Helsinki University of Technology
Networking Laboratory
S-38.138 Special Assignment on Networking Technology

Creation of a New S-38.133 Laboratory Work: Network Security, Background Material

Author: Jan Tapper, 60172W
Supervisor: M.Sc. Niko Suominen
Date: 22.11.2004

Author:	Jan Tapper
Supervisor:	M.Sc. Niko Suominen
Title:	Creation of a New S-38.133 Laboratory Work: Network Security Background Material
Date:	22.11.2004

Abstract

The purpose of this material is to provide students general background information about security issues on networking. Understanding basics of network security is essential in order to maintain any computer network without security incidents. The aim of this laboratory work is to illustrate a few common security issues and make clear how one can be protected from attacks taking advance of these vulnerabilities.

This document covers topics handled in the laboratory work briefly but does not provide straight answers to questions in the assignment. Students should, however, get a good idea where to look for answers or what keywords to use while looking for additional information.

Cryptographic topics are not generally covered in this document because they are represented in other laboratory works in adequate scale. Wired Equivalent Privacy, WEP, is however covered, because it is a major issue in wireless LAN security in WiFi networks.

Keywords: Security, Hacker, Vulnerability, Exploit, WEP

Table of Contents

Abbreviations

AP	Access Point. Term that is used of a base station for wireless networks. In infrastructure mode mobile stations seek for an access point to associate with.
FMS	Fluhrer, Mantin and Shamir (FMS) attack is the most popular attacking method against WEP.
FTP	File Transfer Protocol, an application layer protocol for file transfer.
IDS	Intrusion Detection System is a system that can detect unauthorized use of or attacks on a system or network and act respectively.
IOS	Internetwork Operating System, is the operating system utilized by Cisco routers.
IV	Initialization Vector is used to conceal any repetive patterns in encrypted data.
MAC	Medium Access Control. In a WLAN device, the MAC is the radio controller protocol (corresponds ISO layer 2).
OSI	Open Systems Interconnect. The OSI reference model is a framework that describes the way how communication takes place.
PRNG	Pseudo Random Number Generator is a process or algorithm that generates a random sequence of numbers.
RC4	Rivest's Cipher #4. A stream cipher that is used in WEP for creating the keystream.
ROOT	A user that can do everything on a computer. Synonym for Administrator.
TELNET	A protocol for remote login.
TFTP	Trivial File Transfer Protocol. A file transfer protocol that is simplified from regular ftp to be a very minimalistic protocol.
TTL	Time To Live. Means how many hops (routers) a packet can pass before getting dropped.
VPN	Virtual Private Network. VPN is a method to create a secure connection between two or more hosts while using public Internet as medium.

WEP	Wired Equivalent Privacy is defined by 802.11 standard as the way to keep wireless medium safe from unauthorized users and prevent eavesdropping.
WiFi	Wireless Fidelity, a name given to 802.11b wireless LAN
WLAN	Wireless Local Area Network.

Network Security

Network security is typically considered as a result of certain factors. These factors vary a little depending on the source material, but normally at least the following matters are covered:

- Confidentiality
- Integrity
- Availability

This classical security triad of three important blocks is not enough to cover all aspects of the networking security these days [1]. These blocks are accompanied by these essential fields of security for fulfilling the complete security of a network:

- Nonrepudiation
- Authenticity
- Possession
- Utility

Availability

Data or service availability is easily monitored by users of a service. Thus unavailability of a service can be a stain the image of a company and even worse, cause a productive process to stall [1]. For any data network, data availability is essential for systems to function correctly.

Confidentiality

There are different kinds of information available on networks. Different data has different groups and users and data may be classified and therefore some restrictions on data rights to access data need to be set. Normally the information in any business network is confidential and access from 3rd parties is denied in order to keep trade secrets and business initiatives from getting this information [2]. Backdoors, for example, violate this because they provide unauthorized access to network. Confidentiality can be improved in some cases by encrypting information or by using VPN [22] [2], these topics are not, however, covered in this text. Access controls are a common way to restrict access to networks. A

simple but yet very powerful way of restricting access is to use username-password combinations to authenticate user and grant access on need-to-know basis [2]. In some networking security frameworks this is covered in a separate block “Authentication” [3].

