. In that case, plug the cable into the motherboard mouse connector and then attach the external mouse connector bracket to the case.
6. Attach the front panel switch, LED, and internal speaker wires from the case front panel to the motherboard.

11. Explain running the Motherboard BIOS setup program. (CMOS setup)

(20 marks)

Now that everything is connect, the system will also test itself to determine whether there are any problems:

1. Power on the monitor first, and then the system unit, observe the operation via the screen and listen for any beeps from the system speakers.
2. The system should automatically go through a power-on self-test (POST) consisting of video BIOS checking, RAM testing and usually an installed component report. If there is a fatal error during the POST, you may not see anything on screen and the system might beep several times, indicating a specific problem. Check the motherboard BIOS documentation to determine what the beep bodes mean.
3. If there are no fatal errors, you should see the POST display on screen. Depending on the type of motherboard, press a key or series of keys to interrupt the normal boot sequence and get to the setup program screen that allow you to enter the important system information. Normally, the system will indicate via the onscreen display which key to press to activate the BIOS setup program during the POST, check the motherboard manual for the key to press to enter the BIOS setup.
4. After the setup program is running, use the setup program menus to enter the current data and time, your hard drive settings, floppy drive types, video cards, keyboard settings and so on. Most new motherboard enters any parameters for it.

5. Once you gave checked over all the setting in the BIOS setup, follow the instructions on the screen or in the motherboard manual to save the settings and exit the setup menu.

12. Explain troubleshooting new installations. (20 marks)

At this point, the system should reset and attempt to boot normally from either a floppy disk or hard disk. The system should boot from Drive A and either reaches an installation menu or an A: prompt. If there are any problems, there are some basic items to check.

If the system won't power up at all, check the power cord. If the cord is plugged into a power strip, make sure the strip is switched on. There is usually a power switch on the front of the case, but some power supplies have a switch on the back as well.

Check to see if the power switch is connected properly inside the case. There is a connection from the switch to the motherboard, check both ends to see that they are connected properly.

Check the main power connector from the supply to the board. Make sure the connection are seated fully and if the motherboard is a Baby-AT type, make sure they are plugged in with the correct orientation and sequence.

If the system appears to be running but you don't see anything on the display, check the monitor to ensure that it is plugged in, turned on, and properly connected to the video card.

Make sure the monitor cord is securely plugged into the cord. Check the video card to be sure it is fully seated in the motherboard slot. Remove and reseat the video card and possibly try a different slot if it is a PCI card.

If the system beeps more than once, the BIOS is reporting a fatal error of some kind, look in the BIOS section for a table of beep codes.

13. How are POST errors displayed? (20 marks)

The POST-tests normally provided three types of output messages: audio codes, onscreen text messages, and hexadecimal numeric codes that are sent to an I/O port address.

POST errors can be displayed in the following three ways:

- **Beep codes – Heard through the speaker attached to the motherboard**
- **POST checkpoint codes – A special card plugged into either an ISA or a PCI card slot is required to view these codes.**
- **Onscreen messages – Error messages displayed onscreen after the video adapter is initialized.**

BIOS POST Beep Codes

Beep codes are used for fatal errors only, which are errors that occur so early in the process that the video card and other devices are not yet functional. Because no display is available, these codes take the form of a series of beeps that identify the faulty component. When your computer is functioning normally you should hear one short beep when the system starts up at the completion of the POST.

BIOS POST Checkpoint Codes

POST checkpoint codes can be used to track the system progress through the boot process from power-on right up to the point at which the bootstrap loader runs. When placing a POST code reader card into a slot, during the POST, will see two digit hexadecimal numbers flash on the card's display. If the system stops unexpectedly or hangs, can identify the test that was in progress during the hang from the two-digit code. This step usually helps to identify the malfunctioning component.

BIOS POST Onscreen Messages

Onscreen messages are brief messages that attempt to indicate a specific failure. These messages can be displayed only after the point at which the video adapter card and display have been initialized.

Most POST-code cards come with documentation listing the POST checkpoint code for various BIOS versions. If your BIOS is different from what I have listed here, consult the documentation for your BIOS or the information that come with your particular POST card.

14. Explain Hardware Diagnostics. (20 marks)

Many types of diagnostic software are used with specific hardware products.

SCSI Diagnostics

SCSI is an add-on technology, and most SCSI host adapters contain their own BIOS that enable you to boot the system from a SCSI hard drive. The SCSI BIOS contains configuration software for the adapter's various features and diagnostics software as well.

For SCSI adapters that use direct memory access (DMA) a Host adapter diagnostics feature is available which tests the communication between the adapter and the main system memory array by performing a series of DMA transfer. It this test fails, you are instructed how to configure the adapter to use a lower DMA transfer rate.

Network Interface Diagnostics

Network adapters have testing capabilities –

- **Register Access test**
- **EEPROM vital data test**
- **EEPROM configurable data test**
- **FIFO loopback test**

- **Interrupt test**
- **Ethernet core loopback test**
- **Encoder/ Decoder loopback test**
- **Echo exchange test**

15. Explain Hardware Boot Process. (10 marks)

The term boot comes from the word bootstrap and describes the method by which the PC becomes operational. Just as you pull on a large boot by the small strap attached to the back, a PC loads a large operating system by first loading a small program that can then pull the operating system into memory. The chain of events begins with the application of power and finally results in a fully functional computer system with software loaded and running. Each event is triggered by the event before it can initiate the event after it.

Error messages displayed during the boot process and those displayed during normal system operation can be hard to decipher.

OS Independent	OS Dependent
- Motherboard ROM BIOS	**- System files**
- Adapter card ROM BIOS extensions	**- Device drivers**
- Master boot record	**- Shell program**
- Volume boot record	**- Program run by autoexec.bat, the window startup group and the Registry**
	- Window (win.com)

16. What are sample weekly and monthly maintenance procedures? (10 marks)

The following is a sample weekly disk maintenance checklist.

- **Backup any data or important files.**
- **Delete all temporary files, such as** .tmp, ~.*, ***.chk, web browser history and temporary Internet files.**
- **Empty the Recycle Bin.**
- **Finally run the defragmenting program.**

The following are some monthly maintenance procedures should perform:

- **Create an operating system startup disk.**
- **Check for and install any updated drivers for video cards, modems and other devices.**
- **Check for and install any operating system updates.**
- **Check for and install antivirus software updates.**
- **Clean the system, including the monitor screen, keyboard, CD/DVD drives, floppy drives, mouse and so on.**
- **Check that all system fans are operating properly, including the CPU heat sink, power supply and any chassis fans.**

17. What are the problems during POST? (10 marks)

Problems that occur during the POST are usually caused by incorrect hardware configuration or installation. Actual hardware failure is a far less-frequent cause. If you have a POST error, check the following:

1. **Are all cables correctly connected and secured?**

COMPUTER SECURITY AND SECURITY TECHNOLOGIES

PhD Lazar Stošić, College for professional studies educators, Aleksinac, Serbia

Dragan Veličković, Master of Laws

Abstract: With the increasing development of computer and communications technology growth and increasing needs and development of information systems security. The problem of security must be approached with greater caution. With the development of computer and communication technologies have developed numerous tools to protect files and other information. A set of tools, procedures, policies and solutions to defend against attacks are collectively referred to as computer network security. It is necessary above all to define and learn about the concepts of attack, risk, threat, vulnerability and asset value.

During the design and implementation of information systems should primarily take into account a set of measures to increase security and maintenance at an acceptable level of risk. In any case, there is a need to know the risks in the information system. Sources of potential security problems are challenges and attacks, while the risk relates to the probable outcome and its associated costs due to occurrence of certain events. There are numerous techniques help protect your computer: cryptography, authentication, checked the software, licenses and certificates, valid authorization...

This paper explains some of the procedures and potential threats to break into the network and computers as well as potential programs that are used. Guidance and explanation of these programs is not to cause a break-in at someone else's computer, but to highlight the vulnerability of the computer's capabilities.

Key words *- computer security, security technologies, threats, security, protection of computer.*

SECURITY

One of the accepted definitions of security is that security is the maintenance of the level of acceptable risk. The risk is the result of accumulation of threats and weaknesses of the consequences. Since it is a process means that it must be planned and systematically monitor the system status and possible threats that can come from outside. We can not say with certainty that a system is fully protected. There is no absolute security. Everything is relative. When the protection system is necessary to accept some level of risk and the possibility that a certain loss i.e. reasonable level of risk. Since security is a process it can not pay for the purchase of a product. Each process is in a dynamic state, so the safety can be implemented using several different products and services, procedures and rules. However, the very products and services, procedures and rules are not sufficient in themselves. Need a proper and timely training of authorized persons in charge of the protection system. All that investment in staff training, procurement of goods and services, procedures and rules are far more profitable than paying damages. On the possibility of losing important data to say nothing. Must find a balance between investments in safety and immediate effects in order to reduce risk.