Integrity

Reliable networking is also based on the fact that the data provided is what it is supposed to be. Networks must therefore be protected from attacks that could alter the data while in transit [4]. Man in the middle –type of attack could compromise data integrity as attacker could hijack sessions or manipulate the data being sent [5]. On secure networking participants of transactions need to know that the party they are communicating with is reliable and trustworthy. Security of communication is needed to be at a level that ensures that no data is altered between the sending and receiving of information. This does not necessarily mean that traffic needs to be encrypted in some way, but that there is no possibility for man in the middle attacks, for example.

Nonrepudiation

Every actions made on a secure system are logged on some level. This can be as a tool for checking if the system functions in a way that it is supposed to function. The logs are also an irreplaceable part of security system if an intrusion or other attacks occur. The logs and timestamps are, for example, valuable piece of evidence in court if a cracker is caught and prosecuted. For these reasons non-repudiation is considered as a factor of competent network security system.

ITU-T has defined nonrepudiation as follows:

1. The ability to prevent a sender from denying later that he or she sent a message or performed an action.
2. Protection from denial by one of the entities involved in a communication of having participated in all or part of the communication [7].

Networks and other data systems are built with many different components which all have their own special characteristics considering safety. A safe network needs security issues to be covered in all sectors, as the complete security chain is as weak as its weakest link [8]. Users are an important link of a chain. Social

engineering is an efficient way to find vulnerabilities on a system [17] and people tend to use relatively weak passwords. It is also common to leave workstation unlocked when leaving seat for lunch etc.

Operating systems are present everywhere. Computers have different operating systems and even routers of a network are run by operating systems. Every OS has its own properties and characters, and others are more commonly used in server environments. Some operating systems may have flaws that could be utilized in a way that causes system to stop responding.

Services on servers are playing an important role of the security. Software developers publish advisories on flaws of software in increasing pace. The reason is that it is common to exploit these flaws to attack a system and everyone running a computer, server or workstation, should check for security updated regularly.

Hardware may be difficult to consider as a potential security breach. The truth is somewhat different. If hardware is located in insecure place there is a risk that unwanted devices may be plugged into network and this could make a network-wide eavesdropping possible. Also, if network hardware can be tampered with by outsiders, devices could be reset and default configuration loaded into device. The selection of transmission methods is an important security issue too. Any confidential information should not be transmitted wireless, at least not without proper encryption, as anyone can listen to carelessly sent wireless communication. It is recommended to use firewalls to restrict access to network for suitable level. Firewall could also be the weakest link [9], as it may create feeling of absolute safety [10]. Firewalls must allow traffic into a network if there is also traffic out of the network through the firewall, and this could be a weak point. More important fact is that not all attacks come through the firewall [10].

Securing the Organization

Securing the organization is 3 phase process. For securing a network threats must be mapped out first.

Prevention

Most of the threats can be blocked out quite easily, even though total completion in safety cannot be reached. Unwanted access to network is prevented by choosing and configuring services run on the network carefully.

Observation

When a network is up and running, and unauthorized access is prevented, the maintenance process starts. Network maintenance should include looking for abnormal log entries that could lead to unobserved security matters. IDS systems can be set up as a part of observation process but using IDS should never lead to ignorance of information the logs provide.

Response

If something unwanted happens and security of a system is compromised, the maintenance personnel need to act somehow. Depending on the actual productive process and severity of security breach, proper actions should be taken. If a process is vital for system function and it would cause more losses to shutdown compromised part of system than to postpone counteractions, it should be considered if the repairing actions are taken later [1]. This is difficult matter, as one could not explicitly know what actions have been taken in system after its breach.

Victims / Statistics

Network security covers a broad variety of different pieces that affect the security in whole. Security attacks and misuse types are for example viruses, abuse of network from inside of organization, hardware theft, system penetration, denial of service attacks, sabotage, wireless network abuse, website defacement and misuse of web applications. Statistics show that the amount breaches in most of these

areas have decreased from the year 2003 numbers [24]. The variety of attack types, however, causes that almost anyone could be an interesting target.

Security Issues

Modern networks are an entity of many small components. Here is presented some weak spots of different components.

Weak Protocols

Network communications use protocols between client and server. Many of the protocols used today have been in use for many years. These old protocols, like file transmission protocol FTP, tftp or telnet [11], were not designed to be especially secure. In fact many of these protocols should be replaced by more secure ones, because there are many vulnerable spots that malicious users could exploit. For instance, one could easily monitor telnet traffic and find out usernames and passwords.

Software Issues

It is more and more common to exploit flaws in software. These flaws are usually not intentionally crafted but almost everyone seems to suffer from weaknesses like these. These flaws usually are grounded to a fact that anything that is run by root, owns root's permissions: ability to do anything on the system. The actual exploit takes advantage of weak handling of data that is not expected from user, for example buffer overflow of format string flaws are very common these days. The exploiting the flaw then leads to situation where user's privileges escalate to higher level. This is called 'rooting' a host because attacker is usually aiming for the root-privileges [2].

Buffer Overflow

Buffer overflow means exactly what it sounds like. Programmer has allocated a certain amount of memory for a specific variable. However, with this kind of flaw, this variable can be written to stack without checking if its length is allowable. If the length for data in buffer is longer than expected this probably overwrites function's return address and therefore programs execution path can be changed. Writers of malicious code usually exploit this return address overwriteablity by changing return address to shellcode of their choice to invoke

shell access with privileges of user-id of exploited program [12]. This shellcode does not have to be included in the program exploited, but it is most commonly written in the overflowing part of the buffer. It is a common trick to use environment variables for this.

Buffer overflow is a problem fundamentally based on the architecture of modern computers. The space for variables and the code itself are not separated in different memory blocks. A change in architecture could easily fix this problem, but the change would not be an easy task, because current architecture is so widespread.

Format String

Format string –attacking method is fairly new attack method, it was announced in public in later year 2000. The method, however, was discovered by hackers over 6 months before that. Fundamentally this flaw reminds common buffer overflow vulnerability quite a bit [13]. Both vulnerabilities are here because lazy, ignorant or just poorly skilled programmers. Format string flaw commonly is caused by lack of format string like "%s" in the part of program that creates output with for example printf-command. If the input is given by passing format strings like %d and %s to the program one could get the stack dump visible or use any other techniques like ones with buffer overflow flaws. The vulnerability is based on not truncated format strings from input. This leads to situation where externally supplied data is interpreted as a part of format string argument [13]. With specially crafted input one could cause vulnerable program to show contents of memory and even control the execution of program by writing anything to location of one's choice, just like in overflow exploits.

Hardware Issues

The actual hardware is usually not vulnerable to attacks. The software the hardware runs and possibly weak technical specifications on the other hand are the weak spots. Here are only a couple of examples about hardware-related security issues:

Example 1: Cisco

Very common Cisco routers were announced to have a systematic flaw in the IOS software they use as operating system in year 2003.The flaw in the software could lead to denial of service state of all router interfaces. The vulnerability is in the IOS way of handling protocols 53(SWIPE), 55(IP mobility) and 77(Sun ND) with TTL values of 0 or 1 [23]. In addition, Protocol Independent Multicast, PIM with any time to live value, could cause router to mark input queue full on interface it is sent to. As queue if full, the router will not process any traffic on the interface in question [3]. Cisco has there vulnerabilities well documented and the required patches have been available for a long time.

Example 2: Linksys

Linksys devices are reasonably cheap piece of equipment and therefore rather popular around the world. Certain Linksys devices, however, suffered from flaws which could lead to denial of service state. Vulnerabilities concerned handling URL embedded parameters sent to device.