Security is based on four basic steps as follows:

Evaluation (assess the possible risks and predictions for their removal),

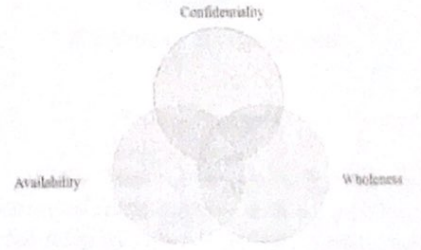
– protection (prevent potential attacks in order to reduce the possibility of compromising the system),

– discovery (the process of identifying the attack) and

– Answer (a recovery with the possibility of further work or restoration of the system itself).

Three basic principles of information security make up the trinity of "great":

- Confidentiality - an attempt to prevent the intentional, unauthorized disclosure,
- Integrity - data is a system and as such must remain and must not be changed,–
- Availability - only certain staff can access the data.



Three basic principles of information security

I'm term safety, security, refers to the preservation and protection of data in computer systems of an enterprise. Security is usually divided into safety resources, network security, security location where the data (server, etc.) and security services.

Possible attacks and threats

Since we defined that the security process, the protection system can select various security products, policies, procedures and practices. When we speak of the protection system must be protected from attacks that threaten the information systems. To protect against possible attacks have the ability to predict and know the attacks and the types of attacks. If you understand the types of attacks and ways in which they come, we can more easily monitor and control the risk of data loss.

Ensuring safety should and must become the responsibility of each system administrator. Should always pay attention and ask: "What is the probability that someone will break into a wired or wireless network, the company where you work and listen to network traffic? If this happens the measures taken? "If you do not take certain steps there is a likelihood that an attack occurs or wired wireless network.

When trying to improve security of information systems are mostly used six categories of security measures including: general security policies and procedures, software, virus protection, digital signatures, encryption, firewalls and proxy servers.[5] Security breaches and attacks on information systems most often arise from the following sources: employees of firms, hackers, terrorists, and computer viruses.

The most common steps in the attack are as follows:

- testing and Assessment,
- exploitation and penetration,
- increased privileges,
- maintenance of access,
- refusal of services.

During the attack may lead to different consequences and the most common are: the destruction of resources, theft of resources, theft of services, refusal of service, corruption of data and applications.

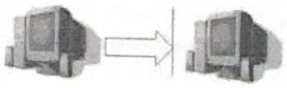
During normal flow of information data is moving from one place to another.

Normal flow of information flow

There are several types of attacks but, generally, all attacks can be classified into four categories:

1. Cutting or breaking

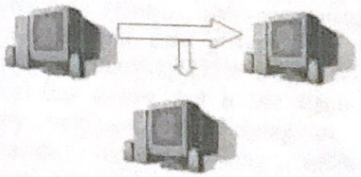
This kind of attack interrupts the flow of information in the system. This is a direct or active attack.



Cutting or interruption of information flow

2. Interception

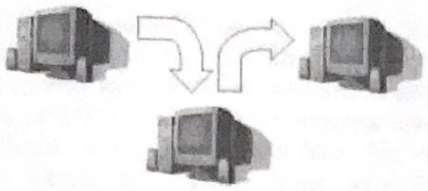
This kind of attack is difficult to see, and unlike the previous, active attacks, are a passive attack. This kind of attack the person trying to collect information or to perform monitoring of current performance. After gathering sufficient data can be exported active attack or some other kind of attack.



Interception of information

3. Changed

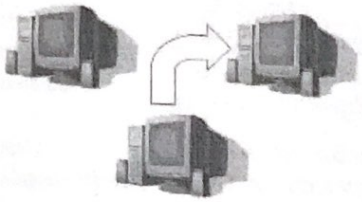
This kind of attack falls into the category of active attacks, because the attack on the integrity. There may be a changing of the data or the whole system.



Changes of information flow

4. Fabrication

This kind of attack is also an active attack and an attack on authenticity. This kind of attack is faking data, traffic etc.



Fabricating information

Attackers could use the software vulnerabilities in operating systems that allow remote programs and entities to be entered into the computer the victim and take control over it. As such, the computer becomes a kind of' "zombie" PCs that can continue to attack other computers, to burden the network and the like. No less dangerous or worms that can do damage, duplicated and converted into zombie computers.

Security of wireless networks

Today, PC cards are most frequently used in home and business networks. All computers have a security protocol called Wired Equivalent Privacy (WEP). A device using an 802.11 card is configured with a key, that in practice usually consists of a password or a key derived from a password.