Misconfiguration

Server and hardware misconfiguration are very common cause for hackers to get into a system. For example web page defacements are commonly executed with help of misconfiguration of the www-server software or any of its modules. Careless configuration may also ease hacking if more free options are selected. For example a system with any of certain ssh-daemons running, is much more easily hacked if usage of protocol version 1 is allowed and/or remote root logins are permitted. This clear misconfiguration would compromise system to flaws in protocol version 1, such as buffer overflow to remote user to gain root privileges, or give brute-force password crackers a chance to guess root password.

DoS, DDoS

Denial of service attacks are attacks, in which the target stops responding [5] or acts otherwise abnormally. Classic DoS attacks are “ping of death” and “syn flood” which luckily are almost extinct these days. Normally DoS attacks utilize vulnerabilities or properties of networking protocols to cause denial of service.

The other technique is to choke target with excessive amount of data sent for it to process.

Distributed DoS is more organized attack style. This needs usually preparation and usual tactics is to utilize beforehand installed backdoors on hacked servers to launch a DoS attack on a host from many sources simultaneously [5]. The notorious Mydoom internet worm was programmed to start huge DDoS attack against www.sco.com –website. The attack was successful as www.sco.com had to be removed from DNS to reestablish service [20].

Viruses

A computer virus is by one definition a program that attaches itself to other object such as executables and different kinds of documents. Besides replication, viruses may contain some sort of payload. Payload could be destructive or practically anything one can imagine. There are viruses that send files found on computer to random recipients, format hard drives, display messages etc [18]. For the virus to distribute in wild it should be undetected after it has infected a computer. If one sees signs of a virus the counteractions are probably taken quickly to clean up any infected files, and thus replication process would stop. Antivirus software detects viruses from specific signatures found from the viral code. Some viruses use polymorphic techniques to remain undetected for a longer period of time. The body of polymorphic virus changes on every infection and detection is more difficult [18]. Practically every computer platform has their own viruses but there are a few multi-platform viruses too. Multiplatform viruses are usually Windows executable / document viruses, and due to its popularity Microsoft Windows and MSOffice are the platforms most viruses are written to work on [4].

Worms

A computer worm is a program that spreads by sending itself to other systems. Worms do not attach to other objects [18]. These days many worms spread by using the fact that people do not update software on their computers. In practice this means that unpatched versions of, for instance, Outlook Express –mail reader

has functionality that allows execution of e-mail attachments even without user interaction.

Trojan Horses

Trojan horses are programs that pretend to be something harmless but are actually something else [18]. One common function of Trojan horses is installing backdoors one could utilize if wanted.

Junk Mail

Junk mail is not necessarily direct security threat, but they often use remote images that could give spammers information on ones email-address. With viruses and worms spreading by e-mail, the amount of junk-mail has also risen. The security threat with these is not actually the junk mail itself but the viruses and worms these e-mails could include.

Time Bomb

Time bombs are software that is used to execute its payload with delay. Some viruses and worms contain same kind of functionality. Time bombs differ from viruses and worms because they do not replicate but they are installed on system by, for example, innocent looking joke-programs or anything else.

Other Malware

In addition to threats mentioned earlier, there are other malware types around too. Spyware is a type of malware, almost everyone using Microsoft Windows operating system and MS Internet explorer in global internet has encountered at some point. Spyware is software that could follow user's actions and habits and report its findings to 3rd party. This kind of software usually has some advertising functionality too. It is very common that advertisement windows pop up or advertising toolbars are installed to a computer with this kind of malware. Malware is practically anything that is installed on computer against users will or this is done secretly.

Hacking: Hackers and Victims

Hackers are categorized in a few different categories depending on their profile. Most hacker are so called script kiddies who use ready made exploit code usually found on the internet [19]. If the goal of hacking is economical gain or even gaining military information the stakes are much higher and targets are carefully selected.

The reasons for hacking vary between these categories. Script-kiddies usually scan ip-blocks for possibly vulnerable hosts and try exploiting a few different daemons found from the network. One group of hackers are ones that just try something they code and see if the stunt works. Nevertheless a hacker can be a so called white-hat or a black-hat. White hat means that if a hacker succeeds in his efforts and, for example, gains access to a system, he afterwards notifies the system administrator that system is vulnerable and sometimes even points the flaw to be fixed. The purpose is usually researching and intensions are never destructive. White hats may be security professionals and hired for making penetration testing or giving security consultation.

A black-hat is a hacker that white-hat hackers call ‘crackers’. Crackers’ intensions are not so good willing. They usually break into systems in order to steal information or to prepare system for another attack, DDoS for instance. They leave no marks from their visit and never notify administrator for flaws. Black hats usually leave a backdoor on a system they crack into, to be utilized later for malicious purposes. Black hats are the ones that generate new non-public exploits that utilize flaws in software.

There is a grey area between these to categories. As nobody wants a hacker to break into a system, any intrusion is always unwanted. This is also why even hackers who do not make damage and even tell administrators what they did to break in, are not considered as white hats. They are not very destructive but still unwanted hackers could therefore be called as grey hats [19].

As script kiddies are not too discriminating when picking their targets any host on the internet could be and more likely will be targeted for intrusion attempt. Large corporations get scanned daily and they are more likely to be targeted for massive distributed denial of service attacks, because the news-value of such attack if succeeded.

Different Types of Attacking

Scanning

Scanning is a method to get as much information about target network/IP as possible. Normally scanning can be made automatically because scanning multiple addresses manually would take a long time. Hackers may gather information, for instance, are there any unpatched ftp-servers on the scanned netblock. Using gathered information hackers start to prepare the actual attack. There are plenty of scanners available for anyone to use.

Nmap is a wide spread network scanner that is very suitable for testing security of one's systems. The hackers, however, use this tool too, though there are scanners crafted for hacking purposes only.

Nessus is an advanced scanner that also reports vulnerabilities it finds. This is extremely handy tool for network administrators as it can be used to check large networks too. As any good scanner for network administrator, hackers tend to use this one too to collect data on networks they are planning to attack.

Some scanners luckily leave signs of their work, and system administrators may find out from system logs that system has been scanned. This should lead to precautions to make hackers intentions more difficult.

Password Cracking

Brute-forcing is a technique, in which all possible passwords are tried to gain access to a system. Cracking a password in this manner is slow but efficient. Every password can be cracked this way if sufficient time is provided. There are many tools available for brute-forcing passwords of different services.

As reversing a password hash is practically impossible task, there still other ways to crack passwords. If one can get a hold of a file that keeps password hashes, one efficient way is to use dictionary based cracking software, such as John the

Ripper. These programs use word lists of common passwords or regular words and their variations and try them to each user to see if the tried password is correct.

Hash Lookup Table way of password cracking is a way in which the hash of a password is compared to a huge table of password hashes. This would be very efficient way but it requires huge amount of disk space and computing power to store and create all possible hashes.

Rootkits

Rootkits are tools that hide presence of hacking software crackers may have left on compromised systems. Rootkits usually include specially crafted versions of system tools, like ps, top etc., to make appear normal by hiding processes and files intruders may have created. By setting up rootkits crackers could utilize system later without any backdoors etc. being noticed [14].

Defending

Firewalls

Computers and networks attached to public internet need to be protected from attacks. Firewalls are a common way to accomplish protection by separating public and private networks, as described in figure 1. More generally firewall separates trusted and untrusted networks. Generally firewalls are set on either network layer or application layer of OSI-model. The ones on application layer are known to use resources and are slower in their actions. Disregardless of the layer firewall is set on, there are a few different types of firewalls of which the most basic, yet very popular is packet filtering firewalls [15].