Wired Equivalent Privacy (WEP) is a protocol for encrypting wirelessly transmitted packets on IEEE 802.11 networks. In a WEP protected network, all packets are encrypted using the stream cipher RC4 under a common key, the root key1 Rk. Rk is the WEP or root key and IV is the initialization vector for a packet. $K = Rk \| IV$ is the session or per packet key. X is a key stream generated using K. The WEP protocol is designed to provide privacy to packet based wireless networks based on the 802.11b standard [7]. The WEP encrypts by taking a secret key and a per-packet 3 byte IV, and using the IV followed by the secret key as the RC4 key. The attacker is able to retrieve the first byte of the RC4 output from each packet.[6]

The potential risks with the advent of wireless networks with manifold increase. Wireless is greatly vulnerable for the simple reason - incompetence that's been properly adjusted. We said that there is no absolute security. The same is true of networks. By placing an increasing number of "hot spots" (the location where the greatest number of people - cafes, parks for the rest ...) opens up the possibility that data theft and intrusion in the user's computer. Wireless networks are defined in IEEE 802.11, which brought the IEEE (Institute of Electrical and Electronics Engineers). Initial version of the IEEE 802.11 standard with the 2.4 GHz frequency and two data rates (from 1 and 2 Mb/s), which was formed in mid-1997. year. Formed by standard formed working groups - group A, B, D, E, F and G. On the IEEE 802.11 specification is based and Wi-Fi networks. In the beginning it was designed for mobile computing devices (laptop computers, Internet access, VoIP, games ...).

Looking at an organization as a system, we can say that the wireless network vulnerable part of the system. Standards often fail to meet the three basic security requirements: reliable user authentication, authorization and user privacy. The first security mechanism (WEP-Wired Equivalent Privacy) has shown that it has significant security vulnerabilities. Relying on this mechanism without taking additional measures did not show good results. He later followed WEP2, EAP, WPA ... Individual explanation of these mechanisms would take away too much time and space so we can keep things in general.

The attacker broke into someone's system, the wireless network; he must first catch a signal that now is not so difficult. By capturing the signal can be performed on active or passive attacks. In the beginning, are

generally conducted passive attacks, i.e. listening for a signal and traffic between access points and users. The attached is clear that the attacker must know the physical layer is defined in the 802.11 standard. For an active attack, the attacker must have the proper equipment that can send data to the network. If the attacker does not have the service set identifier SSID - Service Set Identifier, the access point rejects the connection. However, since all control frames are not sent in encrypted form, an attacker can capture the control frames sent by the access point to communicate with other network users, find out the SSID and join the network. What will still work, we assume.

Probability of interception at different locations:[1]

Location	Full description	Probability of interception
Rural / remote	In his house, which is quite distant from other houses	Extremely small
Remote connection	Connection via remote, point-to-point connection with a wireless Internet provider, or neighboring network	Small, the targeted nature of point-to-point connection
Densely populated urban place or suburb	In his home, located in a densely populated area with few houses in the near abroad	Generally high, especially if you have neighbors who use high technology, but actual attacks are unlikely.
Mixed	The neighborhood, which is a mixture of commercial and residential buildings	Generally high, because the business systems attractive targets, and most probably use the wireless network
Public places in the neighborhood	The neighborhood, near public parks, or in places where parking is allowed on the street.	Great, because public networks use different layers of the population and anonymous users.
Commercial buildings	The buildings used by a number of companies, or companies, or near the parking lot with the optical visibility of the building.	Very high, because of the proximity and attractiveness of the target.
Roaming	While on the road, in airports, hotels, cafes and other locations	Generally high, for easy tracking, but with relatively low risk because no one knows just tapping your network traffic.

Tools to attack wireless networks

In order to best protect the information system, i.e. wireless networks need to, in addition to the administrator knows these things and others familiar with the tools to attack wireless networks. The purpose of these schemes is the creation of the attacker (punishable by law), but shows the possible intrusion and abuse of wireless networks. Network administrator is desirable to test these programs in order to know the probability and the possibility of attacks that allow these programs and the ability to protect against them. Due to abuse of the program and the names of potential attacks is not mentioned in this paper. Hereby only draw attention to how the administrator can better train and what can and should be ready when it comes to wireless networks. There are tools to carry out an attack on the WEP key, tools to crack WEP encryption and the like.