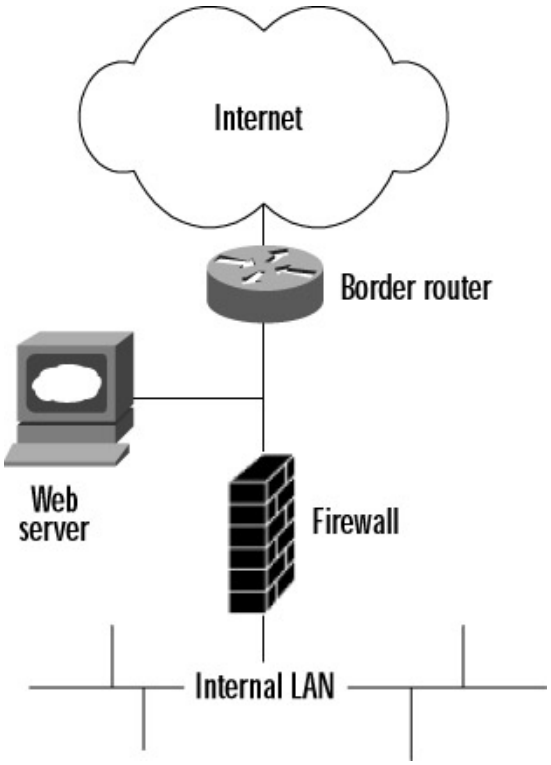

Figure 1. One possible firewall-setup. [22]

In a packet filter firewall every packet going through firewall from inside to outside network or vice versa, is taken to inspection and compared to firewall rules in use [15]. If, for example, a rule is set to disallow traffic to port 80 at a host, every packet going to port 80 are dropped. If the rule set permits the

connection, firewall forwards packet to its designated target host. The rules can also be set on port basis to allow traffic to certain ports but drop some other ports. Stateful packet filter (SPF) reminds ordinary packet filtering a lot but it has a few advantages. SPF (also called dynamic packet filtering) keeps track which connections are initiated from hosts in the private network, which is useful as it makes traffic outbound possible and at the same time inbound traffic is blocked [16].

Proxy –firewalls break traffic flow between the host in the public network and the host in the private network. Proxies do not simply block traffic to certain ports but they act as proxy servers and process access requests. Proxies prevent direct communication with hosts on different sides of the proxy. This is safe, but needs more processing power than ordinary packet filter style firewalls.

Logs

The administrators of a network should check up the logs on the system time to time. By peeking firewall logs administrator can keep up with new winds on hacking scene as scriptkiddies tend to try out new exploits and hacking tools as soon as they are available. Suddenly increased attempts on a certain port could indicate that there is a new vulnerability to the service on that port.

Service specific logs could reveal password misusage attempts etc. In general the logs contain much useful data which could lead to actions to improve security [25].

IDS

One way to automate intrusion detection is to use an intrusion detection system. Intrusion detection systems detect abnormal activity on network by using statistical data or fingerprints of common software used by hackers. Intrusion detection systems may report the abnormalities they detect or block the malicious traffic.

Honey Pots

Honey pots are decoy servers or systems that pretend to be vulnerable parts of a network and their function is to lure intruders to attack them. The point in honey pots is that they do not offer any real services but because hackers do not know that, they believe that they are breaking into a real service. By breaking into a honey pot hackers leave valuable data about the techniques they use behind. Honey pots can also be used to gather evidence about security incidents in order to have intruders prosecuted.

Configuration

As mentioned earlier, careful configuration of services help defending from attackers. Statistics based on reports given by crackers reveal that over one fourth of all web page defacements are done by taking advantage of bad configuration or other mistake in site administration. The same applies to any other services on any network. Badly configured service could compromise the whole system as root privileges could be granted to 3rd party by a single misconfiguration.

Medium Safety

WLAN

Wireless local area networks have increased their popularity in the last few years. As lesser experienced users can set-up a network without any modifications on the infrastructure, such as cabling routes, with relatively cheap price this has lead to fast gain of markets. When using acronym WLAN, 802.11b or g –versions are normally what is meant. 802.11b, WiFi, -networks operate at 2,5 GHz frequency at 11Mbit/s speed. B-standard supports wired equivalent privacy (WEP), scheme for encrypting traffic between mobile node and access point on OSI layers 1 and 2. As its name tells, WEP was designed to be as secure as ordinary wired lines. It certainly makes casual eavesdropping more difficult but is still far away from wired equivalent.

WEP Theory

WEP is used for encrypting plain text data, which is to be sent over a wireless link. WEP-process first calculates CRC32 –value of the plain text and attaches this value to the end of plain text. After that initialization vector (IV) and secret WEP-key are attached and processed with RC4 (PRNG) algorithm to produce so called keystream. WEP uses RC4 –algorithm for creating keystream that is used to create ciphertext. RC4 is a nonpublic algorithm which has leaked into public in 1994. Plaintext with CRC-value in its tail and keystreams are then XORed to produce ciphertext. The final packet to be sent over wireless link is formed by unencrypted IV and this ciphertext block [21]. The process is described in the following figure 2.

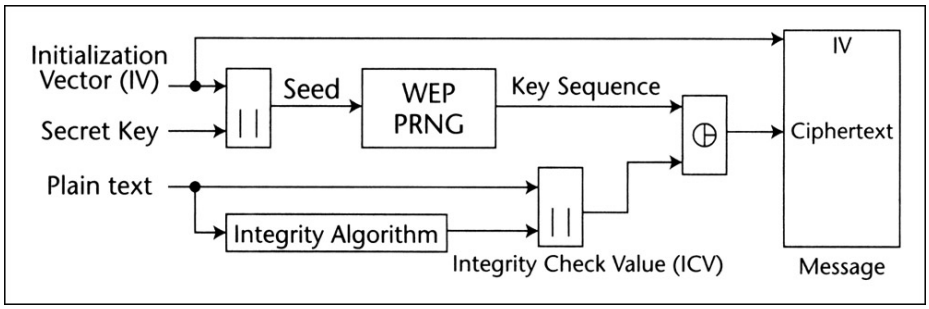

Figure 2, Encryption process in WLAN [21]

The corresponding node that receives the packet decrypts the packet with same functions but in reverse. Ciphertext without IV is first XORed with keystream, which is calculated in the same manner as in encryption scheme. From the resulting block of plaintext and crc-value the crc-value is compared to recalculated crc value. If these do not match, the packet has been tampered with or WEP-key has been incorrect [21].

WEP Flaws

WEP has a weakness in its way of creation of initialization vectors. The initialization vector is 24 bits long value so there are 1677216 different IV: s available. Because initialization vector should not be used more than once, the amount of transmitted data is limited before the initialization vectors have run out.

WEP does not have any decent key management system either. The key used in WEP is the same for encryption and decryption, so the key must be known by the both sender and receiver. Because of the flaw with initialization vectors, the WEP-key should be changed before IV-exhaustion, but system does not have scheme for key interchanging between access point and mobile node. This also leads to scalability issues, as the same key is used by everyone on the network. In large networks, or any semi public network in general, anyone can leak the key to an outsider and thus provide access to network for an unauthorized party. If the key has leaked or the IV –pool has been used there is no method to distribute a new key for, say 1000 or even 100 mobile nodes, so WEP definitely suffers from scalability problems.

Though WEP is told to use 64 or 128 bit keys, truth is that 24 bits are taken by clear initialization vector. So the length of a key is actually 40 or 104 bits [19]. This does not make practically any difference if two IV-vectors are used; the time for cracking the key remains the same. But if 40 bit key is used, the time for brute-forcing the key is clearly less than a year using a normal Pentium 2 computer. This may sound like a lot of time, and the key is probably changed during that time, but there is a possibility that there is a whole cluster cracking the key, so the time could be a lot less. With 104 bit key the time for brute-forcing a key would take hundreds or thousands of years [12].

Maybe the most popular way of attacking WEP is a method that encryption analysts Fluhrer, Mantin and Shamir introduced. They discovered that there are flaws in RC4 and the WEP implementation of RC4. One important observation was that RC4 algorithm generated weak initialization vectors, and if a sufficient amount of these are collected one could crack the WEP key. Implementations of this FMS –attack can manage to resolve the WEP key with a few million sent packets. [21] FMS –attack could resolve WEP key within a few hours in a network with high load. If the traffic on wireless network is light retrieving the key could take weeks. Attackers use methods that generate traffic into wireless network to shorten the time required to crack the WEP key in use.