Closing a wireless network (SSID hiding) is not a secure solution that the

network will not be visible. With a little trouble and patience can be detected network name. The network can detect many programs that the commercial to those who are open source and completely free. Furthermore, allowing access only to specific network adapters (MAC addresses) is not safe because it is not difficult to change MAC address wireless network adapter. Since the MAC addresses transmitted over the air, unencrypted, it is not difficult to catch such address and assign it your network adapter.

Preventing and limiting public access computer network

"The public computer network in terms of criminal law is considered a set of interconnected computers that communicate by exchanging data. A public computer network is the computer network that it is subject to certain conditions, available to everyone and it can be global in character as the internet, regional or local character.

Preventing and limiting public access computer network protecting the rights of citizens, that is, communication and information through computers, and access to a public computer network sanctioned by criminal legislation.

By *preventing access* to the public computer network involves completely disabling the second to use the computer network.

By *restricting access* to public computer network involves the creation of access difficulties and efforts to prevent it.

Prevention or obstruction should be performed without authorization, otherwise there is crime prevention and restriction of public access computer network if there is any legal basis to prevent someone access to a public computer network.

Criminal offenses against computer data is often called cyber crime. The term "cyber" is often used to describe new concepts in computer technology and terms associated with the Internet. Cyber crime would identify all criminal activities committed using computers. The Convention on Cyber crime of the Council of Europe, the terms "computer" and "cyber" crime is used as synonyms.

The term "computer" and "cyber" crime can involve all forms of computer use in crime. Often this form of high-tech crime, rather than the word "cyber" uses the term "cyberspace." The prefix "cyber" is a word that comes from the ancient Greek word derived from "cyber", hence the name of scientific disciplines, "Cybernetics".

With cyber crime, we can distinguish two types of crimes that can be done by computer.

In one group, the new criminal offenses like the spread of computer viruses, destruction of files or software etc., or crimes where the computer is a means of attack and care for the facility required separate legislation.

In the second group are the classic crimes such as fraud, child pornography, gambling, copyright infringement and the like, where the computer is used as a means of execution, and that caused it in a new form of cyber space.

The rapid growth of computer crime has led to numerous problems, which can be classified as:

- Technical problems are caused by rapid changes in technology and the inability of law enforcement to continually keep up to date, as well as technical deficiencies that make it difficult to find and prosecute perpetrators.
- Legal problems are caused by the inability of the legal framework to monitor technological developments.
- Operational problems are caused by lack of equipment, training and adequate organizational structure and the need to work at high speed regardless of time zone, language and cultural differences.

The main problem is in finding and gathering evidence." [3, 4, 8]

Conclusion

Tools that are available on the Internet, both commercial and free, they are not designed for intruder wireless networks. On the contrary, are designed to indicate the

potential weaknesses of the system, network resources and security failures so-called security holes. Knowledge of these programs is very important for administrators to better understand how to protect its network and prevent data theft. Tools that are available are usually divided into categories:

1. Tools to search the area to find the network signal, of the protection network and the strength of its signal.
2. Tools to intercept the data sent over the air and convert them into readable form, breaking the protective key.
3. Using these tools is mostly illegal and therefore punishable by law. For these reasons, the names of these tools are not mentioned in this paper. We draw attention to the administrators with the help of these programs can realize significant errors and omissions in the networks that can be used to protect your network and I have an information system.

References

1. Adam Engst, Glenn Fleishman (2004): Wireless networking, Computer Library, Cacak
2. Andy Ruth, Kurt Hudson (2004): Security + Certification, Computer CET Beograd
3. Criminal Code RS art. 112 page 18 and art. 303
4. Expert comment Code of Criminal Procedure in offenses against the security of computer data
5. James A. Seen (2007): Information technology: principles, practices, opportunities, computer library, Belgrade
6. L. Stošić, M. Bogdanović (2012). RC4 stream cipher and possible attacks on WEP, *(IJACSA) International Journal of Advanced Computer Science and Applications*, Vol. 3, No. 3, march 2012, (pp. 110-114), ISSN 2156-5570 (Online), ISSN 2158-107X (Print), https://www.thesai.org/Downloads/Volume3No3/Paper19-RC4_Stream_Cipher_And_Possible_Attacks_On_WEP.pdf
7. LAN/MAN Standard Committee, Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, 1999 edition, IEEE standard 802.11, IEEE Computer Society, 1999.
8. Ljubisa Lazarevic: Commentary of the Criminal Code of the Republic of Serbia, page. 750, 751
9. http://www.niap-ccevs.org/cc-scheme/
10. http://all.net/books/ir/nswc/incident.handle.html
11. http://www.cert.org/stats
12. http://nvd.nist.gov/