The weak key issue is noticed among the WLAN hardware manufacturers. Enlightened manufacturers have updated their firmware to such that simply skip the weak initialization vectors.

MAC Authentication

Some wireless access points have of feature that allows only predefined MAC-addresses to connect to AP. When a mobile node connects to access point the AP checks the so called hardware address (MAC) of the connecting node. If the address is not found from the list of allowed addresses, mobile node is not allowed to connect [17].

This may sound like a good and secure idea, but actually is not even as good method to protect access to network as WEP, because mac-access can be easily forged [17].

Denial of Service in WLAN

Wireless environment is sensitive to disturbance and even the 802.11 –protocol leaves a few possibilities for denial of service attack. Malicious user could easily block traffic on one or more WLAN channels by saturating the media. This is mainly because of half-duplex environment WiFi is based on and the ease of flooding bogus data on the media [17].

References

[1] Bosworth Seymor, Kebay M.E: Computer Security Handbook 4ed, John Wiley & Sons 2002

[2] Check Point Software Technologies: Principles of Network Security, Check Point Software Technologies 2003

[3] Kaye Doug, Loosely Coupled: Missing Pieces of Web Services, RDS Press 2003

[4] Skillsoft Press: Cryptography Protocols and Algorithms, Skillsoft press 2003

[5] Menga Justin, Timm Carl: CCSP: Secure Intrusion Detection and SAFE Implementation Study Guide, Sybex 2004

[6] Howard Michael: Designing Secure Web-Bases Applications for Microsoft Windows 2000, Microsoft Press 2000

[7] ITU-T: Compendium of Approved ITU-T Security Definitions edition 2003 February, ITU 2003

[8] Peuhkuri Markus: Lecture Material: Securing the Network and Information, 2004

[9] Nguyen Hung Q., Johnson Bob, Hackett Michael: Testing Applications on the Web: Test Planning for Mobile and Internet-Based System 2nd Edition, John Wiley & Sons 2003

[10] Russell Ryan et al., Stealing the Network: How to Own the Box, Syngress Publishing 2003

[11] Koconis David, Murray Jim, Purvis Jos, Wassom Darrin: Securing Linux: A Survival Guide for Linux Security, SANS Institute 2003

[12] Erickson Jon: Hacking: The Art of Exploitation, No Starch Press 2003

[13] Mirza Ahmad David R. et al.: Hack Proofing Your Network, 2nd Edition, Syngress Publishing 2002

[14] Wang Wallace: Steal This Computer Book 3: What They Won't Tell You About the Internet, No Starch Press 2003

[15] Preethan V.V.:Internet Security and Firewalls, Premier Press 2002

[16] Brenton Chris, Hunt Cameron: Mastering Network Security, 2nd Edition, Sybex 2003

[17] Rittinghouse John, Ransome James:Wireless Operational Security, Digital Press 2004

[18] Crayton Christopher A.: The Security+ Exam Guide:TestTaker's Guide Series. Charles River Media 2003

[19] Schmied Will et al.:MCSE/MCSA Implementing & Administering Security in a Windows 2000 Network Study Guide, Syngress Publising 2003

[20] Netcraft: Site Outages for The SCO Group, http://news.netcraft.com/archives/2004/05/27/site_outages_for_the_sco_group.html

[21] Vines Russell Dean: Wireless Security Essentials: Defending Mobile Systems from Data Piracy, John Wiley & Sons 2002

[22] Shimonski Robert J. et al.: The Best Damn Firewall Book Period, Syngress Publishing 2003

[23] Andres Steven, Kenyon Brian: Security Sage's Guide to Hardening the Network Infrastructure, Syngress Publishing 2004

[24] CSI/FBI: Computer Crime and Security Survey 2004

[25] Andress Mandy, Cox Phil, Tittel Ed (ed): CIW Security Professional Certification Bible, John Wiley & Sons 2001